KEEPING IT TO THEMSELVES: BANK PRIVACY TOWARDS 2000

Simon Crawford[*]

Financial institutions and their families of service providers are among the largest collectors of the personal information of the everyday consumer. As these corporate families become larger, through relaxed powers of investments and mergers among Canada's banks, centralized electronic warehouses of information are being amassed. It is trite to say that these data banks serve more than a mere functional role in the administration of bank accounts. The information that a financial institution collects about its customers is a marketable commodity, both within the bank's own family of institutions and, to an immeasurable number of marketers who wish to target people of a specific income level, risk sensitivity, job group, age group, geographic group, or any combination of the many criteria by which a financial institution classifies its customers. In fact, the value of the information is inflated by the absence of rules governing its collection, use and disclosure. Information that can be freely bought or sold, is of greater value than information that can only be transferred with consent, for a specific purpose, or some similar limitation. Thus, it's not surprising that the collection, use and disclosure of customers' personal information by banks has gone largely unregulated in this age of electronic information. The free flow and marketability of personal information, while flying in the face of personal liberties, has

Les institutions financières et les groupes de sociétés de services qu'elles possèdent comptent parmi les plus importants collecteurs de renseignements personnels sur les consommatrices et les consommateurs ordinaires. Comme ces groupes de sociétés deviennent de plus en plus gros, grâce à l'élargissement des pouvoirs d'investissement et aux fusions parmi les banques canadiennes, de larges banques de données centralisées sont en train d'être constituées. Inutile de dire que ces banques de données jouent plus qu'un simple rôle fonctionnel dans l'administration des comptes bancaires. L'information qu'une institution financière recueille sur sa clientèle est un produit commercialisable, aussi bien parmi le groupe de sociétés de la banque que parmi un nombre incommensurable de spécialistes en commercialisation désirant cibler un niveau de revenu particulier, l'acuité d'un risque, un groupe d'emploi, un groupe d'âge, un groupe habitant une région géographique ou une combinaison des nombreux critères dont se sert une institution financière pour catégoriser sa clientèle. En outre, l'absence de règles régissant la collecte, l'utilisation et la divulgation des renseignements accroît leur valeur. Des renseignements qui peuvent être commercialisés, achetés ou vendus librement ont plus de valeur que des renseignements qui ne peuvent être communiqués qu'à la suite d'un consentement, à une fin précise ou en respectant une restriction semblable.

---

* The author would like to thank those members of QMI who suffered questions on the technicalities of the recognition process.

The author received insight into the goals of the CBA thanks to the patient contributions of Consumer Affairs, Canadian Bankers Association.

The author is indebted, in part, to the contributions of Industry Canada, and the Ministry of Finance, for the following discussion.

made good economic sense. It has been a profitable commodity.

For the greater part of the twentieth century a bank customer has had to rely on the common law in order to protect that information she provided to her manager when opening an account or applying for a loan. The common law has maintained the notion that there exists in every bank/customer agreement, an implied term of confidentiality which allows the bank to disclose information either with the customer's consent, or when compelled by law, its own interests, or the interests of the public. While this notion has survived and developed with the changing personality of banking, it has fallen behind as of late. Banks now provide more services than ever before, to more individuals than ever before, and with less personal contact than ever before. There now exists the possibility that the personal information of hundreds of thousands of individuals can be transmitted in a single transaction – and that this same information can almost instantaneously be adapted to a mailing list to market a product entirely unrelated to each individual's interest in the bank. This ability is entirely beyond the contemplation of the implied term of confidentiality.

Accordingly, the international community, through the OECD and the European Union have looked to regulatory schemes to control and protect the personal information of individuals. Both organizations have set out principles for their constituent members governing the collection, use and disclosure of individuals' information. In Canada, the Canadian Standards Association has set the national standard through its voluntary code of privacy principles. Likewise, the Canadian Bankers Association has adopted privacy principles for its members, and has required that each financial institution adopt its own privacy compliance program. However, as encouraging as these voluntary codes of conduct and guidelines are, they do not place a legal obligation on financial institutions, backed by enforceable sanctions, to take care with their customers' personal information. Instead, they operate in the shadow of the

Il n'est donc pas surprenant que la collecte, l'utilisation et la divulgation des renseignements personnels sur la clientèle des banques n'aient pas été beaucoup réglementées en cette ère de l'information électronique. Bien qu'elles entravent les libertés individuelles, la libre circulation et la commerciabilité des renseignements personnels représentent le bon sens économique, car elles sont payantes.

Pendant la majeure partie du 20e siècle, la clientèle d'une banque devait compter sur la common law pour protéger les renseignements qu'elle fournissait à la direction de la banque lors de l'ouverture d'un compte ou d'une demande de prêt. La common law a conservé l'idée qu'il y a dans toutes les ententes entre la banque et sa clientèle, une condition implicite de confidentialité qui permet à la banque de divulguer des renseignements lorsqu'elle a le consentement de sa clientèle ou lorsque la loi, ses propres intérêts ou ceux du public l'exigent. Bien que cette idée ait subsisté et mûri en raison de la nature changeante de l'activité bancaire, elle a reçu une moins grande adhésion ces derniers temps. Les banques offrent maintenant plus de services que jamais, à un plus grand nombre de personnes que jamais, avec lesquelles elles n'ont jamais eu aussi peu de contacts personnels. Il est maintenant possible que les renseignements personnels de centaines de milliers de personnes soient transmis en une seule opération et que ces mêmes renseignements soient traités presque instantanément pour constituer une liste d'envois dans le but de commercialiser un produit qui n'a aucun rapport avec l'intérêt que chaque client ou cliente porte envers la banque. Cette possibilité n'est absolument pas prévue par la condition implicite de confidentialité.

Par conséquent, la communauté internationale, par l'entremise de l'OCDE, et l'Union européenne se sont penchées sur les systèmes de réglementation permettant de contrôler et de protéger les renseignements personnels. Ces deux organismes ont établi, pour leurs membres, des principes régissant la collecte, l'utilisation et la divulgation de renseignements personnels. Au Canada, l'Association canadienne de normalisation a fixé la norme nationale grâce à son code

law, and at best rely on the good corporate citizenship of financial institutions.

As the millennium approaches there is a need for comprehensive and enforceable Canadian legislation governing how not only banks, but all private sector collectors of consumer information, handle the sensitive and personal records of individuals. Arguably, the movement has begun, built on the back of the Canadian Standards Association initiatives, and spurred by the momentum of recent privacy legislation in Quebec and the insistence by the European Union that action be taken. Towards 2000 the individual will have to recapture her interest in her personal information by insisting that the state legislate protection.

d'autoréglementation sur la protection des renseignements personnels. De même, l'Association des banquiers canadiens a établi pour ses membres des principes sur le respect de la vie privée et a exigé que chaque institution financière adopte son propre programme de respect de la vie privée. Cependant, aussi encourageants que ces codes d'autoréglementation et ces lignes directrices soient, ils n'imposent pas aux institutions financières d'obligation légale, assortie de sanctions applicables, qui les forcerait à traiter avec soin les renseignements personnels de leur clientèle. Au lieu de cela, leur application est volontaire et au mieux ils comptent sur la conscience sociale des institutions financières.

À l'aube du deuxième millénaire, il faut que l'on adopte au Canada une loi exhaustive et applicable qui régit la façon dont les dossiers personnels et confidentiels sont traités non seulement pas les banques mais aussi par toutes les entreprises du secteur privé qui recueillent des renseignements sur les consommateurs et les consommatrices. On peut soutenir qu'un mouvement en ce sens s'est amorcé dans la foulée des initiatives de l'Association canadienne de normalisation, de l'adoption récente d'une loi sur la protection de la vie privée au Québec et des démarches insistantes de l'Union européenne visant à ce que des mesures soient prises. Vers l'an 2000, les gens devront se réintéresser à leurs renseignements personnels et insister pour que l'État adopte une loi protégeant ces renseignements.

TABLE OF CONTENTS

I. INTRODUCTION

> I simply think that when you concentrate so much economic power in one place, and so much of the sensitive, frequently intimate, personal information of Canadians in one hand, that...a well-intentioned promise to be good and respectful of people's rights is not sufficient.[1]

Efficiency in information transfer has increased rapidly in the last decade, and with this efficiency new threats to the security of that information have surfaced. The unauthorized disclosure of information by banks was, at one time, a personal matter. Typically a customer might have one complaint with one bank about an isolated injurious breach of confidence. However, as banks amass greater storehouses of client information, and as the commercial potential of that information is increased, the threat of grand scale disclosures becomes a reality. Unauthorized information is transferred not in loose tongued conversations, but in streams of silent modem and satellite transfers.[2] A present day cost-analysis, however, suggests that the potential profit of unauthorized information disbursement far outweighs the worst pecuniary sanctions. This is especially true in light of the changing face of Canadian banks. The proposed Toronto-Dominion Bank/Canadian Imperial Bank of Commerce and Bank of Montreal/Royal Bank of Canada mergers, if successfully consummated, would result in two of the largest private sector collections of the personal information of Canadians. Banking mergers, though not prohibited by law, have historically been prevented by a Federal policy of containment. Not since the 1960s when John Diefenbaker's Finance Minister, Donald Fleming protected the Toronto-Dominion Bank from New York-based Chase Manhattan's take-over bid, has this policy of containment been so openly challenged.[3] But while many Canadians see the proposed Canadian mega-banks as global competitors to the U.S. giants, few recognize that the new banking forces will know more of us more intimately than any bank before them and will remain largely unregulated in their use of our personal information.

The following discussion has two parts. The first looks at how the common law has regulated the use of information passed from customer to bank through both contract and tort constructions. The second explores the method for regulating information privacy that has emerged in the last decade - voluntary privacy codes, and the recent proposals to replace (or at least enforce) them through legislation. There are international, national, sectarian, industry and consumer pressures for certainty in how information is controlled in the hands of financial institutions. Whether that certainty is realized by the courts, the legislature or by self-regulation, remains to be determined.

---

[1] Standing Committee on Finance, Minutes of the Privacy Commissioner's presentation to the Standing Committee on Finance, 1996.

[2] C. Bennett, "Privacy Protection for the Information Highway in Policy Options" (1995) 16 Policy Options 43 [hereinafter "Privacy Protection"].

[3] Andrew Willis, "Banking on It" *The [Toronto] Globe and Mail* (13 December 1997) D1.

II. CONFIDENTIALITY IMPLIED -THE CONTRACT

A. Tournier *v.* National Provincial Bank

There is an implied duty of confidentiality attached to contracts between a bank and its customers. The *locus classicus* for the expression of this duty is *Tournier v. National Provincial Bank.*[4] The Court of Appeal was presented with Mr. Tournier who, having no residential address, had given the name and telephone number of his new employers to the bank. The bank subsequently discovered a cheque that had been made payable to Mr. Tournier, which he in turn had endorsed to a bookmaker – a wholly unsavory relation in the eyes of the 1920's British bankers. When Mr. Tournier defaulted on a payment plan the bank manager contacted Mr. Tournier's employers to receive his current address. In that conversation the bank manager disclosed the fact of the overdraft and the default and reported that Mr. Tournier had been engaged with bookmakers. As a result, Mr. Tournier's employers refused to extend his probationary employment to full employment.

Bankes L.J. held that the bank had a contractual duty to maintain the confidentiality of Mr. Tournier's information subject to some clawbacks:

> The Court will only imply terms which must necessarily have been in contemplation of the parties in making the contract. Applying this principle to such knowledge of life as a judge is allowed to have, I have no doubt that it is an implied term of a banker's contract with his customer that the banker shall not disclose the account, or transactions relating thereto, of his customer except in certain circumstances.[5]

The duty of confidentiality is qualified by four conditions which permit disclosure: 1) under compulsion of law; 2) where there is a duty to the public to disclose; 3) where the interests of the bank require disclosure; and 4) where the disclosure is made with the express or implied consent of the customer.

Atkin L.J., in his concurring opinion, further qualified Bankes L.J.'s categories.[6] He held that the bank may disclose information with the customer's consent, and if without consent, then only when it is necessary to protect: the public, the bank, or interested persons against fraud or crime; or the bank's interests in relation to transactions for or with the customer.[7]

In reality, the contract between the bank and customer sets up a series of conflicting duties or a hierarchy of obligations on the bank. The bank has a duty to the public, which according to Atkin L.J., includes a duty to protect the public against fraud or crime. And, it has a duty (or power) to protect the bank's interests, but perhaps only those interests that are related to the specific relationship between the bank and the particular customer. There is a duty (or compulsion) to comply with the law, although what "law" signifies is ambiguous. There may also be a duty to protect *interested persons* against fraud or crime, though who these persons are is undefined. Running

---

[4] *Tournier* v. *National Provincial Bank* [1924] 1 K.B. 461(C.A.) [hereinafter *Tournier*]. At trial before Avory J. judgment was entered for the bank. Although the Court of Appeal ordered a new trial, no evidence that the second trial was held exists which implies that the case settled.

[5] *Ibid.* at 480.

[6] *Ibid.* at 486.

[7] *Ibid.*

alongside this carriage of duties, and easily overtaken by them, is the implied duty of confidentiality to the customer.

B. *Scope of the Duty of Confidentiality*

The Court in *Tournier* looked also at the scope of the duty - how much of the ongoing bank/customer relationship would be covered by the duty and whether the duty extended beyond the life of the relationship and the contract.[8] Bankes L.J. set three limits on the duty: 1) the duty does not cease immediately on the closing of the account; 2) the duty is not confined to the "actual state of the customer's account" but extends to information "derived from the account itself"; and 3) the duty is not confined to information obtained from the customer; rather, information acquired by bankers, *acting in the character of bankers,* is covered.[9]

Atkin L.J. delineated the parameters of the duty more broadly, stating that the duty covers more than just account information "if the occasion upon which the information was obtained arose out of the banking relations of the bank and its customers - for example, with a view to assisting the bank in conducting the customer's business, or in coming to decisions as to its treatment of its customers".[10] Atkin L.J. held also that the duty of confidentiality could attach to information acquired both before the relation of banker and customer was in contemplation and after it ended.[11] Strutton L.J., concurring, restricted the duty to that information acquired from the account of the customer, excluding information gathered about one customer from the records of another. This latter limitation has been eroded in subsequent cases.[12]

1. *Disclosure under Compulsion of Law*

Courts have applied the duty under compulsion of law to compel the discovery of bank documents, that would otherwise be confidential, to assist the police,[13] and to assist tax collection by the taxation authorities.[14] The underlying premise is that a contract between bank and customer is subject to the general law of the land. *In Parry Jones* v. *Law Society*, Diplock L.J. stated:

> Such a duty (of confidence) exists not only between solicitor and client, but, for example, between banker and customer, doctor and patient and accountant and client. Such a duty of confidence is subject to, and overridden by the duty of any party to that contract to comply with the law of the land. If it is the duty of such a party to a contract, whether at common law or under statute, to disclose in defined circumstances confidential information, then he must do so, and any express contract to the contrary would be illegal and void. For example, in the case of banker and customer, the duty of confidence is subject to the overriding duty of the banker at common law to disclose and answer questions as to this customer's affairs when he is asked to give evidence on

---

8 *Tournier* at 473.
9 *Ibid.*
10 *Ibid.* at 485.
11 *Tournier* at 481.
12 I. Baxter, *The Law of Banking* 3d ed. (Toronto: Carswell, 1981) at 12.
13 Compare *Bankers Trust Company* v. *Shapira and others* [1980] 3 All E.R. 353.
14 Compare *Attorney-General* v. *National Provincial Bank Ltd.* (1928) 44 T.L.R. 701.

them in the witness box in a court of law.[15]

a) *Canada*

In Canada, it is clear that disclosure under compulsion of law includes disclosures made pursuant to court orders[16] and legislation. [17] The courts have also determined that compulsion of law does not mean necessarily compulsion of Canadian law.[18] However, there is a distinction between the implied term of confidentiality and privilege. In other words, the implied duty of confidentiality does not support a claim for privileged communications in the discovery process. Atkin L.J. stated that "it is plain that there is no privilege [in bankers] from disclosure enforced in the course of legal proceedings."[19] While Canadian law recognizes the need to protect certain categories of confidential relationships[20] from disclosure requirements, these do not include the relationship between banker and customer. As Lord Denning stated:

> The only profession that I know which is given a privilege from disclosing information to a court of law is the legal profession, and then it is not the privilege of the lawyer but of his client. Take the clergyman, the *banker* or the medical man. None of these is entitled to refuse to answer when directed to by a judge.[21]

The rule of thumb is that confidentiality of information does not equate to privilege.[22] Beyond the recognized categories one would have to satisfy Wigmore's four criteria in order to claim privilege.[23] In *I.T.L. Industries Ltd.* v. *Winterbottom*[24]

---

[15] [1969] I Ch.d. 1 [hereinafter *Parry-Jones*].

