

LAW REFORM COMMISSION OF SASKATCHEWAN
CONSULTATION PAPER: RENEWING THE PRIVACY ACT

JULY, 2009

I. INTRODUCTION

Privacy is valued in our society. But in the age of the Internet, identity theft, and electronic surveillance, most of us have the sense that privacy is increasingly under threat. A recent special issue of *Scientific American* on privacy and technology observed that

A cold wind is blowing across the landscape of privacy. The twin imperatives of technological advancement and counter terrorism have led to dramatic, and possibly irreversible changes in what people can expect to remain of private life.¹

Although many actions that compromise privacy may be illegal, in most provinces there is no general legal rule that invasions of privacy are inherently wrong. Saskatchewan, along with British Columbia, Manitoba, and Newfoundland, is an exception. The Saskatchewan *Privacy Act* was adopted in 1972.² Its principal innovation was the creation of a tort of invasion of privacy. A tort is a civil wrong. An individual whose privacy has been wrongfully invaded may sue for damages.

The privacy acts were adopted at a time when public concern about wiretapping and other forms of electronic eavesdropping (new technologies at the time) focused attention on protection of privacy. *The Privacy Act* is a relatively short piece of legislation, setting out the general principle that invasion of privacy is actionable in court unless it can be justified. It was anticipated that the courts would develop the new tort, paralleling experience in the United States, where a tort of invasion of privacy was extracted from the *Bill of Rights* and elaborated by

¹ Peter Brown, "Privacy in an Age of Terabytes and Terror," *Scientific American*, September, 2008.

² See now *The Privacy Act*, R.S.S. 1978, c. P-24. The other provincial privacy acts are British Columbia: *Privacy Act*, R.S.B.C. 1996, c. 373; Manitoba: *Privacy Act*, C.C.S.M. c. P125; Newfoundland: *Privacy Act*, R.S.N.L. 1990, c. P-22. The Uniform Law Conference of Canada has also adopted a model *Uniform Privacy Act*.

the courts. However, this did not happen. There have been very few cases under the Saskatchewan *Privacy Act* or its counterparts in other provinces. This has led some commentators to describe the *Privacy Acts* as dead letters.³

In the years since *The Privacy Act* was adopted, concerns about privacy have not diminished. In fact, public concern appears to be increasing. A report issued in 2003 observed that “privacy in Canada is at a crucial point — likely to change in the near future and already a hot topic for discussion, debate and press interest.” The report identified new information technologies as a primary reason for concern, and gave several examples of incidents that have attracted public attention:

From January 18 to 28, 2003 there has been widespread press coverage about a new Royal Bank initiative that would result in personal financial information being shared across the Canadian/American border, a scandal involving gun registry documents discovered unshredded in a dumpster, [and] the unexplained theft of a hard drive storing the unencrypted personal financial records of 180,000 Canadians owned by major insurance company. . . .⁴

But it should not be thought that new information technologies are the only reason for concern. An American public interest group, the Privacy Rights Clearinghouse, lists 17 “current issues,” including biometrics, video surveillance, workplace monitoring, financial privacy, and medical records confidentiality.⁵

The Privacy Act is potentially broad enough to encompass new threats to privacy as they emerge. Because it is a law of general application, it can (at least in principle) be adapted to new, unforeseen challenges. For this reason, it may be premature to abandon the approach to protection of privacy taken by the *The Privacy Act*.

However, the price paid for the generality of the legislation is lack of specificity and certainty.

3 D Flaherty. “Some reflections on privacy in technology.” 26 *Manitoba Law Journal* 1998-1999, 219.

4 Caryn Mladen, “Privacy in Canada,” A Report of Research on Privacy for Electronic Government, 2003.

5 “Privacy Today: A Review of Current Issues,” Privacy Rights Clearinghouse, March 2001-September 2008 (privacyrights.org).

The Saskatchewan *Privacy Act* has been described as “very general and vague.”⁶ The Saskatchewan *Act* does attempt to provide some guidance by referring directly to some of the most serious threats to privacy when it was adopted. But the focus of concern has shifted since it was enacted. Although wiretapping and eavesdropping are still problems, and are in fact now technologically more sophisticated,⁷ other issues now seem more pressing. *The Privacy Act* does not directly address them. Certainly, both new information collection and retrieval systems require more specific and detailed regulation than *The Privacy Act* could provide by itself. In recent years, the focus of efforts to protect privacy has been on specific legislation, directed primarily at regulation of disclosure of personal information, such as the Saskatchewan *Freedom of Information and Protection of Privacy Act*⁸ and the Federal *Personal Information Protection and Electronic Documents Act*.⁹

But despite adoption of more specific protections and detailed regulations than the privacy acts provide, there are still gaps in the scope of the more recent legislation. As technology changes and the focus of public concern shifts, unexpected new problems can be expected to emerge. It can be argued that *The Privacy Act* remains a useful complement to more detailed legislation addressing specific privacy concerns.

This consultation paper is intended to provide background and discussion of two questions: First, is there a place for a broad, open-ended tort of invasion of privacy? Second, can *The Privacy Act* be improved to better define the scope of the tort to make it a more attractive remedy for invasion of privacy?

We welcome your comments and suggestions.

