Privacy Enters the Canadian Courtroom: The Privacy Rights of Litigants and Witnesses

Simon CHESTER*

I. Privacy Enters the Canadian Courtroom

Canadian courts are slowly coming to terms with the concept of privacy. They are exploring its complexity, locating its unusual status within the realm of constitutional values, and balancing it against other interests. And they are doing so within a society where the advances of global communication and ever-more powerful technologies of information management and data-surveillance matching pose problems of privacy ever more starkly. In a post-September 11, 2001 world, it has become apparent that privacy does not function solely as an accepted legal imperative — we now realize that it must contend with other social or constitutional goods, such as security or the apparent confidence of perceived security. Privacy is becoming increasingly complex and compromised, its value touched by nuance and scruple.

In this paper, I do not intend to canvass the entire range of such emerging theories of privacy, but instead to concentrate more modestly on two issues:

- An exploration of how the limited jurisprudence under the *Personal Information Protection and Electronic Documents Act* reveals the Act's impact on civil litigation, and
- A canvass of English developments applying privacy rights located within the *European Convention on Human Rights* and enshrined in the *Human Rights Act* to expand the law of breach of confidentiality as a partial tool for vindicating the privacy interests of rich celebrities.

---

* Partner, Heenan Blaikie LLP. Recognition is given to Jayashree Goswami, Student-at-Law for her research help in the drafting of this paper. The grosser errors are acknowledged by the author.

As the United States weakens its limited legal commitment to privacy in the name of security, it is useful to note the special position that Canada has taken within the global law of privacy. Since we share an increasingly integrated market with the United States, we are accustomed to regulatory mechanisms which adopt a reliance on market-based mechanisms or self-regulation or light regulatory oversight. Yet our legal and social democratic traditions betray their origins within European approaches to community and social order. For three decades, Canadian policy-makers have been active participants in the Organization for Economic Co-Operation and Development's initiatives to develop shared national, regional and international understandings of privacy. So it is no surprise that, unlike American states, Canadian jurisdictions, at all levels, have privacy commissioners mandated to advance privacy interests and comprehensive privacy laws spanning all businesses, rather than being restricted to specific sectors. In an earlier paper [1], I advanced the argument that in the American regulatory framework, privacy interests are more comfortably sheltered under consumer protection measures rather than under fundamental human rights. Privacy within America is thus a commodity that can be subject to market forces. European values of personal control over information, identity and autonomy are so alien to the U.S. that they defy easy comprehension. That tension led to the Clinton-era negotiations between the European Union and the State Department to avoid the threat of suspension of data flows between Europe and the US, and the adoption of a non-legislated Safe Harbor regime to protect personal information.

II. Canada's New Privacy Regime — An Overview

From a European perspective, much of Canada's approach to privacy is familiar. Canada's *Personal Information Protection and Electronic Documents Act*[2] (*PIPEDA)* is a complex statute that is not easy to read and interpret. Its second part, establishing the functional equivalence of electronic records and documents, need not concern us. But to understand the ambiguous state of privacy protection, it is

---

[1] Simon Chester, "The Internationalization of Privacy" (Paper presented at the Canadian Bar Association's Annual Meeting, August 2004) [unpublished].

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

necessary to appreciate the scheme of Part 1, which deals with the protection of personal information and Schedule 1, which imports guidelines from an industry code.

Unlike Quebec law, the Act does not proclaim a broad right to privacy. Instead it imposes responsibilities on those who collect, use or disclose personal information in the course of commercial activities. "Personal information" receives an extremely broad definition: essentially anything that relates to an identifiable human being. "Commercial activities", a term necessary to place the statute under the constitutional shelter of federal trade and commerce, is similarly so broadly described to capture all activities which fall outside governmental, individual, journalistic and not-for-profit domains. This is a statute which by definition applies to a vast range of disparate activities — an insurance company, law firm, video rental, child's summer camp, construction company and book publisher — all of which are considered commercial. Because of the breadth of its field of application, its ground rules for the handling of personal information must necessarily be abstract and somewhat vague. Separate and somewhat inconsistent provisions deal with the collection of data, its use and its disclosure.

In an unusual step to integrate federal law with industry norms that were generally accepted, the statute incorporated the Canadian Standards Association Model Code for the Protection of Personal Information as a Schedule. The move has been controversial as well as unusual because the Model Code was never drafted in statutory form, establishing clearly delineated rights and precise obligations. As we shall see, the courts have struggled to give clear meaning to the Schedule. The Act's administration falls under the Privacy Commissioner of Canada whose role is more one of an ombudsman than a conventional adjudicative tribunal.[3] After investigations, the Commissioner issues findings. The Act's remedial teeth and the Federal Court's oversight are only revealed if a finding is ignored. These cases have been extremely rare. The few compliance surveys to have been conducted of Canadian business have shown very spotty awareness of the statute and quite

---

[3] See J. Stoddart, Cherry-Picking among Apples and Oranges: Refocusing Current Debate about the Merits of the Ombuds-Model under PIPEDA (2006), 44 Can.Bus.L.J.1.

limited changes to comply. The Act had a staggered phase-in and has only applied to all Canadian businesses (except those in Quebec, British Columbia and Alberta, which are regulated by substantially similar provincial laws) since January 1, 2004. Businesses which fall within the domain of federal works and undertakings (such as banks, airlines and telecommunication companies) and whose labour relations fall under the *Canadian Labour Code*, have been governed by the Federal Act since January 1, 2001 wherever they are located. Their employees are also given rights concerning employment information under the Act. This is because of the constitutional limits of the federal Parliament's powers to regulate workplaces. Only if a specific provincial statute governs privacy in employment are other workplaces covered. A constitutional reference to challenge the entire Act is pending before the Québec Cour d'Appel,[4] although there has been virtually no discussion of the progress of this reference in the two years since it was announced.