[16] In *Haughton* v. *Haughton* [1965] 1 O.R. 481, the Court held that a bank manager could only be compelled to testify by a specific order of the court, and that a subpoena would be insufficient. This specific order, the Court held, would constitute the requisite 'compulsion of law' to override the banker's duty of confidentiality. This was later affirmed in *Royal Bank of Canada* v. *Art's Welding & Machine Shop* (1980), (1989) 34 C.P.C. (2d) 190, A.W.L.D. 653, C.L.D. 895 [hereinafter *Art's Welding*] in which the Court held that a court order would constitute the *compulsion of law.*

[17] The Court in *Budzisch* v. *Toronto Dominion Bank* [1996] 2 C.T.C. 278 [hereinafter *Budzisch*], dealt with the statutory power of Revenue Canada to demand that a bank provide a customer's bank records for inspection. However, in this case the parties conceded that the demand constituted a *'compulsion of law'.*

[18] In *Park* v. *Bank of Montreal* [1997] B.C.J. No. 787 (B.C.S.C.) (Quicklaw), the Court found that a bank's disclosure through its Korean Branch to the Korean criminal prosecutor's office constituted a compulsion of law because the disclosure was required under Korean law.

[19] *Tournier supra* note 4 at 486. In fairness, Atkin L.J.'s comment is *obiter dicta*; however, it is likely that the matter of disclosure in legal proceedings operates notwithstanding the rule in *Tournier.* Arguably, no party can contract out of the duty to testify or to disclose in legal proceedings.

[20] S. Schiff, *Evidence in the Litigation Process* Vol. 2 (Toronto: Carswell, 1993) at 1099.

[21] *Attorney General* v. *Mulholland* [1963] 1 All E.R. 767 at 771.

[22] *Upham* v. *You* (1986) 73 N.S.R. (2d) 73, 176 A.P.R. 73, 11 C.P.C. (2d) 83 (N.S.S.C.) Note that the Court also gives brief consideration to *Tournier.*

[23] The law has recognized the Wigmore criteria in *Slavutych* v. *Baker* [1976] 1 S.C.R. 254, 260, 55 D.L.R. (3d) 224, 228-29. The criteria are enumerated in J. Wigmore, *Evidence*, sections 2332-41 (3 ed. 1940) as: "(1) the communications must originate in a confidence that they will not be disclosed (2) this element of confidentiality must be essential to the full and satisfactory

the Court considered the relationship between the contractual duty of confidentiality and discovery privilege. In this case there was an application under s.34(5) of the *Evidence Act* to discover bank records. The Act provided that "on the application of a party to an action, the court or judge may order that such party be at liberty to inspect and take copies of any entries in the books or records of a bank for the purposes of such proceeding, but a person whose account is to be inspected shall be served with notice of the application".[25] The Court noted that there exists no privilege over bank records analogous to that protecting communications between a solicitor and client, indicating that it is not necessary to resort to the 'compulsion by law' exception when compelling a bank employee to testify or to disclose bank records at discovery.

b) *United Kingdom*

As in Canadian law, the English position since *Tournier* has remained that duties of confidentiality arising out of private ordering are subject to the general law,[26] whether it be a court order[27] or legislation.

c) *Australia*

The Australian courts have affirmed the application of this exception to the duty of confidentiality, and have, like the British and Canadian courts, often framed it as the subordination of private ordering to the general law. In *Smorgon* v. *Australia and New Zealand Banking Group Ltd.*, the Court affirmed the allowance in *Tournier* of a bank's disclosure under compulsion of law. The Court reasoned:

> [T]he duty of confidence [between banker and customer]...is no more than a simple contractual one which, like any other contractual term, will be subject to the operation of the general law. As Diplock L.J. said in *Parry-Jones* (1969) 1 Ch. at 9, speaking of such a mere contractual duty, "[s]uch a duty of confidence is subject to, and overridden by, the duty of any party to that contract to comply with the law of the land" ... if the legislature plainly says that those having information shall disclose it to the

---

maintenance of the relationship between the parties (3) the relation must be one which in the opinion of the community ought to be sedulously fostered (4) the injury that would enure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation. Only if these four conditions are present should a privilege be recognized."

[24] *I.T.L. Industries Ltd.* v. *Winterbottom* (1979) 24 O.R. (2d) 161, 97 D.L.R. (3d) 553.

[25] *Evidence Act*, R.S.O. 1970, c. C151, s. 34(5). For the current law see R.S.O. 1990, c. E23 as amended by S.O. 1993, c.27, s.33.

[26] Among the early decisions which dealt with contractual rights of confidentiality was *Parry-Jones, supra* note 15. In that case, Diplock L.J. stated that any mere contractual duty such as a duty of confidence is overridden by the "duty of any party to comply with the law of the land".

[27] The British Court in *Barclay's Bank P.L.C.* v. *Taylor* [1989] 3 All E.R. 563 C.A. found that a court order provided to the bank by the police allowing them to inspect bank records constituted compulsion under law. In *Robertson v. Canadian Imperial Bank of Commerce* [1994] J.C.J. No.33 (Privy Council) [hereinafter *Robertson*], the Court found that a court subpoena compelling a bank official to testify with respect to a customer's account constituted the compulsion of law.

Commissioner then no mere contractual duty of confidentiality shall stand in the way.[28]

Banks may be compelled by law under a number of Australian regulations[29] to disclose customer information, including:

Cash Transaction Reports Act 1988 - This Act requires banks to report significant or suspicious transactions to the regulatory agency and to report information to law enforcement and taxation authorities.[30]

Proceeds of Crime Act 1987 - This Act may compel disclosure of information to police officials and allow the ongoing monitoring of accounts.[31]

It would appear, however, that the term "law" pursuant to which the duty exists, may not be restricted to legislation[32] or to court orders. In *A.* v. *Hayden*[33] the Court suggested that it is likely that the duty of confidentiality is overridden by a duty to disclose customer information to an officer of a "competent police force investigating a reasonably apprehended breach of the criminal law."[34] What is unclear from this comment is whether this overriding duty to disclose customer information in order to facilitate the enforcement of criminal law is a duty under compulsion of law or a duty in the public interest.

Interestingly, the Australian courts have also found that where a disclosure is made by a bank under compulsion of law, the agency receiving the information is under a duty

---

[28] In *Smorgen* v. *Australia and New Zealand Banking Group Ltd.* (1976) 134 C.L.R. 475 the Court followed *Parry-Jones, supra* note 15, and found that no contractual duty of confidentiality, including that implied in a banking contract, can override a party's duty to comply with legislation. This position was affirmed in *Re: Peter Lawrence Crowley* (1981) 52 F.L.R. 123.

[29] S. Blay, *Australian Law of Financial Institutions* (Sydney: Harcourt Brace, 1993) at 298. The author is indebted to this text for the majority of this section. It provides a comprehensive address on the legislative instruments that require banks to disclose customer information.

[30] *Ibid.* at 325 reports that, when this Bill was before the Senate in 1988, the Democrats voiced concerns that the legislation would 'undermine the safeguards for the citizen which evolved in the common law over centuries, and [has] more than a passing flavour of totalitarianism."

[31] *Ibid.* at 328. As a matter of comparison, it is interesting to note that section 74 of the Act prohibits the bank from informing the customer that officials have been given access to the financial records. This should be considered in light of the ruling in *Robertson supra* note 27 in which the Privy Council recognized the possible existence of an implied contractual duty to inform a customer of disclosures compelled by law.

[32] In *Re: Kingston Thoroughbred Horse Stud and Australian Taxation Office No. N85/130* (Administrative Appeals Tribunal) (1986), 15 April 1986 AAT No.2624, document 2360 (QL) [hereinafter *Kingston Thoroughbred*] the Court specifically confirmed that the duty under law would include laws requiring the bank to provide documents to administrative agencies. The Court in *Kabwand Pty. Ltd.* v. *National Australia Bank Limited* (1989) No.G355 of 1988, Fed No. 195 (Federal Court of Australia), pointed to the disclosure requirements in the *Banker's Books Evidence Act* as being a compulsion under law. In *Australian Securities Commission* v. *Westpac Banking Corporation* No. QG3018 of 1991, Fed No. 746, 10 A.C.L.C. 11/6, A.C.S.R. 350, (1991) 105 ALR, (1991) 32 FCR 546, the Court found that the *Australian Securities Commission Act 1989* requirement that banks provide customer information to the regulators constituted 'compulsion under law'.

[33] (1984) 156 CLR 532, 6 November 1984, document 5529 (QL).

[34] *Ibid.* at 152 (QL).

with respect to the information received. In *Kingston Thoroughbred* the Administrative Appeals Tribunal found that when a bank is compelled to provide documents to a government agency for administrative functions, there is an implication that the provision of those documents is in confidence and that the agency will use the documents only for its own purposes. The tribunal stated:

> [There is] a long-existing understanding by the supplying banks, that the extent and detail of the information they contain and the co-operation extended, were being given on the implication that their supply,...was within confidence, and to be used only for the Commissioner's own purposes. Such an implication may more readily be arrived at we believe, when one has regard to a bank's obligations at law as to preserving the secrecy as to its client's affairs.[35]

Accordingly, it may be that, at least in Australian law, the basic duty of confidentiality binding banks obliges and binds those recipients of confidential information obtained from the bank by operation of law.

d) *United States*

There is some indication that the American courts are limiting the exceptions in *Tournier* to disclosure either with customer consent or under compulsion of law (court orders and legislation)[36], and may be distinguishing between the rights of depositors and borrowers.[37] In *Suburban Trust Co.*[38] the Court stated that the criteria in *Tournier* "confer upon a bank entirely too much discretion" and that, in the absence of consent, disclosure should only be made when compelled by law.[39] However, it would appear that in many cases the bank's duty to subordinate the customer's right to confidentiality to a court order is prescribed by statute.[40] One case suggests that neither a court order

---

[35] *Kingston Thoroughbred, supra* note 32 at 6 (QL).

[36] The Court has stated that a court order is not required in order for a bank to provide customer records to the Internal Revenue service. Compare *Jacobsen* v. *Citizens State Bank* 587 SW 2d 480 (Tex. Civ. App., 1979). A customer deposited cash in consecutively numbered $50 and $100 bills. The bank contacted the police because it was suspicious and the police arrested the customer. It later became evident that the customer had been wrongly accused. The customer sought damages from the bank for breach of its duty of confidentiality.

[37] R.E. Huhs Jr., "To Disclose or not to Disclose Customer Records" (1991) 108:30 *The Banking Law Journal* 30. At 34, the author points out that in *Graney Development Corp.* v. *Tasken* 92 Misc. 2d 764, 400 N.Y.S. 2d, 717 (1978) the Court stated that a distinction can be drawn between a depositor's and borrower's expectations of bank confidentiality – that "while a creditor, who publishes his debtor's defaults to the public at large may be liable for breach of privacy..., he will not be liable (in the absence of malice) if he divulges the defaults not to the public at large, but privately to selected individuals..."

[38] (1979), 44 M.D. 335 (Spec. App.), 408A 2d at 758 [hereinafter *Suburban Trust Co.*].

[39] There is an American commentary (10 AM. Jur. 2d *Banks 332* (1963)), which holds that the criteria in *Tournier* are consistent with American law; however, the Court in *Suburban Trust Co.* considered and dismissed this commentary at 764.

[40] A grand jury subpoena of bank records does not violate any federal common law duty of confidentiality. In fact, the purpose of the *Bank Secrecy Act* (12 USCS § 1829b(a)(1)), is record keeping for use in possible later criminal regulatory investigations. Compare *United States v. Nelson* 91980, WD Mich, 486 F. Supp 464. Huhs, *supra* note 37 at 41, does point out however, that the decision in *Suburban Trust Co.* might be explained, at least in part, by the fact that the

nor legislation may be required where a bank is faced with a police inquiry and has knowledge of its customer's potentially fraudulent activities.[41]

In any event, it would appear that the American courts have, in many cases, dealt with many of the issues of bank confidentiality outside the scope of the *Tournier* decision.[42]

2. *Duty to the Public to Disclose*

a) *Canada*

The Courts have recognized that the duty of confidentiality can be overridden by a "high[er] duty" to protect public interests where there is a danger to the state or the public.[43]

The duty to the public exception has developed sporadically in Canadian common law. To date it has been suggested by the court that there is a public interest in protecting the wellbeing of children[44] and in inspecting the accounts of a liquidated financial institution[45]. However, in at least one case the court has rejected the idea that this exception permits a bank employee to communicate to members of the public its

---

Maryland Legislature, under which it was decided, had passed extensive legislation on banks' disclosure of information. For a more comprehensive examination of the legislative initiatives taken to control the disclosure of information, consider Mary Catherine Green, *The Bank Secrecy Act and the Common Law: In Search of Financial Privacy*, in Arizona Journal of International and Comparative Law, Vol 7 '90 261-286. Green suggests that exceptions such as those in *Tournier* make it easy to do away with the common law principle of confidentiality and that a better approach would be to weigh the rights of the customer against those of the government to determine if information should be disclosed. For a discussion of the *Right to Financial Privacy Act*, compare Sarah Elizabeth Jones, *Right to Financial Privacy: Emerging Standards of Bank Compliance* in *The Banking Law Journal* v. 105 Jan/Feb 1988 37. The R.F.P.A. prohibits Federal bodies from obtaining financial records without the customer's consent or notice provisions.

[41] In *State* v. *McCray*, 15 Wash App 810, 551 P2d 1376, the Court determined that a bank may answer police questions when it is obvious that its customer has acted fraudulently.

[42] For instance, in *Burrows v. Superior Court of San Bernardino County*, 13 Cal 3d 238, 188 Cal 3d 238, 118 Cal Rptr 166, 529 P2d 590, the Court found that a customer has a reasonable expectation of confidentiality in bank papers that he provides to the bank and in bank statements of his account irrespective of the ownership of the documents themselves. Compare also *Pigg* v. *Robertson* (1977), Mo App 549 SW2d 597. Another example may be found in *Taylor* v. *Commercial Bank*, 174 NY 181, 66 NE 726, in which the Court provided the principle that a bank teller is not required to opine to a third party about a customer's record.

[43] *Jubbal* v. *Royal Bank of Canada* [1987] B.C.J. No. 1715 [hereinafter *Jubbal*]. In this case the Court accepted the validity of *Tournier supra* note 4 and ordered a new trial on, among other things, the matter of an implied duty of confidentiality. That trial was not reported.

[44] One early case that gave context to the exception was *Glover* v. *Glover* 29 O.R. (2d) 401, 113 D.L.R. (3d) 174 (O.C.A.) – a case that dealt not with bank records but with phone company records. In this case the dissenting judge argued that there is an overriding public interest in the enforcement of custody orders affecting the wellbeing of children.