6 I.J. Turnbull et al, *Privacy in the Workplace, The Employment Perspective*, (The Canadian Privacy Institute: CCH).

7 See Whitfield Diffie and Susan Landau, “Brave New World of Wiretapping,” *Scientific American*, September, 2008.

8 S.S. 1990-91, c. F-22.01.

9 S.C. 2005, c. 5.

II. PRIVACY LAW IN SASKATCHEWAN: AN OVERVIEW OF THE CURRENT LAW

1. *The Privacy Act*

The Privacy Act makes intentional invasion of privacy a tort:

2 It is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person.

The common law recognized no general tort of invasion of privacy, though some other torts (such as breach of confidence and defamation) provided some protection for privacy rights. Although some decisions in other jurisdictions suggest that a common tort of invasion of privacy may now be evolving,¹⁰ as recently as 1996, the Saskatchewan Court of Queen's Bench stated that "it is questionable whether such a right [a common law right of privacy] exists," and observed that "this likely accounts for enactment of *The Privacy Act*."¹¹

The most difficult challenge in formulating a tort of invasion of privacy is defining limits. Privacy is not an absolute. Normal social intercourse reveals information about the participants; no one can expect to avoid the gaze of neighbours, whether it is curious or disinterested. Business transactions often require disclosure of private information. Security concerns require that not all secrets are protected. The *Act* does not attempt to define privacy. As the British Columbia courts have observed, any useful definition of privacy must be elastic.¹² No doubt the

10 See below.

11 *Peters-Brown v. Regina District Health Board* [1996] 1 W.W.R. 337 (Sask. Q.B.); aff'd. [1997] 1 W.W.R. 638 (Sask. C.A.).

12 *Davis v. MacArthur* (1969), 10 D.L.R. (3d) 250 (B.C.S.C.) (Reversed on other grounds).

intention of the drafters of the privacy acts was to leave the new tort as open-ended as possible, to be developed by the courts.¹³ It was anticipated that the courts would identify appropriate limits, but in some cases, the drafters of the legislation provided some guidance. This guidance took several forms.

1. Exclusion of unintentional violations of privacy. That innocent or even negligent invasions of privacy are not actionable is clear from inclusion of wilfulness and absence of claim of right as elements of the tort. The term “wilfully” has been interpreted in the British Columbia *Privacy Act* to mean that the defendant knew or ought to have known that an act would violate the privacy of the plaintiff, not merely that the defendant voluntarily performed the offending act. “Claim of right” has been interpreted to mean “an honest belief in a state of facts which, if it existed, would be a legal justification or excuse.”¹⁴ These interpretations appear to have been adopted in Saskatchewan in *Peters-Brown v. Regina District Health Board*.¹⁵ The court observed that “there are no Saskatchewan decisions construing this act,” and approved what it characterized as the “narrow interpretation” given the privacy acts in British Columbia and Manitoba. In the *Peters-Brown* case, the plaintiff sought damages from a hospital for “circulating confidential patient information implying she suffered from an infectious disease.” Although the court found that the hospital had breached a statutory duty to maintain the confidentiality of medical records,¹⁶ it found no violation of *The Privacy Act*:

On the facts as presented, it cannot be said the hospital "wilfully and without claim of right" violated the privacy of the plaintiff. . . . Internal distribution of the plaintiff's private information was wilful in the sense that it was done

13 This was certainly true in the case of the British Columbia *Privacy Act*, the first of the *Privacy Acts* to be adopted (1968). The Attorney General of the province explained that the legislation was “worded in such a way as to leave the legal definition of privacy in a specific case to the discretion of the court.” See discussion in British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.

14 *Hollinsworth v. BCTV* (1998), 59 B.C.L.R. (3d) 121 (C.A.).

15 [1996] 1 W.W.R. 337 (Sask. Q.B.); aff'd. [1997] 1 W.W.R. 638 (Sask. C.A.).

16 *The Hospital Standards Act* R.S.S. 1978, c. H-10. This confidentiality requirement has been superceded by new legislation governing medical records. See below.

intentionally by the hospital. However, there was never an intention to violate the plaintiff's privacy. Moreover, there was a "claim of right". The aim of the hospital was to safeguard its employees, and it did not mean thereby, to infringe the rights of the plaintiff by revealing confidential patient data. Quite the opposite. The hospital intended to preserve secrecy by limiting the circulation to restricted, non-public areas. The only persons who were entitled to see the list were in turn, sworn to secrecy.

2. *Statutory examples of violations of privacy.* The Saskatchewan *Privacy Act* includes a restricted list of "Examples of violation of privacy:"¹⁷

3 Without limiting the generality of section 2, proof that there has been:

- (a) auditory or visual surveillance of a person by any means including eavesdropping, watching, spying, besetting or following and whether or not accomplished by trespass;
- (b) listening to or recording of a conversation in which a person participates, or listening to or recording of messages to or from that person passing by means of telecommunications, otherwise than as a lawful party thereto;
- (c) use of the name or likeness or voice of a person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of gain to the user if, in the course of the use, the person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person; or
- (d) use of letters, diaries or other personal documents of a person;

without the consent, expressed or implied, of the person or some other person who has the lawful authority to give the consent is prima facie evidence of a violation of the privacy of the person first mentioned.