III. Eighteen Months After: How Have Courts Responded to *PIPEDA*?

Because of the ombudsman-like role of the Privacy Commissioner under *PIPEDA*, the courts were never anticipated to have anything more than an ancillary role, providing enforcement muscle if a business refused to comply with the Commissioner's findings. During the first two years of *PIPEDA* (when it applied only to businesses which fell under the federal works and undertakings category within the Canadian Constitution), twenty applications were made to the Federal Court, the majority of which were discontinued, dismissed, or settled before the court pronounced on the merits. These cases included both de novo applications under section 14 of *PIPEDA* and applications for judicial review.[5]

---

[4] Simon Chester, PIPEDA Reference Raises Vital Constitutional Questions From Canadian Privacy Law Review - Vol.1, No.5, Special Issue - The Quebec Constitutional Challenge to PIPEDA, March 2004

[5] Since the research for this chapter was originally undertaken, a number of other cases have considered various aspects of the Federal Act. See *Mccue* c. *Younes*, (2002) IIJCan 8618 (QC C.S.); *IMS Health Canada* v. *Maheu*, (2003) 24 C.P.R. (4th) 70, 226 F.T.R. 269, 29 C.P.R. (4th) 425, 246 F.T.R. 159; *Glikstein* c. *West Island College*, (2003) IIJCan 1028 (QC C.S.); *Air Canada* c. *Constant*, (2003)

Only four cases resulted in the Federal Court commenting on substantive aspects of *PIPEDA*.[6] Interestingly, most involved the troubling issue of consent with one case about how far video surveillance can be justified in the workplace.

In the *Englander* case[7], the Federal Court of Appeal expressed concern about the form and substance of *PIPEDA*, despairing about applying a strict interpretative analysis of Schedule 1 of *PIPEDA* (which incorporated the Canadian Standards Association Model Code for the Protection of Personal Information[8] by reference as the normative heart of the law) commenting that "because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction".[9] The vague wording of much of the Act left the court with little, if any, guidance in applying it.

IIJCan 1018 (QC C.S.); *BMG Canada Inc*. v. *John Doe* (F.C.), [2004] 3 F.C.R. 241, 239 D.L.R. (4th) 726, 32 C.P.R. (4th) 64, 250 F.T.R. 267 [*BMG Canada*]; *Strategy First Inc. (Bankruptcy), Re,* (2004) CanLII 21470 (QC C.S.); *MEI Computer Technology Group Inc. (Bankruptcy), Re*, (2005) CanLII 11660 (QC C.S.); *Blood Tribe (Dept. of Health)* v. *Canada (Privacy Commissioner)*, [2005] 4 F.C.R. 34; *Dupont Industries Inc. (Faillite), Re*, (2005) IIJCan 10503 (QC C.S.); *Reischer* v. *Love*, (2005) BCSC 580 (CanLII); *R.* v. *Smith*, (2005) BCCA 334 (CanLII); *Innovative Health Group Inc.* v. *Calgary Health Region*, (2005) ABQB 438 (CanLII) ; *Avance Pharma Inc. , Re*, (2005) IIJCan 21273 (QC C.S.); *Lawrence* v. *Toronto Humane Society*, (2005) CanLII 25634 (ON S.C.) ; *Avance Pharma Inc.* c. *Raymond Chabot Inc*., (2005) IIJCan 26781 (QC C.S.); B.M.P. *Global Distribution Inc. et al* v. *Bank of Nova Scotia*, (2005) BCSC 1091 (CanLII); *IMS Health Canada, Limited* v. *Information and Privacy Commissioner*, (2005) ABCA 325 (CanLII); *Fishing Lake First Nation* v. *Paley*, (2005) FC 1448 (CanLII); *Turner* v. *Telus Communications Inc*., (2005) FC 1601 (CanLII)

6 *Eastmond* v. *Canadian Pacific Railway*, (2004) 33 C.P.R. (4th) 1, 254 F.T.R. 169; *Englander* v. *TELUS Communications Inc*. aff'd [2005] 2 F.C.R. 572 (C.A.) [*Englander*]; *L'Écuyer* v. *Aéroports de Montréal*, (2003) 233 F.T.R. 234; *L'Écuyer* v. *Aéroports de Montréal*, [2004] CAF 237 (C.A.).

7 *Englander, ibid.*

8 Canadian Standards Association, "Model Code for the Protection of Personal Information" (Q830-96), online: <http://www.csa.ca/standards/privacy/code/Default.asp?language=English>.

9 *Englander, supra* note 6 at para. 46.

Although *PIPEDA* provides for the publication of summaries of findings concerning the Commissioner's investigations, these have not amounted to the sort of elaboration of jurisprudential or interpretative guidelines that one would have expected from a court's attempts to come to terms with a new statute. The findings tend to be fact specific, without any sustained attempt to develop common themes or principles. In fairness to the Privacy Commissioner's office, the statute did not appear to require the exegesis of conventional interpretation and the former Commissioner, George Radwanski, appeared anxious to preserve flexibility to deal with future cases by issuing fact-bound rulings.

In the year running up to the coming into force of *PIPEDA*, a number of analyses explored the problems that the breadth (and looseness) of some of the language in the statute might pose for civil litigation. Since private lawyers were caught by the breadth of the definition of commercial activities, which is the triggering point for the application of the legislation, there was significant uncertainty about whether the conduct of civil litigation would be transformed. Some commentators predicted chaos, others pointed out discrepancies and inconsistencies in the statute, questioning whether compliance was feasible.