[45] *Canada Deposit Insurance Corp.* v. *Canadian Commercial Bank* (1989), 95 A.R. 24, 64 Alta L.R. (2d) 329, 71 C.B.R. 239 [hereinafter *CDIC*].

opinion of the customer.[46]

In *Canada Deposit Insurance Corp.* v. *Canadian Commercial Bank*[47] the CDIC requested that the Court make an order directing the liquidator of the Canadian Commercial Bank to produce documents pursuant to the *Winding-Up Act*,[48] and argued that there was an overriding duty to the public to disclose the documents.[49] Although the Court provided limited reasons, it held that "there is an overriding public interest...that requires disclosure on a broader basis than would be obtainable by way of discovery of documents in the possession of a third party."[50] The *CDIC* decision is subject to at least two criticisms: (i) it fails to delineate the threshold at which a public interest gains sufficient import to override the duty of confidentiality; and, perhaps as a result of this, (ii) it treats *Tournier* as a potential vehicle for compelling the disclosure of confidential records beyond those circumstances where required by law.

The protection of the public interest was considered by the Court in *CIBC* v. *Sayani*[51] and was found to include the disclosure of confidential information for the purposes of *preventing* fraud. This is different from the disclosure of information that is required for the prosecution of an individual that has committed fraud already. In *CIBC*, a trust company was considering extending credit to a developer but was unaware that the developer had defaulted on a loan. The bank disclosed this information to the trust company and was sued by the developers for breach of confidence. The Court stated: "it seems to me inconceivable that an honest banker would ever be willing to do business on terms obliging the bank to remain silent in order to facilitate its customer in deceiving a third party."[52]

However, since the Court did not find that fraud had been committed in this case it lowered the threshold of the exception to include misrepresentations "whether or not it constitutes fraud or deceit in law."[53] Although the Court was reluctant to further define the requisite 'level' of misrepresentation it would appear from the judgment that the protection of the public interest may allow the disclosure of confidential information in order to prevent a third party from relying on a *materially misleading statement.* One danger in this holding is that a bank may adopt too great a discretion in its protection of third party interests, where those interests would already be protected by that third party's contract and tort remedies. A second danger is that a bank may take advantage of an innocent misrepresentation in order to justify its disclosure of information.

---

[46] In *Murano* v. *Bank of Montreal* (1995) 31 C.B.R. (3d) 20 B.L.R. (2d) 61, [hereinafter *Murano*] the Court rejected the argument that the disclosure by a bank to a customer's business associates, suppliers and other lenders that the customer was "dishonest" was justified by a duty to the public.

[47] *CDIC supra* note 45.

[48] *Winding-Up Act*, R.S.C. 1985, c W-11 Section 123(1) states: "after a winding-up order has been made, the court may make such order for the inspection...of its books and papers, as the court thinks just".

[49] The Court in *CDIC supra* note 45 at 8 notes that the *Evidence Act* could not be applied to the instant case because the documents were the property of the Winding-Up court.

[50] *Ibid.* at 17.

[51] *Canadian Imperial Bank of Commerce* v. *Sayani* (1993), [1994] 2 W.W.R. 260, 11 B.L.R. (2d) 28, (B.C.C.A.) [hereinafter *Sayani*].

[52] *Ibid.* at 266.

[53] *Ibid.* at 267.

b) *United Kingdom*

In the United Kingdom, "public interest" has been defined broadly. In *Price Waterhouse* v. *B.C.C.I. Holding (Luxembourg)*[54] the Court held that, where a bank's records are required for a public enquiry, there exists an overriding public interest in their disclosure for the effective regulation of banks and the protection of customers. In this case, B.C.C.I. was found to owe its customers a duty of confidentiality. It had, in confidence, relayed that information to Price Waterhouse, who was then likewise bound by the duty of confidentiality. When Price Waterhouse was requested to provide this information to an enquiry, it made application to the Court for a declaration. The Court determined that while there was an interest in maintaining the information's confidentiality, there was a competing and overriding public interest in its disclosure, and more specifically, the need for the effective regulation of banks and the protection of customers.

c) *Australia*

In Australia, the "public interest" criterion has been defined more narrowly. In a general dialogue on the scope of *Tournier*, the Court in *Kabwand Pty. Ltd.* v. *National Australia Bank Limited*[55] indicated that an overriding public duty to the public may arise where there is a danger to the state. Two Australian academics[56] have identified the following series of factors as relevant to the determination of the constitution of public interest: 1) Whether a reasonable banker would recognize a public interest giving rise to a duty to disclose; 2) Whether a clear, real and extensive danger to the public exists; 3) Whether the sole intent of disclosure is the danger to public interest; 4) Whether the bank considered carefully if its action is constructive? 5) Whether the bank considered alternate action? and, 6) Whether the bank weighed the effects of disclosure on the customer against the effects of retention on the public interest? When removed from a fact scenario these considerations appear to make sense; however, they would be difficult to implement in Canada. The suggestion that a tort-like reasonableness standard be employed and a balance of effects be considered would tend to place an inappropriate burden on bankers and would attribute an unrealistic level of social judgment to banks.

3. *Where the Interests of the Bank Require Disclosure*

The classic example used to illustrate when a bank's interests can override the duty of confidentiality is the case in which the bank discloses the existence and quantum of a customer's overdraft in order to collect repayment.[57] However, a few typical bank interests have emerged in the common law.

---

[54] [1992] B.C.L.C. 583 (Ch.) [hereinafter *Price Waterhouse*].

[55] *Supra*, note 32.

[56] Walter and Erlich, "Confidences-Bankers and Customers: Powers of banks to maintain secrecy and confidentiality-Attorney General's Information Service" (June 1989) 63(6) Australian Law Journal 404.

[57] Compare *Jubbal supra* note 43.

a) *Canada*

This exception to the duty of confidentiality is, according to the Court in *Park* v. *Bank of Montreal*, one "that should be construed narrowly".[58] Generally speaking, there is no overriding bank interest in disclosing to others the fact of the bank's contractual claim against its customers.[59] Likewise, a bank does not have an overriding interest in communicating its opinion to others that a customer is dishonest. [60] However, where a bank has a security interest in a customer's property, it may protect that interest by advising others that it the security interest exists.[61]

The extent of information that can be communicated under this exception was broadened by the British Columbia Supreme Court in *Sayani* which noted that to reveal the existence of the potential litigation with respect to a disputed loan arrangement is "no more serious than to reveal the state of a customer's account by returning a cheque marked 'NSF'".[62] However, it would appear that the Supreme Court erred in *Sayani* when it suggested that this information could be disclosed in order to protect the interests of the plaintiff bank and the interests of the bank to which the information was communicated.[63] Arguably, neither *Tournier* nor any subsequent decision supports the proposition that the duty to protect the interests of the bank extends to the protection of any other financial institution. Nevertheless, *Sayani* does beg the question of whether or not a bank would be allowed to disclose the confidential records of its customers in order to protect the interests of one of its affiliates, for example, a bank-owned trust company or securities division.

The matter is made simpler when a bank discloses information in an attempt to protect its security interests. This issue was addressed in *Brattberg*.[64] The Court stated

---

[58] *Supra* note 18 at para. 112.

[59] In *Canadian Imperial Bank of Commerce* v. *Sayani* (1991) B.C.J. No. 3042 (B.C.S.C.) (QL). the British Columbia Supreme Court held that a bank that informed a potential lender of a possible claim the bank had against a customer was protecting its own interest in preventing the customer from incurring further debt. However, on appeal, (1993) 83 B.C.L.R. (2d) 167, [1994] 2 W.W.R. 260, 33 B.C.A.C. 85, 54 W.A.C. 85, 11 B.L.R. (2d) 28, B.C.W.C.D. 2430, the Court found that the bank was not protecting its own interests but was instead protecting an interested party against misrepresentations by the customer.

[60] In *Murano supra* note 46, the Court found that where a bank has put a customer into receivership it is not protecting its interests by subsequently opining to other institutions and business contacts of the customer that the customer was dishonest.

[61] In *Royal Bank of Canada* v. *Brattberg* [1993] 8 W.W.R. 139 (Alta. Q.B.), 11 Alta. L.R. (3d) 190 [hereinafter *Brattberg*] the Court found that a bank may disclose the matter of a security interest it holds in its customer's property in order to protect that interest.

[62] *Sayani, supra* note 59 at 38. Note that on appeal the BCCA, *supra* note 51 used different reasons but did not state that the BCSC's comments on the duty to protect the bank's interests were incorrect. The BCCA stated at 269: "The scope of that exception must, of course, be a limited one, for if a bank could make disclosure of its customers' confidential information whenever this served its interests, the duty of confidentiality would have little meaning, but I need not deal with this."

[63] *Ibid.*

[64] *Brattberg supra* note 61. As this case was decided on the basis that the plaintiff could not satisfy the requisite proof of damages, the comments on *Tournier* are, necessarily, *obiter dicta.* Compare also *Polar Heating Ltd.* v. *Banque Nationale de Paris (Canada)* (1991) 7 C.B.R. (3d) (Alta Q.B.).

that a bank is "entitled to protect the ownership in the [property] which vested in the bank".[65] While this would seem to be the end of the matter, a later decision of the British Columbia Supreme Court addressed a similar matter using the consent exception in *Tournier*. The Court's position in *Royal Bank of Canada* v. *Vincenzi*[66] was that the grantor, in granting a secured interest, *"impliedly* authorizes the grantee to inform those persons who have some involvement in the assets so secured of the grantee's interest."[67] Accordingly, where such consent can be implied a bank may not have to prove subsequently that the disclosure was justified by being in the bank's interests. However, the Court did make a faulty distinction when it stated that such implied consent constitutes an inference that the information "was not confidential".[68] On the contrary, the effect of consent is to allow a limited use of confidential information, not to make that confidential information non-confidential.

It should also be noted that courts have been reluctant to allow banks to disclose more than the minimum amount of customer information required to protect their own interests. For example, in *Murano* the bank elaborated its disclosure to more than the mere fact that it had installed a receiver, leading the Court to find that it had breached the implied term of the contract.[69]

b) *United Kingdom*

In England, the position taken in *Tournier* — that a bank may disclose certain information in the process of collecting on a non-sufficient funds cheque, has been affirmed.[70] A second (somewhat questionable) situation suggested by at least one U.K. commentator is that a bank may claim against a third party based upon information it holds on its customer where the bank's interests so require.[71]

C. *Where the Disclosure is Made with the Expressed or Implied Consent of the Customer*

1. *Expressed Duty of Confidentiality and Expressed Consent*

Nothing in the analysis of *Tournier* should be taken to suggest that the breach of an expressed term of confidentiality in a contract is not actionable.[72] While a bank may

---

[65] *Ibid.* at 153.

[66] *Royal Bank of Canada* v. *Vincenzi* [1994] B.C.W.L.D. 1221, B.C.J. No 772 (QL) [hereinafter *Vincenzi*].

[67] *Ibid.* at 17 (QL).

[68] *Ibid.*

[69] *Murano supra* note 46.

[70] In *Sunderland* v. *Barclay's Bank* (1938) *The London Times*, 25th November at 4, the Court affirmed that certain disclosures made by a bank in the process of collecting on an N.S.F. cheque would be in the interests of the bank.

[71] J M. Holden, *The Law and Practice of Banking* Vol 1, (London: Pitman, 1986) at 73.

[72] It is interesting to note that the Plaintiff in *Tournier* claimed for the breach of an implied term of the contract, yet the passbooks issued by the bank stated: "The officers of the Bank are bound to secrecy as regards the transactions of its customers", which may suggest that expressions of consent in contracts may be reinforced by an overarching implied consent created by the relationship. See Holden *supra* note 71 at 67.

disclose information that is either outside the scope of the given transaction or not collected pursuant to the contract, this power may be limited by expressed terms of confidentiality.[73] While expressed terms of confidentiality may afford customers added protection, they are not iron-clad vehicles of privacy protection. As discussed earlier, all private arrangements are subject to the general laws of the land. Accordingly, it is unlikely that a confidentiality clause would prevent a bank from disclosing information relating to its customers' fraudulent activities to the police. Furthermore, where a financial institution has included an express duty of confidentiality in the contract, it will likely include a countervailing clause giving the bank expressed consent to disclose.[74] One consumer activist, in an attempt to *expose* banks' intentions, devised a contract containing a right of action for wrongful disclosure that consumers could try to utilize upon opening an account.[75] The activist's rationale was that a bank's refusal to sign the contract would indicate its hidden agenda to disclose customers' information without consent.[76] Arguably, commercial reality would discredit any such project given that personal loans and account agreements are invariably negotiated using standard terms. It is precisely because of the fact that there exists a disparity of bargaining power in the relationship, and that banks can insist upon standard form agreements, that an implied term of confidentiality is justified.

2. *Implied Duty of Confidentiality and Implied Consent*

In some circumstances courts may conclude that not everything the parties agreed to is contained in the oral statements or written documents which appear to constitute the contract. A term that courts construe as being in the contract is said to exist in the contract.[77] The implied existence of certain contractual terms is necessary to recognize longtime banking practices:

---

[73] *Litholite Ltd.* v. *Travis and Insulators Ltd.* (1913), 30 R.P.C. 266. In this case the Court enforced the clause in a service contract that required the parties to maintain the confidentiality of contract details.

[74] An example is the Royal Bank, *Application: Royal Bank Visa Gold,* form 3114 (11-95), which states: "You may collect credit and other financially-related information about me (information) from me, from credit bureaus and from other parties. You may use information as follows:

- You may give it to credit bureaus and other parties who have or may have financial or other business dealings with me;
- You may use it to determine my financial situation;
- You may use it for any purpose related to the provision to me of services I request from you. You may also give it to anyone who works with or for you, but only as needed for the provision of those services;
- You may use it to promote your services to me. You may also add it to client lists you prepare and use for this purpose; and
- You may share it with your affiliates (where the law allows this), in the form of client lists or otherwise, so that they may promote their services to me.
- Even if I am no longer your client, you may keep information in your records and use it for the purposes noted above.

[75] I. Lawson, *Privacy and Free Enterprise* (Toronto:1991) at 297. The author describes this 1972 project of Robert Ellis Smith. The contract itself was designed to be in plain English.

[76] *Ibid.*

[77] R.E. Brown, *The Law of Contract in Canada supra* note 71 at 448.

> The contractual relationship which exists between banker and customer is a complex one founded originally upon the customs and usages of bankers. Many of those customs and usages have been recognized by the courts, and, to the extent that they have been so recognized, they must be regarded as implied terms of the contract between banker and customer. It follows, therefore, that this is a breach of the law where implied terms are of vital importance.[78]

With respect to the banking relationship, however, courts have been reluctant to suggest that a relationship of absolute confidence is created by the contract.[79] For instance, the relationship between customer and banker does not share the same absolute duty of confidentiality that characterizes the solicitor and client relationship.[80] The operation of the last exception in *Tournier* - that disclosure may be made with the expressed or implied consent of the customer - is what determines whether exceptions (a) through (c) will have to be invoked; that is, the disclosure of confidential information under compulsion of law or to protect the bank's or society's interests, is moot if the consent of the customer is first obtained.

One view holds that the customer's consent will always be implied when the bank's disclosure practices are lucid, or openly communicated to the client. The problem arises when the consent is given either no object, or so broad an object that it is open to limitless interpretation. Madeliene Plamondon of the *Service d'Aide au Consommateur* has conducted various studies in Quebec to answer the question of whether there is privacy in financial institutions. In one such study she visited various regional bank branches in order to determine if privacy was being enforced in practice and observed that banks were using blanket consent clauses that afforded them vast power to obtain or deliver customer information.[81] Studies like this suggest that if banks are permitted to leave the scope of the consent undefined or indefinable, the protections under *Tournier* can be short-circuited.