As noted above, the list is weighted toward the privacy issues most prominent in the late 1960s

¹⁷ The Manitoba and Newfoundland, but not the British Columbia, *Acts* include similar examples.

and 70s, when the privacy acts were adopted. Eavesdropping and wire tapping were novel issues at the time, products of the first generation of electronic devices facilitating invasion of privacy. In fact, the British Columbia *Privacy Act*, the first in Canada, was adopted on the on the recommendation of an inquiry into a high-profile case involving wiretapping of a trade union.¹⁸ Misappropriation of personality, recognized in clause (c) of the Saskatchewan act, was a topical issue. It was included despite the fact that it was one of the few examples of violation of privacy that was actionable at common law.¹⁹ In retrospect, it is perhaps the limited scope of the list that is most remarkable.

3. *Factors for the court to consider.* The *Act* also conditions the definition of actionable violations of privacy by setting out “Considerations in determining whether there is a violation of privacy:”

6(1) The nature and degree of privacy to which a person is entitled in any situation or in relation to any situation or matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others.

(2) Without limiting the generality of subsection (1) in determining whether any act, conduct or publication constitutes a violation of the privacy of a person, regard shall be given to:

- (a) the nature, incidence and occasion of the act, conduct or publication;
- (b) the effect of the act, conduct or publication on the health and welfare, or the social, business or financial position, of the person or his family or relatives;
- (c) any relationship whether domestic or otherwise between the parties to the action; and
- (d) the conduct of the person and of the defendant both before and after the act, conduct or publication, including any apology or offer or amends made by the defendant.

¹⁸ See R.A. Sargent (Commissioner), *Report of the Royal Commission of Inquiry into Invasion of Privacy* (Victoria: The Queen’s Printer, 1967).

¹⁹ See *Krouse v. Chrysler Canada Ltd.* (1973), 40 D.L.R. (3d) 15 at 28 (Ont. C.A.).

Section 6(1) makes it clear that whether an act amounts to a violation of privacy depends on the context, and likely on the normal expectations of citizens in differing contexts. The British Columbia Law Institute, reviewing decisions on the parallel language in the British Columbia *Act*, suggests that

[The] section . . . recognizes that normal social interaction requires the interest in privacy to be balanced against the legal rights of others. The ultimate degree of privacy cannot be expected on all occasions and under all circumstances. Outside the confines of a dwelling or other enclosed private space, some degree of observation by others is inevitable. British Columbia courts have held that the degree of privacy to which a person is entitled for the purpose of the Act is greatest where the expectation of privacy is greatest. Expectations of privacy would normally be highest in the home. They would be incrementally less in less private settings.²⁰

In one British Columbia case, it was held that a television crew did not violate privacy when it filmed and broadcast an incident on the plaintiff's parking lot because the lot was open to public view. The Institute concluded that the decision stands for the general proposition that "there can be no reasonable expectation of privacy in a place normally open to public view, regardless of the nature of the place."²¹

4. Defences. Finally, the *Act* sets out certain defences:

4(1) An act, conduct or publication is not a violation of privacy where:

- (a) it is consented to, either expressly or impliedly by some person entitled to consent thereto;
- (b) it was incidental to the exercise of a lawful right of defence of person or property;
- (c) it was authorized or required by or under a law in force in the province or by a court or any process of a court; or

²⁰ British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007, citing *Getejanc v. Brentwood College Association* (2001), 6 C.C.L.T. (3d) 261 (B.C.S.C.) and *Milner v. Manufacturers Life Insurance Company*, [2005] I.L.R. 1-4479.

²¹ See *Silber v. BCTV* (1986), 69 B.C.L.R. 34 (B.C.S.C.).

- (d) it was that of:
 - (i) a peace officer acting in the course and within the scope of his duty; or
 - (ii) a public officer engaged in an investigation in the course and within the scope of his duty;and was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of trespass;
- (e) it was that of a person engaged in a news gathering:
 - (i) for any newspaper or other paper containing public news; or
 - (ii) for a broadcaster licensed by the Canadian Radio-Television Commission to carry on a broadcasting transmitting undertaking;and such act, conduct or publication was reasonable in the circumstances and was necessary for or incidental to ordinary news gathering activities.

(2) A publication of any matter is not a violation of privacy where:

- (a) there were reasonable grounds for belief that the matter published was of public interest or was fair comment on a matter of public interest; or
- (b) the publication was, in accordance with the rules of law relating to defamation, privileged;

but this subsection does not extend to any other act or conduct whereby the matter published was obtained if such other act or conduct was itself a violation of privacy.