Among the questions raised were:

- What sort of consents should litigators get for the use of personal information?
- Would *PIPEDA* limit the ability to disclose an opposing party's personal information in pleadings (of course without consent)?
- How should litigators deal with witness interviews? Do they have to disclose how any personal information revealed during the interview will in fact be used?
- Would there be problems with surveillance evidence, obtained through a private investigator, if the evidence revealed personal information that had obviously been obtained without the subject's consent?
- Can a law firm make an investigation into whether a potential defendant has enough assets to justify suit — or is judgment proof — and then pass that information on to a US client or another law firm?

- Would the fact that the statutory provisions on disclosing personal information do not match those for collecting or using personal information constrain the extent to which lawyers could receive personal information that others had lawfully collected?
- How should litigators deal with requests to examine personal information contained in litigation files, particularly since the statutory drafting concerning privilege overrides is arguably incomplete? *PIPEDA* spoke about solicitor-client privilege. Did this include litigation privilege?
- Was it significant that the provisions in Section 7(3)(c), exempting disclosure without consent where required to comply with a subpoena, warrant or order or to comply with rules of court concerning documentary production, failed to mention oral examinations?

While there were no clear answers to these questions in the legislation, since 2004, courts have taken a robustly common sense view, reasoning that if Parliament had intended to revolutionize the conduct of civil litigation (leaving aside the constitutional issue of whether this is possible in a federal statute, enacted under the trade and commerce power), its intention was not clearly manifested. Instead the courts have eschewed highly technical or forced interpretations.

The courts did not wait long before moving to a pragmatic view of *PIPEDA*. The first major case dealt with a private investigator[10]. Denise Ferenczy sued her doctor alleging that he had been negligent in mistreating a cyst on her left hand. During the second day of the trial, the defendant's counsel, faced with Ferenczy's inconsistent evidence on cross-examination, tried to introduce video surveillance evidence gathered by a private investigator that showed Ferenczy holding a Tim Horton's coffee cup in her left hand — something she had said she was unable to do as a result of her disability.

The video recording was made after *PIPEDA* had come into force. The court had to consider whether *PIPEDA* allowed the use of such evidence. The Plaintiff's argument was simple. Video surveillance was

---

[10] *Ferenczy* v. *MCI Medical Clinics,* (2004) 70 O.R. (3d) 277 (S.C.J.).

private information collected in the course of commercial activity. She had never consented. *PIPEDA* prohibits the collection of such information. The court went back to evidence first principles. *Prima facie* relevant evidence is admissible except when 1) the probative value of the evidence is outweighed by its prejudicial effect and 2) admission of the evidence would render a trial unfair. The prejudicial effect of admitting the evidence refers to the danger that the evidence will be misused. In this case, a proper limiting instruction would prevent the use of such evidence for improper purposes. Nor would admitting the evidence make the trial unfair, since the plaintiff would be given a chance to provide an explanation, on the basis of which the trier of fact would assess its reliability and weight. *PIPEDA* is not an evidence statute. It does not contain a provision that prohibits admissibility of evidence collected which results in an investigation and subsequent report. In this case, Ferenczy could still lodge a complaint with the Privacy Commissioner.

> "The legislation (*Personal Information Protection and Electronic Documents Act*) is complex and so broadly worded that a reasonable argument could be made to extend its reach so far as to transform both civil and criminal litigation into something very different than it is today."
>
> "If the plaintiff's argument were to be accepted, an accused would be prevented from employing a private investigator to collect information for his or her defence even though the legislation permits other law enforcement agencies to do so. This would be unfair."

One way to avoid this result would be to apply the principles of agency. *PIPEDA* allows an individual to collect information without consent if the information is used for personal or domestic purposes. Applying the law of agency in this case, the video surveillance evidence would be admissible if it was collected by the defendant through an agent for a personal purpose — that of defending himself. This conclusion is consistent with the overall purpose of the Act which is aimed primarily at information collected as a part of commerce.

The judge also tentatively reached for a concept that is controversial in privacy law — implied consent. Dawson J. of the Ontario Superior Court: "A plaintiff must know that by commencing action against a defendant, rights and obligations will be accorded to the parties to both prosecute and defend". By putting the degree and effect of her injury into issue, the plaintiff has given implied consent to the defendant to gather information relating to the veracity of her claim. Since consent is not a defined term in *PIPEDA*, there is nothing to suggest that consent would not encompass implied consent.[11]

"Having reached these conclusions, it is nonetheless my view that the wording of the provisions leaves a lot to be desired in terms of clarity and usefulness. This is particularly so in many situations which can be envisaged that are common to and a part of the fabric of litigation". As one commentator put it:

> Dawson J's *Personal Information Protection and Electronic Documents Act* analysis appears to be a fairly transparent effort to avoid transforming litigation 'into something very different from what it is today'." … "In the end, *Ferenczy* is notable not so much for what was said, but the implications of what was not discussed in any depth, namely the reasonable expectation of privacy and the reasonableness of the surveillance … *Ferenczy* likely reaches the correct result but marginalizes the impact of the *Personal Information Protection and Electronic Documents Act*.[12]

In a Privacy Commissioner Finding dated August 9, 2005, the Assistant Commissioner had to deal with whether the federal Act had been breached when an insurance company used investigation

---

[11] See generally J. Barrigar, J. Burkell and I. Kerr, Let's Not Get Psyched Out on Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information, (2006), 44 Can.Bus.L.J. 54 at 59 et seq.