It could be argued that *Tournier* contains a hidden fifth criterion for disclosure that is closely aligned with implied consent. Scrutton L.J. stated: "I doubt whether it is sufficient excuse for disclosure, in the absence of the customer's consent, that it was in the interests of the customer, where the customer can be consulted in reasonable time

---

[78] J Milnes Holden, *The Law and Practice of Banking* Vol 1, (London: Pitman, 1974) See also *Hutton v. Warren* (1836), 1 M & W, 446, 150 E.R. 517, in which the Court states: "It has long been settled, that, in commercial transactions, extrinsic evidence of custom and usage is admissible to annex incidents to written contracts, in matters with respect to which they are silent." For an example of when the court has refused to acknowledge that a term can be implied in a contract between bank and customer. See *Canadian Pacific Hotels Ltd.* v. *Bank of Montreal*, [1997] 1 S.C.R. 711, (1987) 41 C.C.L.T. 1, 77 N.R. 161, 21 O.A.C.321.

[79] Parliament of New South Wales, *Report on the Law of Privacy* (1973). This report, also known as the Morison Report, states that the court must only imply "such terms as must necessarily have been in the minds of the parties when making the contract or they must necessarily have been prepared to agree upon had they directed their minds to the matter."

[80] Compare Canadian Bar Association, *Code of Professional Conduct (1987)* Rule 4. The code states that "the lawyer owes a duty of secrecy to every client without exception, regardless of whether it be a continuing or casual client. The duty survives the professional relationship and continues indefinitely after the lawyer has ceased to act for the client, whether or not differences have arisen between them."

[81] Currently there is no English translation of these studies. The above was based upon the author's interview with Ms. Plamondon on October 28, 1996.

and his consent or dissent obtained."[82] The syllogistic corollary of this is that, when the disclosure is clearly in the interest of the customer, and the customer cannot be consulted within a reasonable time, consent may not be required for disclosure. While it remains to be seen whether or not this exception will find a place in the *Tournier* rule, it is unlikely that it will often be the subject of litigation.

a) *Canada*

Interestingly, one of the earlier Canadian considerations of *Tournier* adds to our understanding of when consent cannot be implied. In *Hull v. Child's and Huron and Erie Mortgage Corporation*[83] the Court found that a signed but incomplete cheque presented to the bank by a customer's relative would not in itself imply the customer's consent that the balance of the account could be communicated to the relative.[84]

However, courts have held that certain relationships between two customers may imply that one has consented to the bank disclosing his personal information to the other.[85] Courts have also found that, in giving a bank a security interest in property, a customer consents to the bank communicating the fact of that security to other interested parties.[86]

b) *United States*

A similar doctrine exists in American law. According to *Graney Development Corp.* v. *Taksen*,[87] where a bank's customer defaults on a loan obligation, the bank will be permitted to communicate that fact to certain parties. This doctrine amounts to a statement that the customer impliedly consents to certain disclosures by the bank on default.

---

[82] *Tournier* at 481.

[83] *Hull* v. *Child's and Huron and Erie Mortgage Corporation* [1951] O.W.N. 116 (Ont. H. C.)

[84] This case deals with the niece and nephew of a hospitalized customer who had given them blank cheques to cover his funeral expenses if he died. The two individuals took the cheques to the bank, were advised of the balance of the account, and closed the account with the instruments pre-mortem. The court held that when a person other than the customer presents the customer's blank signed cheque to the bank, that does not indicate that the customer consented to the disclosure of their account balance.

[85] In what appears to be a stretch of the exception, the court in *Art's Welding, supra* note 16, was prepared to find that where a customer knew that another party's livelihood relied on their contractual relations, this implied the customer's consent for the bank to disclose his record to the other party. In *Hong Kong Bank of Canada* v. *Phillips* [1997] M.J. No.134 (MAN. Q.B.) (QL), the court found that where a customer brings in new clients to a bank to which he is in arrears so that those clients may borrow money to invest in his schemes, he impliedly consents to the bank disclosing the information he has given it with respect to those schemes.

[86] In *Vincenzi supra* note 66, the Court found that where a bank has a secured interest in the customer's property, it is implied in that contract that the customer consents to the bank's disclosure of that security to others who have involvement in that interest.

[87] *Supra* note 37.

c) *United Kingdom*

Other initiatives have supplemented the common law rule in England. The Report of the Committee on Privacy, or the Younger Committee,[88] addressed some of the lacunae in the common law rule, including the matter of implied consent. The committee's position was that banks have a responsibility to make clear to present and prospective customers their practices of referring, and that consent can be implied only when the customer is aware of, and understands, these practices.[89]

D. *Duty to Protect Against Fraud*

1. *Canada*

According to Atkin L.J., a bank has an overriding duty to protect itself, the public or another interested party against fraud or crime. The British Columbia Court of Appeal in *Canadian Imperial Bank of Commerce* v. *Sayani*[90] found that a bank not only has the duty to disclose information to prosecute fraud, but also to prevent fraud. It held further that this exception might be expanded to include the prevention of misrepresentations, whether or not they constitute fraud or deceit.

2. *United States*

Something similar to this duty may exist in American common law. In *Richfield Bank & Trust Co.* v. *Sjogren*[91] the Court found that the bank has a duty to disclose to potential borrowers knowledge that it has regarding the fraudulent nature of another customer's venture if the potential borrower is borrowing to invest in that venture.

E. *Duty to Disclose in the Interest of Justice*

In an unusually cavalier decision on the disclosure of the bank records of a nonparty, Master Breitkreuz stated that where consent could not be implied, and where there was no clear compulsion under law, he "would be prepared to add a further category, namely, where the interests of justice require disclosure".[92] There can be no doubt that this exception has not been added to Canadian law.

F. *Duty to Warn the Customer of Disclosure*

1. *Canada*

There has been some discussion in Canadian courts concerning whether a bank that discloses customer information under compulsion of law has a corresponding duty to

---

88 Cmnd. 5012 (1972).
89 Holden *supra* note 71 at 76.
90 *Supra* note 21.
91 (Minn) 2424 NW2d 648.
92 *Art's Welding supra* note 16.

warn the customer first that it is going to disclose the information.[93] The present position in Canada appears to be that where the compulsion is with respect to a non-criminal matter there is ordinarily a duty on the bank to use its best efforts to warn the customer of the disclosure.[94] However, where the disclosure is with respect to an alleged criminal activity, there is no implied term that the bank should first warn the customer.[95]

2. *United Kingdom*

The English courts have taken the position that where a bank is compelled by law to disclose confidential information in a criminal matter, there is no duty to inform the customer of that disclosure. In *Barclay's Bank P.L.C.* v. *Taylor*, the police served notice on Barclay's Bank that they would be applying to the court for an order allowing them to inspect the account of a customer. The customer argued that his agreement with the bank contained an implied obligation to warn him of such an application. Lord Donaldson M.R. stated:

> There is no doubt that the banks were free to ignore the request not to inform Mr. and Mrs. Taylor of the application. However, I should have been surprised and disappointed if they had done so in the context of a criminal investigation unless they were under a legal duty to do so. There is a public interest in assisting the police in the investigation of crime and I can think of no basis for an implied obligation to act in a way which, in some circumstances, would without doubt hinder such inquiries.[96]

Furthermore, the Court has held that this duty to warn is subject to whether or not the bank is able to make contact with the customer.[97] In *Robertson* v. *Canadian Imperial Bank of Commerce*, the Court considered the actions of Mr. Dennie who, in

---

[93] This duty was first suggested in *Budzisch supra* note 17, in which the Court, considering the British *Robertson* decision, infra, suggested that a bank may have a duty to warn a customer when it has been compelled by Revenue Canada to disclose the customer's information. In the instant case the plaintiff's records had been supplied to Revenue Canada pursuant to Section 231.2(a) and (b) of the *Income Tax Act* R.S.C. 1985 c. 1. Section 231.2(a) provides, in part that "...the Minister may...for any purpose related to the administration or enforcement of this Act...require that a person provide...any information or additional information, including a return of income to a supplementary return". It should be noted that this provision is not necessarily one that satisfies 'compulsion under law'. In the instant case the plaintiff conceded this point.

[94] The matter was alluded to in *Foundation Co. of Canada Ltd.* v. *Dhillon* [1995] O.J. 3211, Oct 26, 1995 (Quicklaw) (O.C.J. Gen. Div.), when the Court stated that, while it would normally be proper for a bank to notify its customer that it had received a Mareva Injunction, where there was a *prima facie* case that the customer had breached a trust, committed fraud, and accepted secret commissions, no such duty existed.

[95] The present position is defined most clearly in *Park supra* note 18. The Court found that the duty to warn is defined by the nature of the compulsion under law that the bank faces. Where the compulsion is with respect to a non-criminal matter, there is ordinarily a duty on the bank to use its best efforts to warn the customer of the disclosure. However, where the disclosure is with respect to an alleged criminal activity, there is no implied term that the bank should first warn the customer.

[96] *Barclay's Bank P.L.C.* v. *Taylor* [1989] 3 All E.R. 563 (C.A.). The Court found that a bank should refrain from informing the customer of the disclosure where it is with regard to a criminal investigation, as there is an overriding public interest in assisting the police.

[97] *Robertson supra* note 27.

order to support his action for repayment of a debt, obtained a *subpoena duces tecum* against the bank at which the debtor was a customer. The subpoena ordered the bank to attend at trial, to give evidence on behalf of the plaintiff, and to produce the bank statements of the debtor. At trial, the bank manager produced a ledger sheet which indicated not only the transaction in issue, but also evidence of the transactions before and after. Among the irrelevant material revealed was the fact that the debtor's account was at one time overdrawn. The Court made the following findings:

- where a bank acts under compulsion of law to disclose, there is a duty on the part of the bank to inform its client of the application unless to do so would prejudice the proceedings being investigated;
- in the instant case, the bank was under no compulsion to withhold knowledge of the subpoena from the appellant;
- it cannot be expressed as an absolute duty to inform the customer of the subpoena, if only because, the bank may be unable to make contact with the customer in the time available ... the obligation imposed upon the bank in the circumstances of the present case could have been no more than to use its best endeavours to inform the appellant of the receipt of the subpoena; and
- moreover, there may be difficulties in specifying the circumstances in which, by implied agreement, the bank is to be regarded as entitled in its own protection or compelled by public duty, to refrain from informing the customer.

In effect, the duty amounts to a best efforts endeavour to warn the customer in circumstances in which a criminal investigation will not be prejudiced.

3. *United States*

In *Valley Bank* v. *Superior Court*[98] the Court held that banks have a duty to provide their customers with fair opportunity to object to the disclosure of their personal information – the reasoning being that the warning given to the customer may afford it the opportunity to commence a legal proceeding to restrict the scope of the disclosure. However, in other decisions the courts have held that neither the bank nor the police are required to inform the customer that its bank records are being investigated in a criminal matter.[99]

G. *Equity Follows the Common Law*

Like the implied term of confidentiality, the equitable duty of confidence and fiduciary duties arise from the instant relationship and the instant parties. This is unlike tort duties which arise from a person's duty to the world generally.[100] Accordingly, it would seem that, while a contractual claim need not exist in order for

---

[98] 542 P 2d, 1977 (Cal. 1975).

[99] In *People* v. *Muchmore* (1979) 92 Cal App 3d 32, 154 Cal Rptr 488 it was held that the police and the bank were not obligated to notify a bank customer that the bank has been asked to disclose his personal information in connection with a criminal investigation. This case may be reconciled with *Valley Bank supra* note 98, because the scope of the disclosure in this case was restricted by statute and the customer would not have been able to restrict it further.

[100] R. Brait, "The Unauthorized Use of Confidential Information" (1991) 18 *Can. Bus. L.J.* 323.

either of these duties to be triggered, it certainly may supplement them. The following provides a very brief window into two other claims that may exist alongside the contract.

III. FIDUCIARIES[101]

Courts have determined that when a customer releases the bank from an obligation under *Tournier* (through consent) there is no corresponding discharge from any other duties which flow from the fiduciary relationship between the bank and its customer.[102] Accordingly, even where a bank has received the customer's consent to disclose, the bank may still be bound to deal with that information as would a person entrusted with its custody (the word fiduciary is rooted in the Latin *Fiducia,* meaning trust).[103] In the absence of special circumstances the debtor/creditor relationship between a banker and a customer does not give rise to a fiduciary duty. The *locus classicus* for when this duty arises is *Lloyd's Bank Limited* v. *Bundy*.[104]

> The first and most troublesome issue which here falls for consideration is as to whether on the particular and somewhat unusual facts of the case, the bank was...in a relationship...that entails the duty on their part of what can for convenience be called fiduciary care ...
> ... such cases arise where someone relies on the guidance or advice of another, where the other is aware of that reluctance, and where the person upon whom reliance is placed obtains, or may well obtain, a benefit from the transaction or has some other interest in it being concluded. In addition, there must, of course, be shown to exist a vital element which in this judgment will for convenience be referred to as confidentiality.

While these criteria have been employed to impose a fiduciary relationship in Canadian cases,[105] in *Lac Minerals Ltd.* the Supreme Court of Canada has reaffirmed the criteria presented in *Frame v. Smith* for identifying the existence of a fiduciary relationship:

> •the fiduciary has scope for the exercise of some discretion or power;
> •the fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interest; and
> •the beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the

---

[101] A more detailed account of the governing fiduciaries is contained in E.P. Ellinger, "Reflections on Recent Developments Concerning the Relationship of Banker and Customer" (1988) 2:2 *Can. Bus. L. J.* 2:2 129 and B. Crawford, "Banker's Fiduciary Duties and Negligence" (1986) 12:2 *Can. Bus. L.. J.* 145.

[102] *Standard Investments Ltd.* v. *Canadian Imperial Bank of Commerce (1985)* 52 O.R. (2d) 473, 30 B.L.R. 193, 22 D.L.R. (4th) 410, 11 O.A.C. 318. Note that an application for leave to appeal from this decision was dismissed by the Supreme Court of Canada at 53 O.R. (2d) 663. Note also that *Murano v. Bank of Montreal* (1995) 31 C.B.R. (3d) 1, 20 B.L.R. (2d) 61 recognizes *Standard Investments* as first endorsing *Tournier* in Canadian law.

[103] Maddaugh, *Definition of Fiduciary Duty* in *Law Society Special Lectures*: Fiduciary Duties LSUC: 1991.

[104] [1975] Q.B. 326 at 340.

[105] *Royal Bank* v. *Guertin* (1983), 43 O.R. (2d) 363, 23 B.L.R. 189, 1 D.L.R. (4th) 68 (Ont. H.C.).

discretion or power.[106]

In the context of privacy issues, the law will treat those unilateral disclosures of confidential customer information that effect the customer's interest, where the customer is particularly vulnerable or is at the mercy of the bank, as being breaches of fiduciary duties.

A. *Breach of Confidence*

The doctrine of breach of confidence has multiple sources, all of which have converged into a type of action that is neither entirely contractual nor entirely tortious in nature.[107] In *Lac Minerals* the Supreme Court adopted three principles from *Coco* v. *A.N. Clark (Engineers) Ltd.*[108] which set the stage for a breach of confidence:

- the information must have the necessary quality of confidence;
- the information must have been imparted in circumstances importing an obligation of confidence; and
- there must be an unauthorized use of that information to the detriment of the party communicating it.

Beyond recognizing these unqualified criteria for the existence of the duty, the Court did little to define when a breach of confidence arises. However, the decision is valuable for its consideration of the standard of care and the remedies that flow from a failure to meet it. The following chart may assist in understanding how the Court sat on these two issues.[109]

Unanimous	The appropriate standard is whether a reasonable person would realize that the information was being communicated in circumstances giving rise to an obligation of confidence.
La Forest Sopinka	The onus is upon the recipient of the information to refute the contention that he was bound by an obligation of confidence.
La Forest Lamer Wilson	The appropriate remedy is to recognize a constructive trust.

[106] *Lac Minerals Ltd.* v. *International Corona Resources Limited*, [1989] 2 S.C.R. 574.

[107] *Privacy and Free Enterprise supra* note 75.

[108] [1969] R.P.C. 41 (Ch. D.) 47.

[109] The author is indebted to the discussion in Privacy Commissioner of Canada, Regulating the Financial Institutions: Protecting the Privacy of Customers' Personal Information - A submission by the Privacy Commissioner of Canada to the Standing Committee on Banking, Trade and Commerce (Ottawa: Report prepared by Gowling, Strathy and Henderson, 1992). However, it would appear that this submission fails to distinguish between the tortious breach of confidence and the contractual breach of the implied term of confidentiality - a necessary distinction for any claim.