These defences are for the most part straightforward matters of policy, likely implied by section 6 in any event (e.g. reasonable actions of the police and media), or necessary to prevent conflict with other legal rules (e.g. law of libel). The most open ended is perhaps clause 4(1)(b), referring to actions “incidental to the exercise of a lawful right of defence of person or property.” A British Columbia case suggests the difficulty in defining the limits of this defence. The defendant in this case intercepted cell phone communications of a neighbour, and justified doing so on the grounds that the neighbour had threatened him some time earlier. The court, not without some misgivings, held the the defence failed in this case.²²

2. Recent legislation protecting privacy

The Privacy Act was adopted before current information technologies were developed. The

22 *Watts v. Klaemt*, 2007 BCSC 662.

examples of violations of privacy contained in the *Act* hardly touch on many of the contemporary issues. Recent provincial and federal privacy legislation, on the other hand, responds directly to concerns about information technologies. In Saskatchewan *The Freedom of Information and Protection of Privacy Act*,²³ and *The Local Authority Freedom of Information and Protection of Privacy Act*,²⁴ both adopted in 1990-91, are administered by the Information and Privacy Commissioner of Saskatchewan. The Commissioner also administers *The Health Information Protection Act*,²⁵ adopted in 1999. These *Acts* govern personal information held by the public sector. They are similar to legislation in other Canadian jurisdictions.

Unlike *The Privacy Act*, the newer legislation provides specific rules and guidelines governing the activities they are intended to regulate. They are examples of the “comprehensive code” approach recommended by some law reform agencies as an alternative to the privacy acts.²⁶ In addition, the legislation mandates proactive enforcement through privacy commissioners appointed under the legislation. Almost all provinces and the federal government regulate the use of personal data by government. The Media Awareness Network has summarized this aspect of the new legislative framework:

In Canada, federal and provincial laws regulate the government's collection, use and storage of personal information by both levels of government. These laws guide the type of information the government can collect, and how such information can be used. They also allow Canadian citizens to access, challenge and correct information about ourselves.

Every province and territory in Canada (except for Newfoundland) has guidelines to protect personal information held by government departments and agencies. The provincial and territorial privacy acts guarantee individuals' rights to view and correct their personal information. The acts are administered and overseen by an independent commissioner or ombudsperson, with the authority to investigate complaints.

The federal *Privacy Act*, in place since 1983, protects the personal information collected by government institutions. Essentially, the *Privacy Act* is a code of

23 S.S. 1990-91, c. F-22.01.

24 S.S. 1990-91, c. L-27.1.

25 S.S. 1999, c. H-0.021.

26 See for example, Ontario Law Reform Commission, *Report on Protection of Privacy in Ontario*, 1968.

ethics for the government's handling of our personal information. The *Privacy Act* ensures that Canadians can access information collected about them, and can challenge the accuracy of the information. The *Privacy Act* is overseen by the Privacy Commissioner of Canada, which has the authority to investigate complaints.²⁷

The federal *Personal Information Protection and Electronic Documents Act*,²⁸ adopted in 2005, and similar legislation in some provinces, extends the protection of the federal *Privacy Act* to the private sector. Saskatchewan does not yet have comprehensive legislation governing personal information held by the private sector, but the federal legislation has application in the province:

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) addresses the collection, storage and use of personal information by organizations in the private sector. Its provisions apply to information collected, used or disclosed by federally regulated agencies, such as telecommunications companies, ISPs, broadcasters, airlines and banks. PIPEDA also applies to federally regulated companies that conduct business online; and it extends to businesses in Nunavut, the Yukon and the Northwest Territories. . . .

Unlike voluntary industry codes, PIPEDA is enshrined in law, and overseen by the Privacy Commissioner of Canada.²⁹

The federal *Personal Information Protection and Electronic Documents Act* has considerable impact on businesses and other private sector organizations operating in Saskatchewan. In addition to applying to activities within federal jurisdiction, such as banking and railways, it applies to any business within joint federal and provincial jurisdiction, presumably including all federally-incorporated companies. In addition, any disclosure of information across provincial borders appears to be caught by the legislation.³⁰ However, the federal government may exempt

27 R.S.C. C. P-51. See “Canadian Privacy Legislation,” Media Awareness Network, 2008.

28 S.C. 2005, c. 5.

29 “Canadian Privacy Legislation,” Media Awareness Network, 2008.

30 The *Personal Information Protection and Electronic Documents Act* provides that:

30. (1) This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information,

businesses subject to both federal and provincial regulation if a province has adopted "substantially similar" legislation.³¹ Similar legislation has been adopted, or is under consideration in several provinces.³²

There can be no doubt that the legislation described above provides clear, focused protection of privacy rights that are within its scope. The general protection offered by the tort of invasion of privacy created by the provincial *Privacy Act* is almost certainly redundant when the new legislation applies. However, the new legislation is specialized as well as specific. It is almost

unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.

(1.1) This Part does not apply to any organization in respect of personal health information that it collects, uses or discloses.

A "federal work, undertaking, or business" is defined as:

2(1) . . . "federal work, undertaking or business" means any work, undertaking or business that is within the legislative authority of Parliament. It includes

- (a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;
- (b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;
- (c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;
- (d) a ferry between a province and another province or between a province and a country other than Canada;
- (e) aerodromes, aircraft or a line of air transportation;
- (f) a radio broadcasting station;
- (g) a bank;
- (h) a work that, although wholly situated within a

entirely concerned with retention and use of information. In Saskatchewan there is as yet no provincial analog to the federal *Personal Information Protection and Electronic Documents Act* applying to the private sector. The provincial legislation is largely confined to information collected by government. The federal legislation has application to some businesses operating in Saskatchewan, but in other cases, the only legal protection against private sector invasions of privacy rights remains the provincial *Privacy Act*.

province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces;

(i) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and

(j) a work, undertaking or business to which federal laws, within the meaning of section 2 of the *Oceans Act*, apply under section 20 of that Act and any regulations made under paragraph 26(1)(k) of that Act.