[12] Anne Uteck,, "Video Surveillance, Evidence and the Personal Information Protection and Electronic Documents Act: A Comment on Ferenczy v. MCI Medical Clinics" (2004) 3 Can. J.L. & Tech 157.

surveillance to defend a court action.[13] A woman who was involved in a motor vehicle accident in 2000, sued the driver of the other car. She ran her own business and claimed that her injuries not only cost her income, but also prevented her from performing her household tasks. A private investigator hired by an insurance company videotaped her. She complained to the Privacy Commissioner but her complaint was rejected as not well founded.

The other driver's insurance company argued that the woman's testimony at her discovery hearing and her medical reports revealed discrepancies and inconsistencies about her injuries. So it hired a private investigator to conduct surveillance on the woman to record and observe her capabilities. The investigator followed the woman for about three weeks, including observing her at home, business, and shopping. Some of activities were videotaped, such as her carrying packages, boxes, leaving her place of business, and driving to the shops. The investigator prepared a report outlining the date that the surveillance took place, the time, location and what was seen. This information, including the videotape, was used in Court. The woman then filed complaints with the Office of the Privacy Commissioner alleging that the insurance company and the private investigator collected her personal information without her knowledge or consent, in breach of the Act. The insurance company's view was that the woman had consented to the collection of her personal information when she filed a claim against the other driver. It had a duty to defend its client and an obligation to verify the truth of the claim, stating that "[I]t would be contrary to the established principle of law if a claimant could put forward a claim and then refuse to consent to the verification of that claim."[14] Assistant Privacy Commissioner Black agreed that, when an individual starts a lawsuit, she or he impliedly consents that the other party may collect information required to defend itself against claim. When the woman's testimony and medical reports revealed discrepancies and were inconsistent with the injuries claimed, the Assistant Commissioner concluded that she gave her implied consent

---

[13] Office of the Privacy Commissioner of Canada, "*PIPEDA* Case Summary #311" (August 9, 2005), online: Commissioner's Findings <http://www.privcom.gc.ca/cf-dc/2005/311_20050809_e.asp>.

[14] *Ibid*.

to the collection of her personal information. Such implied consent does not authorize unlimited access to an individual's personal information, but only relevant to the merits of the case and the conduct of the defence.

Here the collection of personal information was limited to what was necessary for the insurance company to defend its client against the court action. The Act only permits surveillance where the collection is reasonable for the purposes of an investigation or legal proceeding. Collection without consent is permissible if there has been a contravention of a law or a breach of a contract, and clearly no contract existed between the woman and the party she was suing.

Thus, to permit information collection of the type considered in this complaint, the Assistant Commissioner concluded that implied consent exists when any party puts forth questionable evidence in a proceeding which the other party has a legal right or a fiduciary responsibility to verify to defend its interests. This is consistent with Dawson J.'s approach in *Ferenczy*.

In *Clustercraft Jewellery Manufacturing* v. *Wygee Holdings*[15], Ducharme J. rejected an argument that a witness on an examination could decline to produce employee service records since *PIPEDA* prohibited this. Citing s. 7(3)(c) of *PIPEDA*, he held that a Master's order was at a minimum an order made by a court with jurisdiction to compel the production of relevant information.

In the *BMG* file sharing case[16], the Federal Court of Appeal touched on the protection of privacy within the framework of identifying customers of internet service providers. The plaintiffs in a copyright infringement case springing from music file sharing sought to have the internet service providers unmask pseudonymous infringers. At trial, von Finckenstein J. had denied the motion brought by the music industry, holding that the privacy rights of the file sharers were relevant and that disclosure of actual identities should not be ordered. The Federal Court of

---

[15] *Clustercraft Jewellery Manufacturing* v. *Wygee Holdings,* (2004) CanLII 1647 (Ont. SC).

[16] *BMG Canada, supra* note 5.

Appeal agreed with him on the privacy point, while holding that he had erred on the copyright issue.

While in a number of Supreme Court of Canada decisions from the mid-1990s, LaForest J. had grounded an expansive right of privacy in the *Charter of Rights and Freedoms*; with LaForest J.'s retirement one can detect a retrenchment in the Court. On October 29, 2004, the Court reversed the Ontario Court of Appeal's decision in the *Tessling*[17] case holding that using heat detection technology to detect a cannabis grow operation did not constitute an unreasonable search and seizure. Law enforcement authorities had equipped an aircraft with a Forward Looking Infrared camera, capable of detecting unusual heat profiles that might indicate suspicious activities.

In the Court of Appeal, Abella J.A. had followed an earlier United States Supreme Court decision that the use of such a camera breached constitutionally protected rights. She had said that, "the privacy interest in the home extends to heat generated in the home but reflected on the outside". Binnie J., writing for a unanimous court, rejected this reasoning, since the data captured from the infrared camera was only on the exterior: "[E]xternal patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy."

These cases show that while privacy may be a valuable card to play in the game of civil litigation, it is far from being a trump card. This is consistent with the modest impact that privacy has had in Canadian law generally.

IV. The Troubled State of the Tort of Privacy

For reasons I analyzed at length last year in an article in the *Advocates' Quarterly,*[18] Canadian courts have been slow and reluctant to invest much life into the statutory tort remedies that proliferated after

---

17 *R* v. *Tessling,* [2004] 3 S.C.R. 432.

18 See generally Simon Chester, "Zapping the Paparazzi: is the Tort of Privacy Alive and Well?" (2003) 27 Advocates' Quarterly 357.