Sopinka McIntyre	The appropriate remedy is damages.

It is also of interest to note that unlike a fiduciary duty, a duty of confidence can arise in the absence of a direct relationship[110] which can make this a valuable claim in circumstances involving disclosures by financial institutions who have no contract with the complainant.[111]

IV. THE NEW PRIVACY – VOLUNTARY PRIVACY CODES

The common law addresses only some of the privacy concerns that have become important in the last decade. The protections created under common law are limited and poorly suited to controlling the use of confidential information by an altogether new form of financial institution. As banks are given latitude in their investment structures and aim to merge into financial giants, there are potential flows of information that could go unregulated. Generally speaking, the cases decided under *Tournier* are reactive - they deal with one-time communications of confidential information. However, as storehouses of bank records are coveted for marketing and other non-banking purposes, personal information becomes a commodity,[112] and the potential for disclosure *en masse* is increased. Clearly, protections arising from the common law are ill-designed for the amount of personal information collected and speed with which current technology can facilitate disclosure.

Voluntary codes of conduct are being drafted in the banking, insurance, direct marketing and other industries to which extensive customer information has value. The Canadian Standards Association developed the *Model Code for the Protection of Personal Information*; the Credit Union Association developed the *Credit Union Code for the Protection of Personal Information (1996)*; the Trust Companies Association of Canada developed the *Customer Privacy Code (1993);* the Canadian Life and Health Association Inc. developed its *Right to Privacy Guidelines No. 96;* the Insurance Bureau of Canada developed the *Model Personal Information Code (1997);* and the Canadian Bankers Association introduced the *Privacy Model Code.* These codes are being adopted and implemented in the shadow of governmental threats to regulate the flow of information and displace the industries' voluntary codes. The second portion of this paper examines the legal status of codes of conduct, the legislative proposals that may enforce them, and the academic criticisms of the commodification of information in banking.

V.WHOSE BUSINESS IS BANKING?

Many of the controversies surrounding the implementation and enforcement of

---

[110] *Supra* note 106.

[111] This is considered in *Sayani supra* note 59.

[112] Information and Privacy Commissioner Ontario, *Annual Report*, Toronto: 1993 at 23 reads: "In the 90's information has become a commodity – a tradable product that can be bought and sold. The Ontario government is seeking opportunities to sell rights to government-held data as a new source of revenue".

privacy controls are rooted in jurisdictional issues. Banks refuse to let provincial privacy commissioners through their doors to audit procedures. Extensive federal public sector legislation does not extend to federally regulated banks being limited to the information of those in the public sector. Ground-breaking Quebec legislation reaches to nearly the entire private sector, but is stopped abruptly at the front door of the federally regulated banks. There are two boundaries causing these constrictions. Firstly, the authority to regulate the privacy interests of banking fall within heading 15 of the *Constitution Act,* "Banking, Incorporation of Banks, and the Issue of Paper Money". Four federal statutes govern financial institutions in Canada: the *Bank Act*,[113] the *Insurance Companies Act*,[114] the *Trust and Loan Companies Act*[115] *and the Cooperative Credit Associations Act*[116].

Three of these acts permit the Governor in Council to make regulations concerning the use of information.[117] Each of these also requires all financial institutions to take reasonable precautions to ensure the protection and accuracy of their records and

---

[113] S.C. 1991, c. 46 as amended [hereinafter *Bank Act*].

[114] S.C. 1991, c. 47 as amended [hereinafter *Insurance Companies Act*].

[115] S.C. 1991, c. 45 as amended [hereinafter *Trust and Loan Companies Act*].

[116] S.C. 1991, c. 48 as amended [hereinafter *Cooperative Credit Associations Act*].

[117] Prior to 1991, no provision in the *Bank Act* (R.S.C. 1985, c.B.1), *Loan Companies Act* (R.S.C. 1985, c.B.1), *Trust Companies Act* (R.S.C. 1985, c.T.20), *Canadian and British Insurance Companies Act* (R.S.C. 1985, c.I.12), *Foreign Insurance Companies Act* (R.S.C. 1985, c.I.B) or *Cooperative Credit Associations Act* (R.S.C. 1985, c.C.41) empowered the Governor in Council to regulate with respect to the privacy of information. In 1991, each of these statutes was repealed and replaced with the *Bank Act* S.C. 1991 c.46, the *Insurance Companies Act supra* note 114, the *Trust and Loan Companies Act supra* note 112, and the *Cooperative Credit Associations Act supra* note 116, respectively. Each of these Acts, with the exception of the *Cooperative Credit Associations Act*, stated effectively that "The Governor in Council may make regulations governing the use by a company of any information supplied to the company by its customers." In 1997, the regulation-making authority in each of the Acts (excluding the *Cooperative Credit Associations Act*) was repealed and the Governor in Council was afforded a more specific ability to make regulations:

- requiring a [financial institution] to establish procedures regarding the collection, retention, use and disclosure of any information about its customers or any class of customers;
- requiring a [financial institution] to establish procedures for dealing with complaints made by a customer about the collection, retention, use or disclosure of information about the customer;
- respecting the disclosure by a [financial institution] of information relating to the procedures referred to in paragraphs (a) and (b);
- requiring a [financial institution] to designate officers and employees of the [financial institution] who are responsible for
  - implementing the procedures referred to in paragraph (b), and
  - receiving and dealing with complaints made by a customer of the [financial institution] about the collection, retention, use or disclosure of information about the customer;
- requiring a [financial institution] to report information relating to complaints made by customers of the [financial institution] about the collection, retention, use or disclosure of information, and the actions taken by the [financial institution] to deal with the complaints; and
- defining "information", "collection" and "retention" for the purposes of paragraphs (a) to (e) and the regulations made under those paragraphs.

registers,[118] and all financial institution directors to establish procedures restricting the use of confidential information.[119] In some cases, regulations made pursuant to these acts restrict a financial institution's ability to share information.[120]

What is less clear is who has jurisdiction over federally incorporated trust and insurance companies, and provincially incorporated trust and insurance companies.[121]

---

[118] Prior to 1991, section 157(3) of the *Bank Act* provided that a bank and its agents should take reasonable precautions to: (a) prevent loss or destruction of, (b) prevent falsification of entries in, and, (c) facilitate detection and correction of inaccuracies in the registers and records required or authorized by this Act to be prepared and maintained. In 1991, this section was amended to include sub-paragraph (d), which provides that reasonable precautions shall be taken to "ensure that unauthorized persons do not have access to or use of information" in the required registers and records. Identical provisions to the amended s.157(3) were also included, for the first time, in the newly enacted *Insurance Companies Act, Trust and Loan Companies Act* and *Cooperative Credit Associations Act.* This provision remains in force in each of the Acts.

[119] Prior to 1991, there were no provisions in any of the acts specifically requiring the directors to develop internal policies with respect to the use of confidential information. Since 1991 each of the acts stipulates that the directors of a financial institution shall establish procedures to resolve conflicts of interest, including techniques for the identification of potential conflict situations and for restricting the use of confidential information (compare S.C. 1991, c.46 x.157(2)(c)).

[120] The 1992 *Insurance Business (Banks) Regulations* made pursuant to the *Bank Act supra* note 113 prohibit a bank or its subsidiaries from providing any insurance company, agent or broker with information respecting a customer or employee of the bank or the subsidiary. Also, the *Credit Information (Insurance Companies) Regulations*, made pursuant to the *Insurance Companies Act*, prohibit a company from using credit information obtained from customers in the promotion of an insurance company, agent, broker or policy unless certain conditions are met. The regulations also prohibit a company or its subsidiary from directly or indirectly providing an insurance company, insurance agent or broker with any consumer credit information.

[121] Some financial institutions are governed by provincial statutes which provide for the protection of information privacy. The Ontario *Credit Union and Caisses Populaires Act* (S.O. 1994, c.11, s.143) requires that the directors, officers, committee members and employees of a credit union keep confidential any information received by the credit union or any information respecting members' transactions with the credit union. In British Columbia, the *Financial Institutions Act* (R.S.B.C. 1996, c.141, s. 95 and 218) requires that certain financial institutions not communicate information about a customer except where necessary to perform the transaction. The *British Columbia Insurance Licensing Regulation* states that any insurance agent who receives customer information shall not communicate the information except where necessary to perform his or her duty. The *Cooperative Association Act* (R.S.B.C. 1996, c.71, s.47) requires that all cooperatives keep confidential financial information pertaining to members. In Alberta, regulations may be made under the *Credit Union Act* (S.A. 1989, c.31.1, s.226) with respect to the confidentiality of information the credit unions possess. The *Financial Consumers Act* (S.A. 1990, c.F.9.5, s.18) also imposes restrictions on a supplier, agent or financial planner with respect to their use of personal finance information provided by a consumer. The Saskatchewan *Credit Union Act* (S.S. 1984-85-86, c. 45.1, s.27) stipulates that registers of members of a credit union are to be kept confidential and cannot be released without the authorization of the board. Similarly, in New Brunswick and Newfoundland, the *Credit Unions Act* (S.N.B. 1992, c.C.32.2, s.28; S.N. 1997, c.C.37.1, s.28) imposes a duty on a credit union to take reasonable precautions to ensure the protection and accuracy of records. The Newfoundland *Co-operative Societies Act* (R.S.N. 1990, c.C-35, s.24) requires that all member institutions keep information confidential unless the member otherwise consents to the information's release. With respect to consumer information obtained from third parties, most provinces have enacted some form of *Consumer Reporting Act* (British Columbia *Credit Reporting Act*, R.S.B.C. 1996, c. 81; Manitoba *Personal*

As the ownership structures among financial institutions become more complex, current jurisdictional distinctions will only become more evasive.

Secondly, there is a distinction between the public and the private sector. As technology flows are facilitated and technology encourages long distance commercial relationships, it will become increasingly difficult to distinguish if one is doing business with the public sector. Accordingly, regulatory efforts have to accommodate for the further erosion of the public/private distinction by encouraging a uniform position on privacy standards.

A. *The Organization for Economic Cooperation and Development*

The OECD conducted studies between 1978 and 1980[122] that resulted in the development of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*[123] When Canada adhered to these guidelines in 1984 it set the standard for domestic privacy initiatives in both the public and private sectors.[124] With the exception of Quebec, only Canada's public sector has been governed directly by privacy

---

Investigations Act, R.S.M. 1987, C.P.34 as amended; Newfoundland *Consumer Reporting Agencies Act*, R.S.N. 1990, c.C.-32, as amended; Nova Scotia *Consumer Reporting Act*, R.S.N.S. 1989, c.C.93; Ontario *Consumer Reporting Act*, R.S.O. 1990, c.C-33 as amended; Prince Edward Island *Consumer Reporting Act*, R.S.P.E.I.1988, c.C-20 as amended; Saskatchewan *Credit Reporting Agencies Act*, R.S.S. 1978, c.C-44, as amended. (Alberta, Quebec and New Brunswick do not have legislation governing consumer credit reporting agencies.). While these statutes specifically govern the business of consumer credit reporting agencies, they also contain several provisions to which financial institutions must adhere. The release of information is granted generally upon written consent of the consumer (R.S.P.E.I. 1988, c.C-20, s.10; R.S.O. 1990, c.C.-33, s.8; R.S.B.C. 1996, c.81, s.12; R.S.M. 1987, c.P34, s.3; R.S.N. 1990, c.C.-32, s.19; R.S.N.S. 1989, c.C.93, s.11) or upon notice to the consumer. (R.S.P.E.I. 1988, c. C-20, s. 10. R.S.O. 1990, c. C-33, s. 10, R.S.B.C. 1996, c.81, s. 12; R.S.M. 1987, c. P.34, s. 3; R.S.N. 1990, c. C-32, s. 23; R.S.N.S. 1989, c. C.93, s. 11). In some provinces, financial institutions must also inform a consumer, at the consumer's request, whether a consumer report has been referred to in connection with a transaction and, if so, must provide the consumer with the name and address of the consumer reporting agency supplying the report. (Sask s.21, R.S.O. 1990, c. C-33, s. 10; R.S.P.E.I. 1988, c. C-20, s. 10. R.S.N. 1990, c. C-32, s. 22). Some statutes also stipulate that when a benefit is refused on the basis of a consumer credit report, the consumer is entitled to know the name and address of the agency and the source of information on which the negative decision was based. (R.S.B.C. 1996, c.81, s. 13; R.S.M. 1987, c. P.34, s. 6; R.S.N.S. 1989, c. C.93, s. 11; R.S.O. 1990, c. C-33, s. 10; R.S.P.E.I. 1988, c. C-20, s. 10). In Ontario, a financial institution extending credit to a consumer cannot supply a list of names and criteria to a credit reporting agency in order for the agency to determine which names meet the criteria without first notifying the consumer in writing of its intention to do so (R.S.O. 1990, c. C-33, s. 11).

[122] B. Cleaver, *Handbook Exploring the Legal Context for Information Policy In Canada* (Toronto: Faxon, 1992).

[123] Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data, September 23, 1980 [hereinafter OECD guidelines].

[124] The OECD guidelines make no distinction between privacy of information in the public and private sectors.

legislation thus far.[125] But the effect of these guidelines has been felt in the private sector. Not only have individual corporations adopted the guidelines by reference in their annual reports and codes of conduct,[126] but industry initiatives have used the OECD guidelines as the threshold of acceptable privacy standards.[127] The adoption of these guidelines has not been entirely voluntary. The European Community has developed a Directive which could preclude Canadian firms from trading with the E.C. if these guidelines are not complied with.[128] The OECD guidelines set out 8 principles of national application.[129]

> 1) Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> 2) Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> 3) Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than the time of data collection and the subsequent use limited to the fulfillment of those purposes and as are specified on each occasion of change of purpose.
>
> 4) Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph [3] except:
> (a) with the consent of the data subject; or
> (b) by the authority of law.
>
> 5) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction use, modification or disclosure of data.
>
> 6) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of

---

[125] In Ontario, the public sector is regulated by the *Freedom of Information and Protection of Privacy Act.* 1987 R.S.O. 1990, c. F-31, and the *Municipal Freedom of Information and Protection of Privacy Act,* 1989, S.O, c.63. At the Federal level look to the *Privacy Act* R.S.C. 1985, c. p-21 and the *Access to Information Act* R.S.C. 1985, c. A-1

[126] Royal Bank, *Royal Bank of Canada Privacy Code* (undated) which states: "The model privacy codes support the government of Canada's adherence to the OECD's guidelines..." and Toronto Dominion Bank, *The TD Commitment: Protecting Your Privacy*, document 13818 (5/93) which states "this code...is consistent with privacy guidelines developed by the OECD - which represents Canada's major trading partners".

[127] OECD Guidelines *supra* note 123 at 'Scope of Guidelines'. The guidelines state that they "should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties."

[128] This non-tariff trade restriction has hung over the heads of Canadian business since the first draft proposal of the Directive was released on July 17, 1990. See Cleaver *supra* note 79 at 19.

[129] OECD Guidelines, *supra* note 123 at 'Part Two: Basic Principles of National Application'.

establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) Individual Participation Principle: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8) Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

In light of the earlier discussion of *Tournier*, it is interesting to note that there is no exception for public interest disclosure nor for disclosure for the interests of the institution under the Use Limitation Principle (4 above), which would suggest that even the minimum standards of legislation would have to exceed the protections of contract law. In theory, some banks have already subscribed to this higher standard by documenting their adoption of the OECD guidelines.[130] In practice, the adoption, by reference, of an international document in a corporation's privacy code provides no tangible remedy to a domestic customer. Accordingly, national standards (under the Canadian Standards Association) and industry standards (under the Canadian Bankers Association) have been built from the base of the OECD guidelines in order encourage compliance at more local levels.