31 The Act provides that:

26(2) The Governor in Council may, by order, . . .

(b) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.

32The Privacy Commissioner of Canada has deemed legislation in Quebec, Alberta and British Columbia equivalent to PIPEDA.

III. REFORMING THE PRIVACY ACT

1. Current challenges and the role of *The Privacy Act*

Since *The Privacy Act* was adopted, the focus of privacy concerns have shifted. As noted above, many of the emerging issues have to do with electronic information gathering, storage, and retrieval. The Canadian Media Awareness Network observes that:

With the development of new information and communication technologies, the ability of the state and the private sector to collect, record and "mine" personal information has grown exponentially. As early as 1996, Bruce Phillips, then Privacy Commissioner of Canada, warned, "We are in fact buying and selling large elements of our human personae. The traffic in human information now is immense. There is almost nothing the commercial and governmental world is not anxious to find out about us as individuals."³³

In Saskatchewan, challenges to privacy posed by information technology have attracted legislation such as *The Freedom of Information and Protection of Privacy Act*. The new legislation is impressive in its detail and sophistication. But the one certainty about evolving concern about privacy is that new threats are difficult to predict, and even known threats can present themselves in novel, unexpected ways. An American public interest group, the Privacy Rights Clearinghouse, has identified 21 "current issues:"

- Biometrics Technologies
- Video Surveillance
- Online Privacy and E-commerce
- Workplace Monitoring
- Wireless Communications and Location Tracking
- Data Profiling

³³"Why is Information Privacy an Issue?" Media Awareness Network, 2008.

Criminal Identity Theft
Background Checks
Information Broker Industry
Public Records on the Internet
Financial Privacy
Medical Records Confidentiality and Genetic Privacy
Wiretapping and Electronic Communications
Youth Privacy Issues
Digital Rights Management
Digital Television and Broadband Cable TV
Radio Frequency Identification (RFID)
Real ID
Absence of Federal-Level Privacy Protection Law
Behavioral Targeting
Cloud Computing³⁴

Some of these, such as “cloud computing” (mass storage of information on the Internet rather than in storage devices directly controlled by the information gatherer), are so new that the full implications for privacy are not yet clear.

The 2003 report on privacy in Canada discussed many of the same topics, and identified several issues that had attracted particular attention in Canada: National Identification Cards, cross border travel, privacy impact assessments, international information sharing, medical privacy, law enforcement and surveillance.³⁵

While many of these issues relate at least in part to information technologies, fewer than half are primarily or exclusively concerned with information gathering, storage and retrieval. The legislative codes adopted to regulate information technology address many of the privacy threats from these sources, but not all, and not with the certainty that makes the code approach most appealing.

The comprehensive code approach of legislation like *The Freedom of Information and*

34 “Privacy Today: A Review of Current Issues,” Privacy Rights Clearinghouse, March 2001-September 2008 (privacyrights.org).

35 Caryn Mladen, “Privacy in Canada,” A Report of Research on Privacy for Electronic Government, 2003.

Protection of Privacy Act is desirable, but may lack the flexibility to deal with unexpected and novel circumstances. The *Privacy Acts* may remain useful to fill gaps in the legislation.

Gaps are apt to exist for several reasons. Not all threats to privacy are apt to attract the kind of attention legislators have given to information gathering. New issues can be expected to arise more rapidly than legislators can react. As the British Columbia Law Institute observes:

Without a general civil remedy for violation of privacy, conduct that does not involve the misuse of personal information and that does not reach the level of criminality, but which is still offensively invasive, might not be subject to any legal sanction.³⁶

In some cases, legislation in the province may simply lag behind developments in other jurisdictions. For example, Saskatchewan legislation does not provide much regulation of private sector information gathering. The federal *Personal Information Protection and Electronic Documents Act* and legislation in three other provinces does regulate the private sector. A novel private sector privacy issue, so called “work place virtue testing,” has been recognized by the Saskatchewan Information and Privacy Commissioner as an emerging problem:

Information and communication technology now affords employers unprecedented opportunity to monitor their employees. Monitoring may be done to safeguard workers and to protect employer interests or those of customers. This monitoring can however be prejudicial to employees.