Dean Peter Burns' seminal article on the tort of privacy.[19] The history of this subject is full of false starts and great expectations. Damage awards have been so low as to make litigation uneconomic.

As for the common law, the courts' approach was typified by decisions like *Roth*[20] and *Wainwright,*[21] in which the separate existence of a privacy tort was denied. In *Wainwright,* humiliating damages for invasion of privacy were refused on grounds that the common law did not recognise such an action. Lord Justice Mummery said:

> "[T]here is no tort of invasion of privacy. Instead, there are torts protecting a person's interests in the privacy of his body, his home and his personal property. There is also available the equitable doctrine of breach of confidence for the protection of personal information, private communications and correspondence."

In Canada, *Hunter* v. *Southam*[22] established that the right to privacy did not just depend upon tort-based notions of trespass but rather was the right to be secure against encroachment upon the citizen's reasonable expectation of privacy in a free and democratic society. Despite this, other decisions, such as *Roth* v. *Roth*[23] and *Palad* v. *Pantaleon*[24] have held that the right to privacy is a general right not dependant on any proprietary right such as nuisance. Thirty years after pioneering decisions such as *Krouse* v. *Chrysler Ltd.,*[25] *Graye* v. *Filiter,*[26]

---

19 Peter Burns, "The Law and Privacy: The Canadian Experience" (1976) 54 Can Bar Rev. 1.

20 *Roth* v. *Roth,* (1991), 4 O.R. (3d) 740. [*Roth*]

21 *Secretary of State for the Home Department* v. *Wainwright*, [2002] Q.B. 1334, aff'd [2003] 4 All E.R. 969 (HL).

22 *Hunter* v. *Southam* , [1984] 2 S.C.R. 145.

23 *Roth, supra* note 20.

24 *Palad* v. *Pantaleon,* [1989] O.J. No. 985.

25 *Krouse* v. *Chrysler Ltd*, [1970] 3 O.R. 135.

Dyne Holdings Ltd. v. *Royal Insurance Co. of Canada,*[27] the courts are still reluctant to strike out pleadings in actions based on the breach of a party's right to privacy because at the very least, it was uncertain whether the right to privacy was recognised at law.

Roth v. *Roth* involved a neighbours' fight over road access to a summer cottage. The court found that the defendants' harassment of the plaintiffs' enjoyment of the property had not reached the level that a reasonable person would regard as offensive and intolerable, so there was no breach of privacy. Mandel J. rejected any general right to privacy "not dependant on trespass to the person or property, nor in my view to proprietary interest as in nuisance." On the question of remedy, Mandel J. said:

> As to whether the invasion of privacy of an individual will be actionable will depend on the circumstances of the particular case and the conflicting rights involved. In such a manner, the rights of the individual as well as society as a whole is [sic] served.

In *Ontario* v. *Dieleman,*[28] the Attorney General of Ontario sought an injunction against anti-abortion protesters near an abortion clinic because of the adverse effects of those working at the clinic, their families and the women attending the clinic. Adams J. stated that "in Canada, privacy interests have been held to be sufficiently compelling to override a *Charter* right."[29] He concluded that interests of personal privacy and health are accommodated by nuisance principles where the adverse effects substantially undermine the reasonable use and enjoyment of property. He concluded:

---

[26] *Graye* v. *Filiter*, (1995) 25 O.R. (3d) 57 (Ont. Gen. Div.).

[27] *Dyne Holdings Ltd.* v. *Royal Insurance Co. of Canada,* (1996) 135 D.L.R. (4th) 142 (P.E.I. C.A.).

[28] *Ontario* v. *Dieleman,* (1994) 117 D.L.R. (4th) 449 (Ont. Gen. Div), additional reasons at (1995) 22 O.R. (3d) 785 (Ont. Gen. Div.).

[29] *Ibid*. at 720.

> From all of the foregoing, it would appear that invasion of privacy in Canadian common law continues to be an inceptive, if not ephemeral legal concept, primarily operating to extend the margins of existing tort doctrine. One significant explanation for this continuing "lack of legal profile" arises from the need to accommodate broad counter privileges associated with free speech and the vast implications of living in a "crowded society."[30]

What can one conclude from this somewhat mixed basket of caselaw?

- While *PIPEDA* may have been touted as giving all Canadians solid privacy protection, the real impact has been much more modest.
- Courts have thus far — and the jurisprudence is in its infancy — eschewed extravagant interpretations of the Act.
- The conduct of civil litigation has not been impeded or transformed. Arguably, inconsistent wording in the Act has been interpreted to avoid any such requirement.
- Parliament will commence a review in 2006 to see how the Act is working and whether changes are required.
- Also in 2006, the constitutionality of the Act will be the subject of a reference hearing, and may even be adjudicated.
- Although the European Commission has deemed Canadian law to provide comparable protection to that mandated under European norms, the reality is that in Europe privacy is a right more robustly protected and more creative approaches to privacy claims and remedies have been embraced.

This can best be explored by comparing the somewhat anomic state of the tort of privacy in Canada with decisions in Europe.

In my earlier paper[31], I explored the extraordinarily low level of damages that have been awarded in Canadian privacy cases over the last thirty years. The paucity of cases is revealing. We now move to consider

---

30 *Ibid*. at 688.

31 *Supra* note 17.

four European cases, three involving famous celebrities. But let's start with a Lutheran parishioner whose enthusiasm to welcome first communicants with an informative website led her to prosecution and notoriety.