B. *Canadian Standards Association*[131]

The Canadian Standards Association released its *"Model Code for the Protection of Personal Information"*[132] in March 1996, four years after the first members of government, business, consumer groups and academia agreed to collaborate in the project. The release itself was somewhat controversial as the Canadian Bankers Association had chosen to release its (arguably more comprehensive) privacy code on the same day. Some participants would later see the failure of the two organizations to release their codes together as a missed opportunity - a missed chance to present a comprehensive national standard with a ready-made industry example.[133] The release of the model codes were also tainted by the comments of the Canadian Direct Marketing Association that certainty of privacy could only be realized through legislation and not

---

[130] See note 123 *supra.*

[131] Much of the discourse in this section has been possible due to interviews held with members of the CSA's Technical Committee on Privacy, and the Ministry of Finance, Industry Canada.

[132] Canadian Standards Association, *Model Code for the Protection of Personal Information*, Etobicoke: CSA, March 1996. Document Can/CSA - Q830-96 [hereinafter CSA *Model Code*].

[133] There are arguments on both sides of this debate. Reportedly, the CBA requested that it be allowed to release its code with the CSA code but was refused. Others have attributed the CSA's refusal to its desire to remain a degree removed so as not to be perceived as being *'in bed with the banks'*.

through voluntary regulations.[134] What is certain is that the CSA code is conservative, or as one author would later say, "little more than a Canadian-made version of the OECD guidelines".[135]

1. *What Does This* Model Code *Do?*

Now that the code has been in existence for over two years one can evaluate its effect on privacy, and compare it to those protections that existed under the OECD guidelines. Despite being called a 'code' it should not be mistaken for a practice document. The CSA has not imposed an example that it itself would comply with necessarily; rather, the model code is a standard or example on which CSA member corporations and organizations can base their privacy codes. [136] According to Colin Bennett, this is one distinction that allows this code to be "integrated into the certification and registration systems implemented through national and international standards bodies".[137] This distinction may be somewhat artificial. Given that any two codes or documents can be compared by an auditor or registrar to determine if they set equal or dissimilar standards. It is more likely that the CSA's code has received its privacy 'yardstick' status because it was so eagerly promoted by industry and government alike long before its release. To have accepted it as anything less than a *national standard* would have been embarrassing to all involved.

Another view of the CSA Model Code is that it is the product of a long process of whittling-down.[138] The long history of debate between banks, consumer advocates and government (to name only three) in the formation of the code meant that unanimity could only be achieved at the lowest common denominator—a level of privacy protection hardly much above the minimum. This being the standard, subsequent industry compliance could hardly be difficult or afford great protection to consumers.[139] By its release date, what may at one time have been a document championing consumer privacy, ended up being a reiteration of the 1980 international status quo.

---

[134] Compare Heading VI - A: "Direct Marketing Association.

[135] C. Bennett, Privacy Standards: An Innovation in National and International Policy in *Privacy Laws & Business Newsletter*, September 1996, 8 [hereinafter *Privacy Standards*].

[136] The CSA is well known for creating industry standards, but of the quantifiable sort. This project, unlike others that the CSA had undertaken, could not be prepared according to measures and mathematics. Instead it involved intangibles and ethics. Accordingly, one might wonder if the CSA was the most qualified organization to undertake this project. The mere fact that a standard was called for should not have meant necessarily that a standards organization was required.

[137] Bennett, *Privacy Standards supra* note 135 at 8.

[138] One participant in the negotiations commented that the representatives of the banking industry were seeking carve outs in the code that would allow them to "downstream" their data banks (include their banking family - affiliates and subsidiaries). One of the bankers' goals is the use of a negative option (an opt-out provision) as opposed to an opt-in for coverage.

[139] Bennett, in *Privacy Standards supra* note 135 at 8, points out that the Model Code was agreed to without dissent in September 1995. The conciliatory manner in which it was created was democratic but subject to the "too many chiefs" rule which leads ultimately to its being an emasculated and compromised standard. As a standard it is offensive to no one because it imposes nothing more on its objects than the international norm.

2. *What Can We Expect of the CSA* Code?

If one accepts that the CSA code is the Canadian privacy standard, then notwithstanding the possibility of overriding legislation in the remaining years of this millennium, the aim of industries should be to establish local privacy codes and apply to the CSA's registrar, the Quality Management Institute (QMI) for an audit and recognition of the local code. The effect of a successful application is that the industry will have a CSA approved privacy code. If, as has been suggested, the effect would be to make the CSA code *'non-voluntary'*, then perhaps the CSA code would gain currency.[140] However, it would appear that beyond some short-lived bad publicity and the possible loss of CSA membership, non-compliant members would face no legal or commercial sanctions. The code remains voluntary because the price of noncompliance for adherents is nominal. The CSA has also prepared a workbook to assist members in implementing their privacy codes.[141]

3. *The Three Tier System*[142]

If the CSA code is ever to gain even some 'soft-law' or 'customary law' status, its registration process must be publicized, accessible and expedient. Arguably, QMI fails on all counts. If one of the aims of the organization is to "make the Canadian public aware of how personal information should be protected",[143] then the process of code recognition itself should be made public. As a matter of policy QMI will not disclose which, if any, of its members have applied, or are applying, for recognition.[144]

The accessibility of the recognition program is also questionable. There is a conspicuous absence of CSA approval of the CBA Model Code, especially since the bankers' code was the first such complying code in the market.[145] Representatives from the CBA assert that they have been refused access to the QMI process on the grounds that their code faces implementation obstacles;[146] however, it would not appear that QMI's refusal is due to the insufficiency of the CBA code. The CBA published a new version of their code in November 1996 which includes an independent certification

---

[140] *Ibid.* at 9.

[141] This workbook is purposed to serve as a guide to industry and is reported to use three example industries to illustrate the process of implementation.

[142] The author would like to thank those members of QMI who suffered questions on the technicalities of the recognition process.

[143] CSA *Model Code supra* note 131 at Introduction (viii).

[144] As a result of this, there is a great deal of industry rumour concerning which organizations have submitted privacy codes for recognition.

[145] There is little debate that the CBA code was a best efforts code that meets the CSA standards. Those who created the CBA code had done so knowing the details of the upcoming CSA code and had complied with it.

[146] One such obstacle is that the QMI recognition requires that the organization be audited to see if it has implemented the requisite internal mechanisms to allow compliance with its own code. As the CBA's code is a standard for its members, the CBA itself has no such mechanisms and cannot be audited. This argument has been discredited by others who attribute the refusal of QMI to consider the CBA code as a product of the ongoing tensions between the two organizations.

from Price Waterhouse that it complies with the CSA code.[147]

The process of recognition is voluntary and a CSA member is allowed to elect from among three different tiers. Tier one is Declaration. It is based upon organizational self-direction. Tier two is Verification. QMI conducts an audit on the organization to determine if it is in compliance with the CSA standard. Tier three is Registration. The organization adopts both a privacy code and the ISO 9000 quality management standard and QMI audits it on compliance with both.

The fact that there is a tiered system of recognition implies that there are corresponding levels of benefit. However, given that the CSA's code provides only those minimum standards required under the OECD guidelines, it is difficult to argue that there can be different levels of compliance. One would hope for certainty in a recognition system—the label of either compliance or noncompliance with the minimum standards.

4. *Complaint Process*

Theoretically, a number of bodies could fill the role of registrar and complaint administrator. It has been suggested that it would have been better to have allotted both the registration process and the complaint process to the same registrar, but that QMI did not want the latter responsibility. The CSA has already abandoned some pilot programs for alternate auditing processes.[148] There have also been limited consideration of the Privacy Commissioner's qualifications, given its current adjudicational role, though it is believed that private sector privacy oversight would add too great a burden to its existing portfolio.

The CSA's committees are looking to Alternative Dispute Resolution (ADR) as a possible enforcement mechanism. The advantage of ADR over court process is that the latter could create two additional problems: (i) it could take a number of years before any case law would be established; and (ii) it could be difficult to quantify those damages that flow from breaches of privacy.

C. *The Privacy Commissioners*

Internationally, privacy commissioners have played dual roles in the development of privacy standards and the legislation that enforces them. Firstly, commissioners have enjoyed standing at almost every stage of standards formation. They are called upon to ensure that information in general enjoys free flow, while limiting sensitive and private information to those who should rightfully control it. Secondly, they are entrusted with adjudicative and enforcement powers to oversee the ongoing application of certain privacy standards. As Canada moves closer towards international standards, its privacy

---

[147] The Canadian Bankers Association, *Privacy Model Code*, (Toronto: CBA, March 1996). This code was varied in its November reprint (Canadian Bankers Association, *Privacy Model Code*, Toronto: CBA, November 1996) [hereinafter *Privacy Model Code*] only by the letter from Price Waterhouse. Arguably, this was an attempt by the CBA to force the hand of QMI to admit them into the recognition system.

[148] The CSA had offered to qualify persons at their own cost (reportedly upwards of $5,000) to be trained as auditors under the QMI tiers, but there was such limited response that the proposal was abandoned.

commissioners may be faced with new challenges in the private sector.

1. *Ontario Information and Privacy Commissioner*

Although the Ontario Commissioner states in its annual reports[149] that it has made submissions to provincial government on the protection of privacy in financial institutions[150] it would appear that the scope of the department's interests rests in the public sector. Having said this, it should be noted that the IPC was an active, though nonvoting, member of the CSA committee that drafted the CSA Model code[151] and continues to play a minor role in the voluntary code debates.

However, it would appear that Ontario's Privacy Commissioner may face a more direct role in the regulation of private sector privacy in the future. Although not all legislative proposals look to the Commissioner as a potential overseer of privacy complaints in the financial sector, the Uniform Law Conference has recognized that a "province might choose to grant jurisdiction on protection to its already existing Privacy Commissioner while another might opt to grant such powers to its Human Rights Commissioner".[152] Whether the banking industry will question the jurisdiction of Ontario's provincial Commissioner remains to be seen.[153]

2. *The Privacy Commissioner of Canada*

The Canadian Privacy Commissioner has faced an entirely different challenge in its ongoing effort to create financial institution privacy standards. The general position of the Commissioner is stated in his April 1992 submission to the Senate Standing Committee on Banking, Trade and Commerce.

> The Commissioner is concerned about the volume of personal information held by financial institutions, the capacity of information technology to sort, categorize and assimilate the data and the subsequent potential for the information to be communicated to and shared among affiliated financial institutions that perceive themselves as having a common interest in its collection and use.[154]

To some extent the Commissioner has taken on the role of a consumer advocate on data protection issues and has supported the implementation of enforceable

---

[149] The author was advised by the Office of the Privacy Commissioner that nothing beyond the Annual Reports could be made available.

[150] *1993 Annual Report supra* note 109.

[151] Information and Privacy Commissioner, *1995 Annual Report*, (Toronto: 1995).

[152] Standing Committee on Finance, 1997 Review of Financial Sector Legislation: Proposals for Change - Fourth Report of the Standing Committee on Finance, October 1996 [hereinafter "Proposals for Change"].

[153] Bennett, Colin, *Canada Sets the Standard on Implementing Privacy Codes* in *Privacy Laws and Business Newsletter*, January 1996. Bennett states that the "Office of the Information and Privacy Commissioners might appear the most logical location for *oversight responsibility*, given the way that privacy codes have been developed in the past".

[154] Regulating the Financial Institutions *supra* note 109 at "Executive Summary".

legislation.[155] In his 1996 submission to the Standing Senate Committee, the Commissioner stated that the present recommendations in Finance Canada's 1997 White Paper[156] "would not in any way constitute an advance...over the status quo."[157] It would appear that, while the Commissioner welcomes (and insists upon) the recognition of privacy in the private sector, the White Paper and the subsequent reports pursuant to it, have confirmed his suspicions that the legislative action will be "excessively timid" and "emasculated by concessions to special interest groups".[158]

3. *Canadian Bankers Association*[159]

The Canadian Bankers Association was established in 1891 to provide support and research for its members, the chartered banks.[160] To its credit, the Canadian Bankers Association has been a longtime participant in the development of privacy codes. In April 1986 the organization adopted the OECD guidelines and created a set of privacy principles (though its membership never formally adopted them).[161]

It wasn't until 1989 that the CBA set up a task force to convene with Canada's Privacy Commissioner, Consumer and Corporate Affairs Canada and Finance Canada. This Task Force deliberated throughout 1989 and 1990, and came up with a Code of Conduct in 1990. This code was amended in 1993.

On a voluntary basis, CBA member banks developed analogous codes and guidelines that reflected their support of the Association's initiatives. It is not incorrect, therefore, to suggest that the CBA had adopted CSA-like standards long before there was a so-called national standard.[162] The only marked difference, although admittedly an important one, is that the older CBA codes recognize the four common law occasions for information disclosure enunciated in *Tournier*.

The confrontational release of the CBA Model Code has already been discussed in part. Although the 1996 Model Code[163] includes an extensive commentary on the application of the principles and was touted to exceed the national standard, it was not endorsed, let alone embraced, by the CSA. Nevertheless, the CBA promoted its *new standard* in bank privacy. At the release, CBA President Helen K. Sinclair stated that

---

[155] Compare *Proposals for Change supra* note 152 at 3. The report reads: "Canada's Privacy Commissioner and the Consumer's Association of Canada...urged that regulation should include a mechanism for enforceability, legislated sanctions for failure to comply, and oversight by an independent third party."

[156] *Ibid.*

[157] Standing Committee on Finance, Minutes from the Presentation of the Privacy Commissioner *supra* note 1.

[158] Privacy Commissioner, Press Release, *"Government's Privacy Message 'Mixed'"* (29 July 1996) [hereinafter "Message 'Mixed'"].

[159] The author received insight into the goals of the CBA thanks to the patient contributions of Consumer Affairs, Canadian Bankers Association.

[160] C. Bennett, *The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association* [hereinafter *The Protection of Personal Financial Information*]. This paper was presented to an Industry Canada seminar in October 1995 and has no published citation.

[161] *Ibid.*

[162] Canadian Bankers Association, 1993. *Model Privacy Code for Individual Customers,* Revised September 1993: Toronto: CBA.

[163] *Privacy Model Code supra* note 147.

"privacy has always been an integral part of the banking tradition" and that "banks are known to be leaders in protecting privacy."[164] Less dramatic comments, but encouraging ones nonetheless, were offered by Consumer Advocacy groups in support of the new code for banking privacy.[165]

D. Privacy Model Code - *What Is It?*

The CBA Model Code is an example to be followed by the CBA's member banks. Like the CSA code and the OECD principles, the CBA code has basic principles covering the collection, use and disclosure of information; however, it expands on those principles, provides sector-specific definitions to circumscribe those principles and provides that each bank may, in its own code:

(i) define how it subscribes to each principle;
(ii) modify details to provide specific examples;
(iii) include additional measures for the protection of privacy.[166]

The effect of these three suggestions is to have the banks change the form of their codes of conduct from traditional policy bulletins to *user-friendly* consumer guides. While this does nothing for privacy *per se*, it does serve to communicate to the consumer how his or her bank's practices are affected and molded by its privacy policy. The goal for each bank should be to create a privacy code that gives the policy context - casts it in its everyday role - so that a consumer can readily identify his or her privacy protections.[167]

---

[164] There has been some suggestion that the CBA made the decision to formulate its code on the CSA model so as not to face criticisms for not meeting the CSA standard. There have also been suggestions that the CBA had been led to believe that the CSA was looking for other codes to be released at the same time as its Model Code in order to exemplify the ease of application. Those who oppose this position state that the CBA's decision to release their code at the same time as the CSA release was a deliberate attempt to *steal some of the thunder*, as it were, of the CSA release.

[165] *Ibid.* Tony Dearness, President, Consumers' Association of Canada (CAC) said, "The CAC is very pleased that the banking industry continues to show concern for its customers' personal information by improving upon its previous code".

[166] *Privacy Model Code supra* note 147 at 3.