He suggests that, despite that limitations of *The Privacy Act*, in the absence of specific provincial legislation, it may provide a remedy:

This Act may well be utilized by employees that are aggrieved by reason of an unreasonable invasion of privacy by an employer. Commencing an action under *The Privacy Act* may be the only legal remedy for many Saskatchewan employees concerned with the monitoring activities of their employer.³⁷

36 British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.

37 R. Gary Dickson and Sandra Barreth, “Privacy Laws and Virtue Testing in the Workplace,” Office of the Saskatchewan Privacy Commissioner, A Presentation for The Canadian Bar Association (Saskatchewan Branch) Mid-

Gaps may also exist when serious privacy concerns are recognized, but there is difficulty in balancing interests and formulating comprehensive rules. A case by case approach may be an attractive way to deal with privacy issues of this type, at least until policy issues are clarified. The privacy issues surrounding public video surveillance are an example. The use of surveillance cameras in places frequented by the public is increasing. Surveillance by public authorities likely falls under *The Freedom of Information and Protection of Privacy Act*, and the Saskatchewan Privacy Commissioner has issued guidelines.³⁸ Surveillance of premises and adjacent public spaces by businesses and other private individuals is outside the scope of the guidelines. Surveillance in such cases raises a difficult set of issues, involving changing expectations of privacy, security matters, and use and control of surveillance information. Although it seems that the language of the privacy acts currently precludes application to violations of privacy in public places³⁹, the British Columbia Law Institute suggests that video surveillance may be an example of a privacy threat well suited to application of a properly formulated tort of invasion of privacy.⁴⁰

Even if there is comprehensive legislation covering a specific activity that may endanger privacy, gaps may still exist. Circumstances that were not foreseen may come to light. In addition, the policy of specific legislation may be inadequate. The courts, applying the general tort of invasion of privacy, could help keep the law in step with public expectations as privacy issues evolve. For example, a recent report issued by the Canadian HIV/AIDS Legal Network points to what it regards as inadequacies in legislation governing medical information:

On the whole, provincial legislation on the protection of health information (existing and proposed) does not adequately protect the privacy and confidentiality of the personal health information of people living with HIV/AIDS. First, privacy is often one among many public policy goals that these laws seek to achieve. Second, existing legislation tends to focus on the sectors covered (private or government) or who is covered (definitions of custodian or

Winter Meeting February 3, 2006.

38 Guidelines for video surveillance by Saskatchewan public bodies, prepared by OIPC, June 24, 2004.

39 See below.

40 British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.

trustee) rather than on protecting the information itself regardless of which sector or person holds it. . . . Third, the discretionary disclosure clauses are overbroad. Health information custodians are given the statutory authority to disclose personal information to third parties without the patient's consent beyond what is required to achieve the purported goal of the disclosure.⁴¹

Whether or not all these criticisms are valid, they suggest issues that might legitimately and usefully be raised under the *Privacy Acts*.

2. The tort of invasion of privacy: Theory and practice

Although legislators have recently favoured the comprehensive code approach of statutes such as *The Freedom of Information and Protection of Privacy Act*, the potential value of a general tort of invasion of privacy has once again begun to be recognized. On the broadest grounds, a general protection for privacy is attractive because privacy is a core value in our society. The Supreme Court of Canada has observed that:

[Privacy is] at the heart of liberty in the modern state.... Grounded in [one's] physical and moral autonomy, privacy is essential for the well-being of the individual.... [I]t is worthy of constitutional protection, but it also has profound significance for the public order.⁴²

The status of privacy as a core value suggests that the law should provide a broad, rights-based protection for it. The gaps in the coverage of privacy legislation discussed above are less tolerable if privacy is regarded as a right. In the United States, the tort of invasion of privacy was derived by implication from the *Bill of Rights*. It has been developed over more than a century by courts and commentators. The proposition that privacy should be a protected right seems to date from an influential commentary by Louis Brandeis,⁴³ who later developed the concept as a Supreme Court Justice. Brandeis argued that adequate protection of privacy must

41 Privacy Protection and the Disclosure of Health Information: Legal Issues for People Living with HIV/AIDS in Canada (Published by the Canadian HIV/AIDS Legal Network).

42 *Hunter v. Southam*, [1984] 2 S.C.R. 145 (S.C.C.).

43 Louis Brandeis, "The right to privacy," *4 Harvard Law Review* 1890.

be general enough to apply to a broad range of privacy issues. He wrote that “any rule of liability adopted must have in it an elasticity which shall take account of the varying circumstances of each case.” After a critical review of the treatment of privacy rights by the American courts from 1890 to 1968, Prosser observed that a rights-based approach to privacy requires a balancing of interests.⁴⁴ Although legislation can codify an appropriate balance when the nature of a threat to privacy is well understood, novel and hard cases may require the kind of discretion inherent in the general tort approach.

In *Hunter v. Southam*,⁴⁵ the Supreme Court found that section 8 of the *Charter of Rights and Freedoms* protects privacy interests. Since then, the court has continued to apply section 8 to cases involving privacy interests. To date, the Supreme Court has stopped short of recognizing a general tort of invasion of privacy, but as Alan Linden observes, “we seem to be drifting closer to the American model.”⁴⁶

The Alberta Court of Appeal held in *Motherwell v. Motherwell* that the common law is capable of evolving protections for privacy rights, and awarded damages for telephone harassment. The court did not expressly recognize an independent tort of invasion of privacy, but found that on the facts of the case, the invasion of privacy amounted to a nuisance.⁴⁷ In *Roth v Roth*, an Ontario court similarly found harassment to be an actionable invasion of privacy, holding that “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”.⁴⁸ It may be premature to conclude that a common law tort of invasion of privacy now exists in Canada, but the trend is clear.⁴⁹

Not surprisingly, there is also some renewed interest in the statutory tort. New Brunswick is considering adoption of a *Privacy Act*, and the British Columbia Law Institute has suggested that the *Privacy Acts* are worth reconsidering and revising to make them more useful.⁵⁰

44 W. Prosser, “Privacy,” *California Law Review* 1968.

45 See above.

46 A. Linden. *Canadian Tort Law*. Toronto: Butterworths, 7th ed, 2001.

47 (1976), 73 D.L.R. (3d) 62.