A. The Case of the Welcoming Parishioner

In November 2003, the European Court of Justice handed down its first case interpreting the substantive reach of the European Data Privacy Directive.[32] It did so in a case whose facts are as sympathetic as the action of the regulators is surprising.

Bodil Lindqvist was a volunteer in a Swedish church. To prepare parishioners for a first communion, she set up a web page with information about herself and eighteen other volunteers in the parish. She included their first names and sometimes their full names, going on to describe the work each did in mildly humorous terms. In some cases, she provided telephone numbers and contact information. She also mentioned that one of her team members had injured her foot and was working part-time on medical grounds.

Lindqvist had not asked her colleagues for permission nor had she notified the Swedish Data Protection Authority that she was intending to put up the website. One of her colleagues asked her to remove the web site, and she took it off the server. However, the Swedish Data Protection Authorities commenced criminal proceedings against her, resulting in a fine of approximately Can. $600 (Swedish Krona 4000), for processing personal data without notifying the Authority in writing, for transferring data outside Sweden without authorization and for processing sensitive personal information (the line about the foot and the part-time work). Lindqvist appealed to the Gota Court of Appeal. She argued that:

- Hosting information on an internet website does not amount to processing personal data;

---

[32] *Lindqvist* v. *Åklagarkammaren i Jönköping*, C-101/01, (2003) online: <http://www.cr-international.com/docs/2003_ecj_bodil_lindqvist_6_11_2003.pdf>. Also see Bodil Lindqvist's home website: http://biphome.spray.se/mors/.

- Hosting information on a website does not amount to transferring data outside her home country to a third country;
- The *Data Protection Directive* was not intended to apply to non-profit activities;
- The sanctions she was facing for violating the data protection law violated her freedom of expression; and
- The sanctions were disproportionate to the harm done.

The Gota Court of Appeal referred several questions to the European Court asking it to clarify the correct interpretation of the *Data Protection Directive*.

When the Court handed down its decision in late 2003, it gave an interpretation to the Directive that surprised even privacy advocates. It rejected all but one of Lindqvist's arguments. Posting individuals' names and phone numbers did indeed constitute the processing of personal data. The directive did apply to Lindqvist's postings, even though she was engaged in non-profit activities. Once personal data is posted on the Internet, it is available to an infinite number of people, and accordingly there can be no resort to an exception for personal or household activities. Lindqvist did however win on the jurisdictional point. There was no evidence that anyone outside of Sweden had accessed the information on the website. Merely posting personal data on the internet does not subject persons to the legal regime governing the trans-border transfer of personal data unless they actually send the personal information to internet users who did not intentionally seek access to the web pages, or used a web server located outside Europe.

Ms. Lindqvist may be an unlikely figure to have established such ground-setting jurisprudence, but her case has quickly led to other activities by privacy regulators, building upon the Court's interpretation. In Norway, privacy authorities recently announced that they would pursue website operators displaying photographs of individuals taken without their prior consent. And privacy compliance could prove onerous and expensive. General Motors had to spend 6 months before it could post

contact information for its staff on the GM intranet, satisfying a privacy regulator's objections.[33]

B. The Case of the Cocaine-Addicted Supermodel

Faced with fierce competition between an untrammelled tabloid press anxious for access to the private life of the famous or notorious and the desire of the rich and famous to want to be alone, the English courts are fashioning a unique remedial doctrine which straddles the law of privacy: exploitation of personality and breach of confidence. On May 6, 2004 the House of Lords,[34] by a 3-2 majority decided in favour of super-model Naomi Campbell, in her action against the Daily Mirror. Super-model Naomi Campbell had a cocaine problem. She was getting help at Narcotics Anonymous in King's Road in Chelsea. As she left the Narcotics Anonymous meeting one night, clad in a singularly unfashionable woolly hat, she was surprised by a Daily Mirror photographer who took a series of pictures. Shortly afterwards, the Daily Mirror ran an expose, talking about her battle against drug addiction. The story was not unsympathetic, but did show the photographs. Naomi Campbell sued the Daily Mirror for breach of confidence. At trial, Morland J. awarded her £3,500, despite the fact that he found that she lied to the media about her addiction. The paper appealed successfully to the Court of Appeal, which held that the paper was entitled to expose the model's lie that she did not take drugs, and that disclosing that she was attending Narcotics Anonymous did not constitute a breach of confidence.

The model then appealed to the House of Lords. The Court had earlier decided against recognizing a free standing tort of privacy, but it nevertheless held that the *Human Rights Act* did provide her with a remedy. Under Article 8 of the *European Convention on Human Rights*,

---

[33] David Scheer "Europe's New High-Tech Role: Playing Privacy Cop to the World" *Wall Street Journal* (October 10, 2003).

[34] *Campbell* v. *MGN Limited*, [2002] EWCA Civ 1373, leave to appeal to H.L. granted, [2004] UKHL 22, [2004] 2 All E.R. 995, online: The United Kingdom Parliament <http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm>.

Campbell had a right to respect for her private life. The question was whether the information about her attending Narcotics Anonymous would be regarded as private rather than public. The test was whether disclosure of the information would give substantial offence to a reasonable person of ordinary sensibility placed in a similar position. Once the information is found to be private, the Court has to consider the balance between Article 8 privacy considerations and Article 10 freedom of expression considerations. Two of the judges felt that the Mirror's freedom of speech should govern.[35]

The majority however was troubled by the fact that the information was medical information, whose disclosure had the potential to cause harm, and also that the photograph had been published. The mere facts of the story were true — what gave offence was the photograph. The Lords held that the fact that someone could be seen by anybody on a public street does not mean that pictures can be taken of them and circulated without consideration for the private life of the subject.