[167] Although it is not a purpose of this paper to critique bank practices, some note should be taken of existing bank initiatives pursuant to the 1990 and 1993 CBA privacy codes. Three banks serve as examples: The Toronto Dominion Bank offers its customers a leaflet which it calls its privacy code. This document is clear and understandable but is below the threshold of detail required under the 1996 Model Code. The Royal Bank has a similar branch leaflet but will produce a two-page restatement of the OECD principles with limited commentary when pressed for further information. One of the more comprehensive packages is offered by the Bank of Montreal. Upon request it will produce its branch leaflet, its Code of Conduct and an eleven-page manual on confidentiality. While the latter is clearly outdated (1990) it is by far the closest document to what the present CBA Model Code contemplates. Compare Bank of Montreal, *Your Privacy,* document 5052440 (05/92), Bank of Montreal, *First Principles – Our Code of Conduct,* document 3700 (4/93); Bank of Montreal, *Confidentiality of Information Manual,* January 30, 1990; Royal Bank, *Straight Talk about Client Privacy,* Document 7568 (07/96); Royal Bank, *Royal Bank of Canada Privacy Code* (undated); Toronto Dominion Bank, *The TD Commitment:*

Accordingly, a bank would not meet the standard set in the CBA Model Code by issuing only a restatement of the 10 principles. The new bank privacy codes, created in the shadow of the CBA example must, by necessity, contain more than a list of principles with annotations.

1. *The Ten Principles*

In order to better illustrate what more is required of a bank's code of privacy than the CSA's 10 standards, some of the modifications and qualifications in the CBA Model Code are compared below:

CSA Model Code Standards	CBA Qualifications to CSA Standards
1. An organization is responsible for personal information under its control and shall designate an individual or individuals...who are accountable for the organization's compliance with the following principles.	This will require employee training and set day-to-day procedures of compliance for handling information and responding to customer inquiries.
2. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.	Not only the use of the information collected, but the potential uses of the information and the right of the customer to withhold consent are to be communicated to the customer.
3. The knowledge or consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.	Consent can be given by oral, written or electronic means, or implied by action or inaction, or through an authorized representative.
4. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.	Information may also be collected from credit bureaus, employers and other lenders.
5. 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 fulfilment of those purposes.	Under some circumstances, banks have a common law right or duty to disclose personal information to protect the bank's or the public interest. A bank may notify the customers if a legal order has been received for disclosure if the law so allows.
6. Personal Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.	Limits for the need for accuracy may be set out clearly by the bank. Customers may challenge the accuracy of information held.
7. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.	These safeguards will be physical, organizational and electronic in nature.

Business Banking Relationship Standards, document 21244 (12/94); Toronto Dominion Bank, *The TD Commitment: if you have a comment concern or complaint...,* document 19460 (08/95); Toronto Dominion Bank, *Your Business. Your Bank. Business Relationship Standards,* document 21244 (03/96).

CSA Model Code Standards	CBA Qualifications to CSA Standards
8. An organization shall make readily available specific information about its policies and practices relating to the management of personal information.	Information about policies will be made available to customers. The privacy code will be made available. It will be easy to understand.
9. Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.	A bank may not be able to provide personal information where: (i) it is too costly, (ii) it contains references to other persons or (iii) it is subject to solicitor/client or litigation privilege.
10. 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.[168]	Each bank will investigate all complaints. If customers are not satisfied they can contact the Office of the Superintendent of Financial Institutions or the Banking Industry ombudsman.

2. *When a Bank Drafts Its Code...*

When a bank looks to drafting its new privacy code it is going to have to begin with a fresh slate. Given the different organizational structure of the new CBA code, a bank would do well to avoid the temptation simply to edit and supplement its existing privacy code. The following considers some of the above requirements in more detail.

a) *The Bank's Accountability*

In order for a privacy code to have any practical value, it must be supported by sufficient employee training, customer booklets and internal policies to give it effect. Should a bank create a new code but fail to retrain its employees, it will face serious conflict in its implementation. The code requires that employees be more conscious of their everyday dialogue with customers. It falls upon the bank, therefore, to develop an employee training program that includes an *'if asked this - then answer this'* type of process.[169] It must be recalled that the transfer of information at the branch level is not always mechanical (it does not always involve physically printing a document for the customer). In fact, more often than not, disclosure will be made orally, and in such a fluid manner that the employee fails to recognize the disclosure. It may be that the bank employee is informally asked information about a customer—an account balance, acomment on credit status, or even a first name. Neither the law nor the Model Code forgives disclosure on the basis of lack of intention or malice. Information is either disclosed or not disclosed—and more importantly, once disclosed it cannot be made

[168] *Supra* note 135.

[169] Compare C. Bennett, *The Protection of Personal Financial Information supra* note 160, who quotes Jeff Smith as stating that, "if an organization's policy is to reflect goals rather than current realities, the only credible approach is to prepare, at the same time as the policy, a concrete list of action steps for achieving compliance". See J. Smith, *Managing Privacy: Information Technology and Corporate America* (Chapel Hill: University of North Carolina Press, 1994) at 236.

confidential again. Accordingly, employees require training that will make them conscious of the potential value to the customer of certain types of information and the boundaries of allowable dialogue.

b) *Identifying the Purposes of Personal Information*

Banks have long been advocates of the opt-out consent clause in a contract in which the customer adjusts the contract only to the extent that she doesn't consent to the information uses and disclosure powers being afforded to the bank. The Model Code makes provision for face-to-face and telephone transactions. To accommodate the former the bank will have to adjust its contracts so that the consent clauses are made conspicuous (either using boldface type or a separate box). Electronic and telephone transactions that create either a new relationship between bank and customer or that could lead to further information access for the bank, should be prefaced by proper communications of the privacy concern to the customer. An on-line computer service, such as internet banking, will require a visible and conspicuous explanation of privacy issues and customer consent. Customer service representatives will have to be provided with a complete and understandable script to the same effect. A further obligation falls upon branch staff to be able to explain purposes "which are not as obvious as others".[170] Clearly this will require a subjective assessment by the employee of the customer's comprehension. A customer that has difficulty filling out the forms, is illiterate, blind, or who has problems speaking English may require that all of the disclosure clauses be explained orally. A bank's failure to ensure that a customer fully understands the disclosure clauses can result in a lack of consent even if the contract is signed without any opt-outs.

c) *Getting the Customer's Consent*

Of the four grounds for disclosure in *Tournier,* the ability to disclose confidential information with express or implied consent, is by far the most attractive to banks. Accordingly, the CBA Model Code gives extensive treatment to defining when it deems consent to be received. It should be noted, however, that a bank would want to err on the side of caution since the Model Code is not determinative of when a court would recognize consent. Consent is expressed when the terms of consent are verbally or in written form communicated to the customer, understood by the customer, and not opted-out of by the customer. This last point should not be confused with consent through inaction or silence as the customer still acts in signing the form or completing the application. Consent may be implied when a customer uses a bank service or product, or does not act to have a name removed from a direct marketing list.

d) *Limits for Collecting Personal Information*

The CBA Model Code adds one important note to this principle - that the information collected is not limited to that obtained from the customer. Information may also be obtained from other lenders, credit bureaus or employers. There may be some question about the source of consent when a bank receives information. One

[170] *Privacy Model Code supra* note 147 at 10.

could contend that the customer contracts with these third parties, allowing them the ability to disclose personal information, and that the bank can assume that it receives this information pursuant to that consent.

The Model Code, however, would suggest a different conclusion. In the Model Code's discussion of principle 3 it states: "when a bank obtains customer lists from another organization, it will assume that the organization providing the personal information obtained each customer's consent before disclosing it to the bank."[171] Accordingly, it would appear that only the transfer of customer lists is governed by customer consent given to the transferor, and that the bank is required to obtain consent in order to receive information about individual customers from third parties.

d) *Limits for Using, Disclosing and Keeping Personal Information.*

Principle 3 has a retrogressive effect since it resorts to the common law disclosure exceptions despite the fact that not all of those exceptions are recognized in either the CSA or OECD standards. The full breadth of *Tournier* disclosure is invoked by this principle. If any limits can be read into this, they are to be found in the notes to Principle 3 which state more restrictive disclosure exceptions:

(i) Legal Reasons
The code cites that the bank may be compelled by the law to disclose information. This exception for disclosure is recognized in *Tournier* and in the OECD guidelines. Principle 5 provides such examples as subpoenas, search warrants, and court orders.

(ii) Security Reasons
Although it is unclear from Principle 3's commentary, it would appear that the prevention or detection of fraud is considered to be a security reason for disclosure. If read into Principle 5's adoption of *Tournier*, this might provide some limits to the 'disclosure for public interest protection exception'.

(iii) Processing Reasons
This exception is decidedly more restrictive than the *Tournier* exception - disclosure in the interests of the bank - and could be said to restrict it. Under this exception a bank may make only such disclosure as is necessary to collect on overdue accounts or to allow its agents to perform their banking tasks.

It is also interesting to note that the Model Code recognizes, at least to some degree, that a bank may have a duty to inform the customer when his or her records have been disclosed under compulsion of law. Admittedly, the code states that a bank 'may' make disclosure; however, as the common law is unclear on this point in Canada, a recognition of the possibility that the duty exists is appropriate.

f) *Keeping Personal Information Accurate*

The CBA Model Code adds two details to the CSA standard on the point of accuracy. Banks will respond to challenges from customers with respect to information

[171] *Ibid.* at Section 12.

accuracy, and there may be some circumstances in which a bank has set limits on the need for accuracy. It is imperative that the latter be given the same conspicuous presence in the contract document as the consent clause. Should a bank not choose to do so, it may not be allowed to rely on the clause if the inaccuracy later causes injury to the customer.

g) *Safeguarding Personal Information*

Three levels of security safeguards are mentioned explicitly in the code, and one is implied. The physical safeguards will include locks and safes. The organizational safeguards will include divided access to lock combinations, electronic terminals, and data centres. The electronic safeguards will include passwords and personal identification numbers. None of these safeguards is new. Regular employee training in privacy policy is the fourth safeguard. It can affect the other measures in significant ways. The division of passwords, safe and lock combinations, access to data bases and the like are only as effective as the personal measures that the participating employees take to keep the information apart from other employees. Assistant managers who notoriously keep their combinations in their wallets, or customer service representatives who frequently enter their terminal passwords in the open view of others, threaten the safeguards in place, and the security of customer information.

h) *Making Information About Policies and Procedures Available*

An important distinction is made between policies and codes in the Model Code. A bank will not necessarily be required to disclose all of the internal rules that enforce its code of conduct. Nevertheless, some information about those policies might be disclosed in order to explain the code of privacy. The Privacy Code itself, which should be a separate document from the branch brochures, should be made available to customers upon request. While public relations may appear to be one of the natural reasons for creating a privacy code, it should be noted that it is not the current practice of all banks to provide more than the branch brochure to inquiring customers.[172]

i) *Customer Access to Personal Information*

The Model Code provides three instances in which the customer may be unable to access information in the control of the bank: when the collection would be too costly, when the document may contain another's personal information, or when solicitor/client privilege or litigation privilege might apply. A bank would do well to reconsider restating these expectations in its codes of conduct. Firstly, they constitute a claw-back from the absolute freedom of access by a person to his or her personal information. Secondly, they pose some implementation problems. It would appear that an issue of data retrieval costs involves a subjective assessment of the importance of the data. This section already places the minimal cost of retrieval on the customer.[173] Those costs that

[172] In his research the author was refused copies of existing privacy codes by two banks on the grounds that they were proprietary documents.

[173] *Privacy Model Code supra* note 147 at 23.

are above the minimal amount should not necessarily block data production.

It is also difficult to envision a matter of solicitor/client privilege which would bar a bank from disclosing a customer's information to her or him. In the absence of some unusual third party claim to privilege the bank and the customer would both be in a position to sever irrelevant portions from the document, waive the privilege, and enjoy proper disclosure.

j) *Handling Customers' Complaints and Questions*

Those complainants who are dissatisfied with the bank's investigation and response can take their complaint to the banking industry ombudsman."[174] Although little is said concerning institutional complaint mechanisms, a bank's code of conduct should provide a comprehensive course of action for a complainant. Each bank has its own ombudsman to whom final complaints can normally be directed.[175] Beyond that, the process for complaints is unresolved. The author's inquiries of the Office of the Superintendent of Financial Institutions established two things: (i) that no complaints have yet reached the office pursuant to the 1996 Model Code, and (ii) that the Superintendent has no written policy, guideline or other document that specifically addresses privacy complaints under the Model Code.

VI. LEGISLATIVE MOVEMENT

It is now widely accepted that the CSA privacy code represents the national standard for the protection of personal information in Canada. While the degree to which the government will recognize, affirm and enforce this standard is not settled officially, there are sufficient indicia to suggest that Canadian legislation will be to the CSA code what the CSA code is to the now outdated OECD guidelines - a restatement and reconfiguration without substantial improvement. To some, however, this would amount to an attractive solution to privacy concerns. Colin Bennett, who has worked closely with the CSA, has remarked that "the [CSA] standard can be used on a more incremental basis to respond to the most egregious abuses of personal data...thus a Canadian legislature could simply say that particular organizations be required to register to the CSA Model Code".[176] This point is easily pressed on the grounds that implementation and oversight would be less costly to government and the burden of enforcement would be kept in the private sector where costs are borne by users. However, protection by reference to loose standards is poor protection. Regulation should not have the effect only of making the voluntary mandatory; rather, it should look to the prevention of information abuse through deterrence mechanisms, it should define clearly the proper uses of information, it should provide specific and enforceable sanctions for noncompliance with those uses and it should delineate a process of

---

[174] *Ibid.* at 10.3 It should be noted that the November 1996 reprint of the code reads somewhat differently: "or, as of early 1997, the banking industry ombudsman."

[175] C. Bennett, *supra* note 169. The author cites a November 7, 1995 press release which states that the ombudsman will be "empowered to investigate and make non-binding recommendations to resolve complaints, will not be a banker and will operate independently of the banks and the CBA".

[176] C. Bennett, "Standards for Privacy" (1995) 3:2 International Privacy Bulletin 4.

complaint and appeal to reach those sanctions. Anything less would place Canada's first national legislative action in the rear of an international movement towards consumer protection.[177]

A. *Direct Marketing Association*

One might expect that the Canadian Direct Marketing Association would support its largest customers, the banks,[178] and lobby for flexible and voluntary privacy standards because of its dependency on access to vast data banks of personal information. However, the CDMA has been an advocate of fixed and enforceable standards. CDMA's President, John Gustavson stated, "legislation is the most effective means of ensuring all private sector organizations adhere to the same basic set of rules...".[179] The CDMA has created its own privacy standards[180] based upon the OECD guidelines and independently of the CSA initiatives. Unlike the CSA or CBA codes, the CDMA code includes detailed enforcement procedures with complaint mechanisms and response deadlines[181] and, arguably, exceeds the level of data protection provided by either of them. Even with this shield of data protection firmly in place, the CDMA has insisted that legislation be enacted to ensure the uniform protection of privacy.

Our discussion of legislative initiatives opens with the CDMA so that two points may be raised concerning legislative proposals: (i) they do have supporters within industry who stand firmly for enforceable privacy standards; and (ii) that legislative efforts, in order to set any meaningful standards will have to surpass the basic principles of the CSA code and, at the very minimum, provide protections equal to those created in existing voluntary codes. The legislative trends, as described below, would imply that the latter requirement will not be met.

B. *Department of Finance*[182]

It would appear that the first serious threat to banks' self-regulating privacy came when the *Bank Act*[183] gave the Cabinet the capacity to regulate in 1990. The *Bank Act*

---

[177] Mr. Phillips, Canadian Privacy Commissioner testified that, by early in 1996, New Zealand, Germany, France and the Netherlands had enacted statutes to protect the privacy rights of citizens in the private sector, and that Australia was in the process of extending its privacy law. Standing Committee on Finance, *Minutes of the Privacy Commissioner's presentation supra* note 1.