48 (1991), 4 O.R. (3d) 740 (Ont. H. C.).

49 See Colin D. Feltham, *The Common Law Tort of Invasion of Privacy*, Barry Sparling Richard, St. John and Moncton, n.d.

50 British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.

3. Criticisms of the tort approach

Shortly after the first provincial *Privacy Act* was adopted in British Columbia, the Ontario Law Reform Commission expressed doubt that creation of a tort of invasion of privacy was a useful exercise:

[L]itigation under this statute will fight over the ground of what is reasonable in each case - a situation which, under our legal process, renders any reference to the general problem of protection of privacy faced by the plaintiff irrelevant, prejudicial to the defendant, and not something which should properly be considered by the court. This legislation is fine as it goes, but, absent what would amount to a comprehensive code of privacy, setting definitive norms for information trafficking, control of the means and physical implements for invading privacy, control of psychological in-depth testing, input and disclosure standards for school, medical and governmental records, and all of the rest - in the absence of clear legislative policy in relation to the larger problem of privacy, in short - then this statute standing alone could easily become a well-intentioned dead letter...⁵¹

No doubt, the privacy acts failed to develop in the way their advocates had hoped. There have been few cases under the legislation. Only one decision has been reported under the Saskatchewan *Privacy Act*, and only a handful of decisions under the other privacy acts. In fact, after 25 years in force, the privacy acts have been dismissed by some commentators as “dead letters.”⁵² The “comprehensive code” approach recommended by the Ontario Law Reform Commission is now favoured by legislators.

What is perhaps not clear is whether the privacy acts have fallen short of expectations because of the inherent flaws in the concept of a tort of invasion of privacy identified by the Ontario Law Reform Commission. The basic criticism made by the Ontario Commission and other critics is that the privacy acts are too vague and uncertain to provide practical protection for privacy. Even Brandeis admitted that a remedy elastic enough to be a general protection for privacy would likely be “difficult of application, but also to a certain extent uncertain in its

⁵¹ Ontario Law Reform Commission, *Report on Protection of Privacy in Ontario*, 1968.

⁵² D. Flaherty. “Some reflections on privacy in technology.” 26 *Manitoba Law Journal* 1998-1999, 219.

operation”⁵³ However, this is not an exceptional state of affairs when common law principles are developed by the courts. The American experience suggests that a general tort of invasion of privacy can have utility.

The British Columbia Law Institute observes that:

When the *Privacy Act* was passed, the law of privacy in Canada was very undeveloped. . . . The statements of officials reported in the press at the time indicate that the Act was originally conceived as a flexible instrument to allow the courts wide latitude to arrive at a reasonable and just result in each case. There was little in terms of established legal principle relating to the protection of privacy to guide the courts in applying the Act.⁵⁴

The advocates of the privacy acts expected that the tort of invasion of privacy would become less vague and uncertain as the courts developed it. Of course, uncertainty would inevitably remain when novel cases or new threats to privacy came before the courts, but as jurisprudence accumulated, advocates expected concepts and boundary conditions to be refined. The important question may be why this failed to happen.

It may be that the task the privacy acts left to the courts was too difficult for the times. As the British Columbia Law Institute noted, legal principles relating to privacy were undeveloped when the acts were adopted. Privacy issues may have been too novel to expect the courts to develop a coherent approach to privacy rights. The courts may now be more comfortable with privacy issues. A new generation of judges may be more willing to develop the statutory tort. The interest in tort protection of privacy evidenced by the courts in cases such as *Roth v Roth* suggests that a renewed *Privacy Act* may be welcomed by the courts, bar and public.

The British Columbia Law Institute suggests that a significant part of the reason for the failure of the privacy acts can be found in the acts themselves. Perhaps because they were entering unfamiliar territory, the drafters of the privacy acts may have been overly cautious. The drafters of the *Privacy Acts* avoided a definition of privacy. However, the language of the *Acts* does condition the concept of privacy. The defences, factors for consideration, and even examples of

53 Louis Brandeis, “The right to privacy,” *4 Harvard Law Review* 1890.

54 British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.

invasions of privacy included in the legislation, constrained the concept of privacy. This may account for the narrow interpretation the courts have given to the privacy acts. These constraints will be discussed in the next section of this paper.

Critics of the privacy acts suggest that privacy can be more effectively protected by the comprehensive code approach recommended by the Ontario Commission and partly implemented in recent legislation. When the *Privacy Acts* were adopted, it may have been thought that case law developing the statutory tort would make more specific legislation unnecessary. The capacity of new technology to generate challenges to privacy has belied this hope. It is unlikely that the courts could keep pace with evolving privacy issues, even if the tort of invasion of privacy was vigorously developed. A general tort of invasion of privacy is not a substitute for detailed legislation regulating specific activities that threaten privacy. Information technology, for example, is a complicated topic. Protecting privacy when personal information is gathered requires the comprehensive code approach of legislation such as the provincial *Freedom of Information and Protection of Privacy Act* and federal *Personal Information Protection and Electronic Documents Act*. However, the dichotomy between the code and tort approaches identified by the Ontario Law Reform Commission may be misleading. They should be regarded as complementary rather than competing approaches. The weakness in the tort approach pointed to by the Ontario Commission, its lack of specificity and certainty, is also its strength.