In *Campbell* v. *MGN*,[36] Lord Nicholls noted that the law of breach of confidence has been adapted to embrace an aspect of invasion of privacy — that of wrongful disclosure of private information. He also stated that Articles 8 and 10 of the *Human Rights Act* now play their part in the redefinition of the cause of action for breach of confidence. Lord Nicholls held:

> "The continuing use of the phrase 'duty of confidence' and the description of the information commented as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private". … "Essentially the touchstone of private life is whether in

---

[35] A Canadian observer would note that Canada's privacy legislation expressly excludes journalistic activities. Nevertheless, the English doctrinal innovations might well be available in the right Canadian case.

[36] *Campbell* v. *MGN,* [2004] 2 All E.R. 995.

> respect of the disclosed facts the person in question had a reasonable expectation of privacy."

Campbell's case cost £1 million, an extraordinary amount for a photograph that was essentially accurate. The Daily Mirror described the Court's decision as "a very good day for lying, drug-abusing prima donnas who want to have their cake with the media, and the right to then shamelessly guzzle it with their Cristal champagne".

The paper was considering an appeal, when the third of the cases was released, this time involving a minor European Royal.

C. The Case of Princess Caroline

Princess Caroline of Monaco is the daughter of the late Prince Rainier III and Grace Kelly. For the last ten years, she has been engaged in litigation against German tabloid publications, which published celebrity pictures. Indeed, her husband, Prince Ernst August von Hannover was once convicted of attacking a photographer. Princess Caroline sued to persuade Germany's Federal Constitutional Court to stop the pictures appearing in three magazines: Bunte, Neue Post and Freizeit Revue. The Constitutional Court on December 15, 1999 upheld an injunction prohibiting the publication of photographs of Princess Caroline with her children on the grounds that children had a greater right to expect privacy. But they held that Princess Caroline was undeniably a figure of contemporary society and thus of general interest, and thus had to expect publication of photographs taken in a public place even if they showed her in scenes from her daily life (shopping, skiing or on a beach) rather than engaged in official duties.

Appealing that decision to the European Court of Human Rights,[37] Princess Caroline won a significant victory:

---

[37] *von Hannover* v. *Germany* (2004), E.C.H.R. 294, online: European Court of Human Rights <http://www.worldlii.org/eu/cases/ECHR/2004/294.html>.

> "the Court considers that the public does not have a legitimate interest in knowing where [Princess Caroline] is and how she behaves generally in her private life — even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public".

The fundamental principle upon which future European privacy litigation would turn is "the fundamental importance of protecting private life from the point of view of the development of every human being's personality". That protection extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection of and respect for their private life. This is the constitutionalization of the right of privacy which LaForest J. of the Supreme Court of Canada has been advocating.

D. The Case of the Uninvited Photographer at a Celebrity Wedding

In November 2000, Michael Douglas and Catherine Zeta Jones were married in New York. Prior to the event, they had entered into an agreement with the UK celebrity magazine, *O.K.!* to sell the rights for the exclusive publication of pictures of the event.

On the wedding day, a stranger managed to circumvent all security measures and sneak into the event. He took some pictures of dubious quality and sold them to *O.K.!*'s competitor *Hello!*. The Douglases and *O.K.!* sought an injunction to prevent *Hello!* from publishing the photographs, arguing breach of confidence and invasion of privacy. The publication of unauthorised photographs of a celebrity wedding by a magazine infringed the law of confidence. The Court dismissed the appeal of the judgment, which found in favour of the couple based on commercial confidence. The Douglases had taken steps to ensure that their wedding was a private event and that no unauthorised photographs were published. A rival paper, *Hello*, was aware of this and was also aware of the fact that the Douglases intended to exploit their private wedding commercially by publishing authorised photographs in *O.K.!*. *Hello* had deliberately obtained photographs, knowing that such

photographs were unauthorised and published them to the detriment of the Douglases, causing them commercial loss. As a result, *Hello* was liable to the Douglases for breach of commercial confidence. The couple was entitled to modest damages for invasion of privacy and damage to their commercial interest in the information about their wedding against the infringing publishers, but the law of confidence did not extend to the publishers who had paid for the exclusive right to publish authorised photographs of the wedding. An injunction was granted by the lower court but overturned by the Court of Appeal.

The Court of Appeal undertook the first detailed analysis of the impact of the *Human Rights Act* on the protection of privacy afforded by English law when discharging the interlocutory injunction. Brooks L.J. concluded that it was difficult to say whether the *Human Rights Act* required the English courts to develop a law of privacy — but he ducked the issue. Sedley L.J. gave a more affirmative answer, "we have reached a point at which it can be said with confidence that the law recognizes and will appropriately protect a right of personal privacy."[38] Keene L.J. remarked that whether the resulting liability is described as breach of confidence or privacy, it is nothing more than a question of choosing labels. In April 2003,[39] Lindsay J. held that there had been an infringement and that the Douglases' publicity rights in a private event were akin to commercial trade secrets and awarded them the almost nominal sum of £14,500 in damages. Considering that the litigation had involved a million pounds in legal fees, it was scarcely an economic return (though one suspects that for Hollywood actors, almost all publicity is good publicity).

Hello! appealed to the Court of Appeal.[40] The main issue about privacy was whether the photographs published by *Hello!* infringed rights of confidence or privacy enjoyed by the Douglases. This raised the

---

38 [2005] 2 FCR 487 para 110.

39 *Douglas* v. *Hello! Ltd.* [2003] 3 All E.R. 996 (Ch. Div.).