[178] Canadian Direct Marketing Association, Code of Ethics and Standards of Practice (Toronto: CDMA). The code states in its Introduction that "Canadian Direct Marketing Association members include *Canada's Major Financial Institutions*, retailers, publishers, cataloguers and charities, as well as a wide range of suppliers of goods and services to direct marketers" [emphasis added].

[179] Ontario, Information and Privacy Commissioner, *1995 Annual Report* (Toronto: Queen's Printer, 1996) at 5.

[180] *Code of Ethics and Standards*, *supra* note 155.

[181] *Ibid.*

[182] The author is indebted, in part, to the contributions of Industry Canada and the Ministry of Finance, for the following discussion.

[183] *Supra* note 113. Recently, the Court acknowledged that the *Bank Act* imposes obligations regarding client information in *Arab Banking Corp.* v. *Coopers & Lybrand* [1996] R.J.Q. 1715 (S.C.).

gives power to the Governor in Council to make regulations "governing the use by a bank of any information supplied to the bank by its customers".[184] In the years since that time the Department has met with increasing pressure to utilize that power to regulate in a manner consistent with consumer interests. To date no regulations exist pursuant to this section.[185] Prior to 1996 the Ministry was hesitant to commit to any specific regulatory response to privacy concerns. See for example, the April 28, 1995 speech of the Secretary of State (Financial Institutions) at the Financial Services Institute's 'Off The Record' breakfast meeting:

> There has been...a lot of discussion of issues related to privacy and the treatment of confidential information by financial institutions. And to be sure, this is not a new issue, as it was also discussed leading up to the 1992 reforms. At that time, the government looked to the financial services industry for self regulation -- and the industry responded...Again we think that the industry codes have been working well. However, we continue to be aware of the needs and concerns of consumers regarding the treatment of personal information.[186]

It wasn't until June 1996 that the Department of Finance indicated its intention to use its *Bank Act* section 459 power to "build on [the CSA code, *inter alia*] with further improvements."[187] According to the White Paper, the proposed regulations would ensure that financial institutions:

> adopt a code of conduct governing the collection, use, retention and disclosure of information. The government encourages financial institutions to use the CSA code as a minimum standard in formulating their codes of conduct;
>
> designate a senior-level officer in each financial institution to implement procedures for dealing with consumer complaints;
>
> provide customers with written information on their privacy code and details of how customers can make complaints;
>
> report annually on the complaints received and the actions taken to respond to these

---

[184] *Ibid.* at s. 459.

[185] Draft regulations were prepared for the Standing Senate Committee on Banking, Trade and Commerce 1993, but have not been adopted. Prior to the 1996 proposals the scope of section 459 could be exemplified in the *Insurance Business (Banks) Regulations* SOR/92-330, May 21, 1992 which provided in s 8.(1) that "No bank shall (a) provide, directly or indirectly, an insurance company, agent or broker with any information respecting (i) a customer of the bank of Canada, (ii) an employee of a customer of the Bank in Canada, (iii) where a customer of the bank is an entity with members in Canada, any such member, or (iv) where a customer of the bank is a partnership with partners in Canada, any such partner".

[186] Finance Canada News Release, "Issues and Ideas For Financial Sector Change", notes for an address by the Honourable Douglas Peters Secretary of State (Financial Institutions) to the Financial Services Institute, 95-040, April 28, 1995. Compare similar comments in Finance Canada News Release, Notes for Remarks By the Honourable Doug Peters, Secretary of State for International Financial Institutions to the Canadian Turnaround Management Association (Ottawa Chapter), 95-103, December 7, 1995.

[187] *Proposals for Changes, supra* note 152 at 15.

complaints.[188]

A House of Commons Standing Committee on Finance was created to explore these proposals. This Standing Committee's report in October 1996[189] provides a strong indication of what can be expected of this legislation, if it is created. At the heart of the report is the comment that "the committee received no evidence involving the abuse of private information by a financial institution...[but] the potential for abuse...is enormous and the need to deal with privacy concerns [is] unquestioned".[190] Arguably, the extent of this legislation's effect is contained in this comment. Without evidence of abuse the committee will be able to avoid a comprehensive regulatory scheme complete with sanctions.[191] It would appear that the committee's failure to hear of privacy breaches in the financial sector is evidence only of their incomplete guest list at the hearings.

Beyond adopting the four requirements set out in the White Paper, the committee recommends that a Consumer Protection Bureau (CPB) be set up, reporting to the Minister of Industry, to somehow deal with consumer complaints that are not satisfied by the banks' complaint mechanisms. The proposed bureau would report directly to Parliament with respect to these complaints.[192]

C. *Department of Justice and Department of Industry: Uniform Law Conference*[193]

In his September 1996 address to the International Conference on Privacy and Data Protection, the Minister of Justice referred to the long term governmental plan for privacy legislation:

> By the year 2000, we aim to have federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector.
>
> In 1984, when Canada signed on to the OECD guidelines on transborder flows of personal data, we adopted a two-tiered approach for its implementation. Basically, it was this: legislation for the public sector, and self-regulation for the private sector. The Government of Canada has now reconsidered that approach. We have done so because it is obsolete.[194]

---

[188] *Ibid.* at 16.

[189] *Supra* note 152.

[190] *Ibid.* at 3.

[191] *Ibid.* The report states "the Committee does not have evidence of actual abuses before it sufficient to justify a full regulatory regime with prescribed penalties at this time, but does believe that the provisions in the White Paper for a self-regulated regime should be strengthened".

[192] *Ibid.* at 4. Despite the fact that the recommendations urge that "the above proposals to protect the privacy rights of financial institution customers be enacted immediately", there has been no further reported action in this area.

[193] This is not the first consideration that the Department of Justice has given to legislative proposals to regulate privacy in the private sector. In 1987 the Minister was presented with the suggestion that the federal Privacy Act be extended to cover the federally regulated private sector. Compare Canada, Department of Justice, *Access and Privacy: The Steps Ahead.* Ottawa: Supply and Services Canada, 1987.

[194] A. Rock, Address (Eighteenth International Conference on Privacy and Data Protection, Ottawa, 18 September 1996) [Unpublished][hereinafter "Rock Address"].

Although the Minister disclosed little more at the time than that he and the Minister of Industry were collaborating in the project,[195] there is now some indication of what this legislation would purport to accomplish.

The Uniform Law Conference of Canada heard in its 1995 proceedings the submission of Denis Kratchanov (also of the Department of Justice) that data protection legislation be created for the private sector[196] and shortly thereafter resolved "that the Steering Committee of the Section create a Task Force to develop proposals for a Uniform Personal Information Protection Act which will include a statement of principles and options for implementation."[197] The following year's conference involved a series of directions and recommendations for the drafting of that statute:[198]

> The [...]CSA Model Code represent[s] a good base on which to build a Uniform statute and these principles are consistent with the principles in the Quebec Act.[199]
>
> There is a large consensus for using existing data protection bodies to oversee laws regulating data protection in the private sector.[200]
>
> A uniform statute should provide the data protection commission with a mandate for public education, powers to receive complaints, conduct investigations, mediation and adjudication. The law should provide the Commission with the power to publicize the names of organizations with poor performance.[201]
>
> The Uniform statute should express universally applicable data protection principles and an implementation mechanism, and should not attempt to set out specific rules for medical information, credit reporting or deal with privacy issues that are broader than data collection.[202]

As both the 1995 and 1996 submissions to the ULCC came from members of the Department of Industry, it is safe to assume that the above proposals reflect the general nature of what the government hopes to create.[203]

The proposed legislation would cover the entire private sector, including the banking industry, and would apply to banks instead of the legislation proposed by the

---

[195] *"Message 'Mixed'"*, *supra* note 158.

[196] D. Kratchanov, "Personal Information and the Protection of Privacy" in *Uniform Law Conference of Canada: Proceedings of the Seventy-Seventh annual Meeting* (Ottawa: ULCC, 1995) at http://www.law.ualberta.ca/alri/ulc/95pro/e95m.htm#g [hereinafter "Personal Information"].

[197] *Ibid.* at 46.

[198] T. McMahon, "Data Protection in the Private Sector: Options for a Uniform Statute" in *Uniform Law Conference of Canada: Proceedings of the Seventy-Eighth Annual Meeting* (Ottawa: ULCC, 1996) at 45 [hereinafter "Uniform Statute"].

[199] *Ibid.* at 204. The concern with compliance to the Quebec legislation is rooted in the desire for national uniformity and inter-provincial comity.

[200] *Ibid.*

[201] *Ibid.* at 205.

[202] *Ibid.*

[203] The author states this despite the disclaimer in "Personal Information" *supra* note 196: "The opinions expressed in this paper do not necessarily reflect the views of the Department of Justice Canada".

Ministry of Finance.[204] Since the legislation is slated for completion following the Ministry of Finance legislation, the latter would apply to the banking industry in the interim.[205]

D. Bill 68—*The Quebec Example*

While the private sector in Canada has some privacy legislation due to Quebec's Bill 68[206], the banking industry remains unregulated in this area. In Quebec the banking industry will not officially recognize the bill on division of powers grounds - banks are regulated federally and this is a provincial initiative. Some banks have said that they will honour the spirit of the Act, but indicate they will not submit to the authority of provincial Privacy Commissioners.[207] This is not to say that financial institutions have skirted the privacy debate in Quebec. Recently, consumer groups were able to pressure members of the insurance industry in Quebec to alter their consent clauses to better protect consumers.

Quebec has set a new standard by being the first jurisdiction in North America to attempt to regulate private sector data protection[208], and the debate promises to continue towards 2000. The effect of being first has been to create a yardstick against which other jurisdictions can measure their compliance to the national standard. At the 1996 U.L.C.C. members heard the following submission.

> Given that the purpose of the Uniform Law Conference is to promote uniformity across the country, and given that Quebec has already legislated data protection in the private sector, any departure from the Quebec model would make uniformity more difficult to achieve.

Though neither Industry Canada nor the Department of Finance has admitted directly that the contents of Bill 68 will affect its legislative proposals, that would seem to be a likely proposition.[209] At the very least, Quebec's law is likely to meet the

---

[204] The author relies here upon the information provided in an interview with Mr. Denis Kratchanov, Department of Justice, November 15, 1996. Mr. Kratchanov is presently working on the legislative proposal to protect privacy in the private sector.

[205] Note that the *Proposals for Change supra* note 152 at 15 recognizes that "any action in the financial services area should be consistent with the federal government's broader approach for [...] a legislative framework to protect personal data".

[206] Bill 68, *An Act respecting the protection of personal information in the private sector.* 2nd Sess. 34th Leg., Quebec, 1992.

[207] Standing Committee on Finance, Minutes of the Privacy Commissioner's presentation *supra* note 1.

[208] "Personal Information" *supra* note 196.

[209] One action that Bill 68 has taken which federal legislation would to well to consider is to impose sanctions for noncompliance. The penal provisions include fines from $1,000-$20,000 according to the offense. Certain officers and directors can be held personally liable for the actions of their corporations. The offenses attach to those who collect, hold, communicate or use information in a manner not authorized by the Act R.S.Q. c.P-39.1, ss. 91-93. Compare "Uniform Statute" *supra* note 193.

standards set by the Economic Union.[210]

VII. GOING TOWARDS 2000—WHERE DOES A BANK STAND?

One of the catalysts to both the legislative and voluntary code project development is the international pressure of the European Union Privacy Directive[211] that has been approved by the Council of Ministers and is being considered by the Legal Affairs and Citizens' Rights Committee of the European Parliament.[212] The directive sets a standard that must be met by those wishing to do trade with the European Union and could create a barrier to trade against non-complying countries. The Privacy Commissioners of the European states will be able to block the trans-border flow of information to countries which, in their opinion, have not enacted adequate privacy safeguards.[213] Needless to say, much of the urgency surrounding privacy matters is in response to the unknown ramifications of noncompliance. The Minister of Justice stated in September 1996 that "we are aware of how the approaching deadline of 1998 will affect the transfer of personal data from the Union's member countries".[214] In fact, most commentaries on either privacy codes or impending privacy legislation cite the EU directive as being among the immediate reasons for uniform regulation.[215] Even if there are no tangible sanctions that flow from Canada's failure to meet the E.U. directive, undoubtedly its major trading partners will be concerned over the abuse that their citizens' confidential information may suffer within Canadian borders.[216]

While the banking industry awaits legislation it will have to give more than passing acknowledgements to the potential effects of these voluntary codes. At the very least a bank's failure to comply with its privacy code or to the CBA's Model Code (which is the industry's accepted standard), could lead to adverse publicity, competitive disadvantage and inter-provincial and international pressures.[217]

While none of these may act as a disincentive to a bank that enjoys lucrative returns

---

[210] C. Bennett, "Privacy Protection for the Information Highway" *supra* note 2 at 44. The author points to the fact that non-tariff trade barriers of this sort threaten Canada internally. [T]he Quebec legislation permits the Commission d'Accès à l'Information to prevent the flow of information to parties outside Quebec if that information will be used "for purposes not relevant to the objects of the file or communicated to third persons without the consent of the persons concerned."

[211] *The protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995, European Union Directive 95/46/EC of the European Parliament and Council, OJ No. L281 at 31.

[212] "Personal Information" *supra* note 196.

[213] Standing Committee on Finance, Minutes of the Privacy Commissioner's presentation *supra* note 1.

[214] "Rock Address" *supra* note 194.

[215] "Uniform Statute" *supra* note 198 at 184. This paper which was read at a Uniform Law Conference states that "there are important trade reasons to develop a uniform statute: to ensure that trade with the European Union countries is not disrupted by failure to meet the adequacy test of the EC Data Protection Directive".

[216] The Commissioner stated to the Senate Standing Committee that "it is the view of most of the Privacy Commissioners in the European Community with whom [he] has had the opportunity to speak that at present Canada's laws are not up to snuff."

[217] Bennett, *Canada Sets the Standard on Implementing Privacy Codes* in *Privacy Laws and Business Newsletter*, January 1996.

from the disclosure of customer information, new theories concerning the evidentiary value of these codes might demand further consideration. One part of Industry Canada's work in privacy has included a Voluntary Codes Project. The most recent work associated with that project has relevance to banking privacy codes.[218] Studies under this project have found that voluntary codes of conduct have been, and continue to be used to indicate the standard of care in an action for negligence. Although the breach of the industry standard would not be *ipso facto* negligence, the standard would certainly be *prima facie* evidence of what is generally expected of a participant within a given commercial circle.[219] A bank's code that is inferior to the CBA Model Code in data protection policy to would do little to overcome this burden. It should also be noted that those banks that have not adopted the CBA Model Code could still find themselves bound by the standard of care that the CBA Model Code imposes on the industry.

It would seem likely that Parliament will enact legislation covering banking as it looks towards 2000. Even if such legislation does nothing more than require compliance with the CSA Model Code, the banking industry will have to reconsider its code and each bank will, in turn, have to comply. Despite the fact that the CBA has received some indication that its code complies with the CSA standard, it has no guarantee that this is the case. The CBA's continued reference to *Tournier* in its code threatens to broaden the criteria for disclosure beyond CSA limits. The CSA code does not make allowances for such considerations as disclosure in the public interest and may be in direct conflict with the CBA Model Code as a result. It is also important to note that bank privacy codes will invariably set more vague criteria than the CBA Model Code, which could place them even further off the CSA mark.

A prudent bank will look beyond the CBA code to the CSA code and to the Directive of the European Union because compliance with these three documents will all but ensure compliance with future legislation. A very cautious bank will also look to Quebec's Bill 68 on the grounds that upcoming legislation may be created in the interest of maintaining inter-provincial uniformity. A forward-thinking bank will incorporate all of these considerations into a comprehensive and precise document with descriptions and examples of bank practice, all in simple and easily understood language.

---

[218] K. Webb, *The Legal Aspects of Voluntary Codes* [unpublished]. Mr. Webb, who is with the Consumer Affairs section of Industry Canada kindly provided the author with a copy.

[219] *Ibid.*