4. Reformulating *The Privacy Act*

In retrospect, it seems that the *Privacy Acts* failed to give enough guidance to the courts to encourage development of the tort of invasion of privacy created by the legislation. Understanding of privacy issues may have been too undeveloped for policy makers to give guidance. This suggests that the *Privacy Acts* could be made more relevant by drawing on experience with privacy issues since the *Acts* were adopted.

The most pressing problem with the *The Privacy Act* is perhaps the constraints on the concept of privacy it contains. The British Columbia Law Institute points to two respects in which the privacy acts have constrained the concept of privacy: the burden of proof imposed on plaintiffs, and limits on the application of the legislation to public places. In addition, the examples of invasion of privacy in the Saskatchewan *Privacy Act* could perhaps be usefully extended.

1. **Burden of proof.** The Saskatchewan *Privacy Act*, like other provincial *Privacy Acts*, renders an invasion of privacy actionable only if the defendant acted “wilfully and without claim of right,

to violate the privacy of another person.” The British Columbia courts have interpreted “wilfully” to require that the defendant knew or ought to have known that an act would violate the privacy of the plaintiff, and “claim of right” to mean “an honest belief in a state of facts which, if it existed, would be a legal justification or excuse.” These interpretations appear to have been adopted in Saskatchewan in *Peters-Brown v. Regina District Health Board*.⁵⁵ It is worth noting that the court used this “narrow interpretation” to deny that an invasion of privacy had occurred, even though it found that the actions of the defendant amounted to breach of confidence, and awarded damages on that ground. It is difficult to regard a definition of invasion of privacy that excludes breaches of confidence concerning release of personal information as the kind of flexible and elastic concept required to encourage development of a broad tort remedy.

The British Columbia Law Institute notes that:

It is unusual in civil matters to require a plaintiff to prove a subjective state of mind on the part of the defendant. The unusually stringent burden of proof may explain in part why so few claims have succeeded under the provincial *Privacy Acts*.

The willfulness requirement was no doubt inserted in the legislation out of caution, to prevent normal social and business contacts from being stigmatized as invasions of privacy. However, there are alternatives to the willfulness requirement that may define more appropriate limits on the right to privacy. The *Uniform Privacy Act* omits the willfulness requirement, providing only that “violation of the privacy of an individual by a person is a tort that is actionable without proof of damage.” Like the Saskatchewan *Act*, the *Uniform Act* includes a list of examples of invasion of privacy, all of which are intentional. The *Uniform Act* thus appears to suggest that actionable invasions of privacy are usually intentional, but leaves it to the court to make exceptions. The British Columbia Law Institute suggests actionable invasions of privacy should be “reckless or intentional.” Consideration should be given to substituting a negligence standard.

2. Application of The Privacy Act to public places. In *Silber v. BCTV* a British Columbia court rejected a claim of invasion of privacy on the sole ground that the incident, the filming of the plaintiff, occurred in a parking lot visible from the street.⁵⁶ The Saskatchewan *Privacy Act*, like

55 [1996] 1 W.W.R. 337 (Sask. Q.B.); aff’d. [1997] 1 W.W.R. 638 (Sask. C.A.).

56 *Silber v. BCTV* (1986), 69 B.C.L.R. 34 (B.C.S.C.).

the B.C. *Act*, provides that:

6(1) The nature and degree of privacy to which a person is entitled in any situation or in relation to any situation or matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others.

The British Columbia Law Institute suggests that the decision in *Silbur* implies that “there can be no reasonable expectation of privacy in a place normally open to public view, regardless of the nature of the place.”⁵⁷ The Institute argues that:

It is unrealistic to limit legal protection of privacy in the civil sphere to activity in enclosed spaces not observable from the outside. The normal expectations of citizens in regard to freedom from interference with their personal autonomy go beyond that. While the degree of privacy that can reasonably be expected in public places is obviously lower than in a dwelling or other private space, it is more than nil. It extends to the ability to move freely about, associate with others and participate normally in society without being subjected to oppressive attention, illegal or unreasonable surveillance, or other forms of harassment from others.

It recommends that the *Privacy Acts* be revised to preclude the interpretation in *Silber*.

3. *Examples of violations of privacy.* *The Privacy Act* contains a list of “examples of violation of privacy.” Useful as these may be, they may also serve to limit the scope of the *Act*. As noted above, the list is weighted toward privacy concerns that were topical when the *Act* was adopted. The list does not include much that addresses current concerns about information technology, for example. A list of examples could assist the courts in identifying violations of privacy, but it may be necessary to revise it as privacy concerns change. The *Uniform Privacy Act* includes some additional examples. The British Columbia Institute has suggested that specific language addressing video surveillance and stalking would be useful.

57 British Columbia Law Institute, *Consultation Paper on the Privacy Act of British Columbia*, July 2007.