40 *Douglas and others* v. *Hello Ltd and others* [2005] EWCA Civ 595, online: England and Wales Court of Appeal (Civil Division) Decisions <http://hei.unige.ch /~clapham/ hrdoc/docs/Douglas%202005%20CA.html>.

interesting question of the interrelationship between confidentiality and privacy, an issue that arose in England because of a human rights statute, but which will surely be explored in Canada.

The court concluded:

> "in so far as private information is concerned, we are required to adopt, as the vehicle for performing such duty as falls on the courts in relation to Convention rights, the cause of action formerly described as breach of confidence…The court should, in so far as it can, develop the action for breach of confidence in such a manner as will give effect to both Article 8 and Article 10 rights…In particular, when considering what information should be protected as private pursuant to Article 8, it is right to have regard to the decisions of the ECTHR. We cannot pretend that we find it satisfactory to be required to shoe-horn within the cause of action of breach of confidence claims for publication of unauthorized photographs of a private occasion.[41]

The Court considered whether the law of confidence could cover the Douglases' right of commercial interest in information about their wedding. The court saw no reason why not:

> We can see no reason in principle why equity should not protect the opportunity to profit from confidential information about oneself in the same circumstances that it protects the opportunity to profit from confidential information in the nature of a trade secret.

Hello was liable to the couple, but not to its rival magazine which had bought the Douglases' exclusivity. The paper succeeded on the argument that while they had breached the Douglases' confidentiality, that confidentiality was personal and did not extend to the paper to whom they had sold exclusive rights. As such, the paper could not recover for the

---

41 *Ibid.* at para. 53.

losses it suffered from the breach. A business cannot rely on invasion of privacy or breach of confidentiality of another as the basis for losing out to competitors over the commercial exploitation of such invasion or breach.

> We agree that the Douglases were entitled to complain about the unauthorised photographs as infringing their privacy on the ground that these detracted from the favourable picture presented by the unauthorised photographs and causes consequent distress.

However, the Court said that rights in confidential or private information, such as photos of a wedding, which can be commercially exploited, but are protected only by privacy and breach of confidence laws, are not transferable. Nor do they amount to intellectual property rights. The paper, which had a license only to publish the authorised photographs — the copyright of which was retained by the Douglases — did not have a right to sue its competitor and the £1 million award was set aside.

In rejecting *O.K.!*'s claims, the court held that privacy rights were personal and non-transferable. The court also held that the interlocutory injunction should not have been lifted: "[O]nly by the grant of an interlocutory injunction could the Douglases' rights have been satisfactorily protected."[42] Through this, the court recognised that an injunction was perhaps the only way to safeguard privacy rights. The appeal against the judgment in favour of the Douglases was dismissed.

The exclusive deal with the Douglases did not give *OK!* a property right over the photographs it had purchased, or over the details of the wedding. All it had was a nine-month exclusive license agreement. As a result, *OK!*'s loss from lost sales, which the court said was *Hello*'s responsibility, is irrecoverable. The judgment stated:

> The grant to *OK!* of the right to use the approved photographs was no more than a license, albeit an exclusive

---

42 *Ibid*. at para. 259.

> license, to exploit commercially those photographs for a nine-month period. This license did not carry with it any right to claim, through assignment or otherwise, the benefit of any other confidential information vested in the Douglases.
>
> The Court of Appeal summarized the applicable principles:
>
> - "Where an individual ('the owner') has at his disposal information which he has created or which is private or personal and to which he can properly deny access to third parties, and he reasonably intends to profit commercially by using or publishing that information, then a third party who is, or ought to be, aware of these matters and who has knowingly obtained the information without authority, will be in breach of duty if he uses or publishes the information to the detriment of the owner. We have used the term 'the owner' loosely."
> - "We have concluded that confidential or private information, which is capable of commercial exploitation but which is only protected by the law of confidence, does not fall to be treated as property that can be owned and transferred."

These decisions contrast markedly with precedents in North America. They reveal that Europeans attach a much higher normative priority to individual privacy. While the Court in both the Princess Caroline and Naomi Campbell cases notes the need to respect freedom of the press, in practice, the media can take scant comfort from these cases. Indeed, to an external observer it looks as if Europe's privacy laws really have teeth.

V. Conclusion

This brief survey illustrates that privacy has yet to impinge much upon the conduct of Canadian civil litigation or the rights and obligations of parties and witnesses within it. Over the next few years, however, one could easily imagine our courts being faced with difficult issues involving the balancing of competing interests and (inevitably) the compromise of cherished principles.

We may hazard some guesses at how those conflicts may emerge:

- Judges will need to rethink the content of open justice in a globally accessible information environment.
- As more court records become generally available over the Internet, courts will need to be sensitive to whether personal details of private life or financial information should be disclosed. There have been incidents in the United States where social security numbers and account information have been disclosed affording ample opportunity for fraud.
- Litigants may start to request that key information be anonymized or redacted once its purpose has been served.
- Parties will need to be aware of the problems of metadata — concealed information about the creation of the computer record — when documents are posted on court websites in native format (Microsoft Word files for example). Deploying metadata strippers or converting to Adobe Acrobat portable document format should become standard.
- We should expect to see increasing resort to arbitration and other forms of alternative dispute resolution where confidentiality can be contractually guaranteed.
- Judges should start to explore the emerging English law on the intersection between privacy and confidentiality.
- We have certainly not seen the last of privacy litigation, although the limits imposed in the last thirty years will necessarily be rethought.
- The Privacy Commissioner will need to explore how the concept of "commercial activities" squares with the traditional conduct of civil litigation.