Vol. LIV MARCH 1976 MARS No. 1

THE LAW AND PRIVACY: THE CANADIAN EXPERIENCE

PETER BURNS*

Vancouver

I. *What is Privacy?*

Over the past decade the Canadian public has been treated to an on-going debate concerning the pressing need to preserve "privacy" which is being threatened by science and technology to the point of surrender. We have seen the enactment of provincial[1] and federal privacy statutes[2] which, if not actually protecting this primary social value, articulate the politicians' concern to be seen to be concerned. We know that everyone is in favour of protecting privacy—so long as it does not interfere with "freedom of the press", the "right to free speech", "legitimate methods of conducting business", the "effective pursuit of criminals", and "the public right to know".

Why the pressing need to reinforce privacy values now? Professor Alan Westin has succinctly made the point:[3]

---

* Peter Burns, of the Faculty of Law, University of British Columbia, Vancouver, and of the British Columbia Bar. The author gratefully acknowledges the support of the Canada Council, Humanities and Social Sciences Division, which enabled the study to be undertaken. I also acknowledge the excellent work of my research assistants Robert S. Reid and Kenneth Jacques.

[1] The British Columbia Privacy Act, S.B.C., 1968, c. 39; the Manitoba Privacy Act, S.M., 1970, c. 74; and the Saskatchewan Privacy Act, S.S., 1974, c. 80.

[2] The Protection of Privacy Act, S.C., 1973-74, c. 50.

[3] Privacy and Freedom (1967), p. 365. Whether or not this "hardware" is as readily available as Westin thinks, the generally held belief that it is is the real impetus to public concern for privacy values today.

> A technological breakthrough in techniques of physical surveillance now makes it possible for government agents and private persons to penetrate the privacy of homes, offices and vehicles; to survey individuals moving about in public places; and to monitor the basic channels of communication by telephone, telegraph, radio, television and data line. Most of the hardware for the physical surveillance is cheap, readily available to the general public, relatively easy to install, and not presently illegal to own.

The concept of privacy has a universality that transcends national boundaries in a way that is lacking in many other cultural conditions and sets it apart from them. Under article 12 of the Universal Declaration of Human Rights:[4]

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This statement of principle has subsequently been incorporated in the international Covenant on Civil and Political Rights[5] which has not yet come into effect. Canada has expressed its intention to sign the Covenant once the federal government has obtained agreement from all the provinces.[6] The right to privacy as a social goal was also reasserted by an international conference in Stockholm in 1967[7] and is currently the subject of examination by the Council of Europe.[8]

But what is "privacy" and what does the claim that one has a "right to privacy" mean?

"Privacy" is a relative concept meaning or describing different things to different observers. To a sociologist, privacy may mean "a value [that] does not exist in isolation, but is part and parcel of the system of values that regulates action in society.[9] . . . Privacy

---

[4] G.A. Res. 217 (iii), dated December 10th, 1948, passed without dissent.

[5] Art. 17 of Annex to G.A. Res. 2200 (XXI), dated December 16th, 1966.

[6] Statement delivered May 10th, 1974, Amnesty International Canada on behalf of the Minister of Justice, at p. 11 *et seq.*

[7] Conclusions of the Nordic Conference on the Right to Privacy, in Privacy and the Law, a report by the British section of the International Commission of Jurists (1970).

[8] See, *e.g.*, the Draft Resolution on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, July 1974, Addendum I to C.C.J. (74) 38.

[9] Simmel, Privacy Is Not an Isolated Freedom, in Privacy (1971), 13 Nomos 71.

boundaries are self-boundaries in the sense that we live in continual competition with society over the ownership of ourselves and a territory is staked out which is peculiarly our own. Its boundaries may be crossed by others only when we expressly invite them to do so. This condition of insulation is what we call privacy".[10]

In one of the few anthropological studies of privacy, Roberts and Gregor adopted[11] the definition of privacy formulated by Westin, a lawyer: "The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[12] They studied forty-two societies and noted that those with domesticated plants and animals were likely to be higher in privacy than those based on hunting, gathering and fishing. Their tentative conclusion was: "Perhaps privacy as we know it is a neolithic development. . . . Appearing in the old world and associated with the Near Eastern cultural complex which later diffused to all areas of high culture in the old world."[13]

It would seem then that "privacy" is really a cultural state or condition, directed towards individual or collective self-realization,[14] varying from society to society. It certainly has been recognized in our culture from the time of earliest records. Konvitz[15] points to the Bible, Socrates, Plato, Thomas More, and Locke as revealing a continuum of awareness that "privacy" is a social reality. In the words of a contemporary political scientist, Herbert Marcuse, there is a notion of a "private space" in which man may become and remain "himself".[16] When we imprison a

---

[10] *Ibid.*, at p. 72.

[11] Privacy: A Cultural View (1971), 13 Nomos 199. See also Westin, *op. cit.*, footnote 3, pp. 11-19.

[12] *Ibid.*, p. 7.

[13] *Op. cit.*, footnote 11, at p. 202. The authors also note, at the same page, "The psychological variables associated with the presence of large domestic animals, games of strategy and high gods, would also seem to have significant relationships to high privacy."

[14] "It is recognized that to preserve the human dignity of the individual and his effective freedom to develop and exercise the full human personality, there must be an area reserved to himself where he can be free from unwanted observations of others." New Zealand Law Revision Commission, Report of Subcommittee on Computer Data Banks and Privacy (April 1973), p. 68.

[15] Privacy and the Law: A Philosophical Prelude (1966), 31 L. and Cont. Prob. 273, at pp. 273-275.

[16] One-Dimensional Man (1964), p. 10.

criminal an essential element of the punishment is not merely loss of freedom of movement but privacy-loss!

Modern concern with privacy is the product of the rise of the middle class which in turn is the result of the drift from village to urban life during the industrial revolution.[17] This concern varies from culture to culture so that privacy may be highly developed socially and legally in a democratic state such as the United States, whereas in closed societies like Spain and the Soviet Union it may be regarded as a low social value and relatively unprotected by law. Between these two extremes, gradations of concern with privacy are apparent in different cultures. Continental Europe[18] has developed what may be loosely described as the "dossier-system" which is entirely repugnant to those social systems derived from the English common law. Spiro[19] puts this dramatic divergence of attitude down to the way in which the English and Continental legal systems developed after the Norman Conquest. Whereas the Continental systems retained the forms of canonical procedures, including inquisition and cameralism, the English developed confrontation and cross-examination as its basic means of fact-finding. Also, the inquisitorial system remained largely part of the organization of government as distinct from the common law courts[20] that established their independence and peculiar constitutional role prior to the eighteenth century.

There have been numerous attempts made to define the right to privacy. The most famous is "the right to be let alone"[21] which has been taken to mean "the right to live one's life in seclusion without being subjected to an unwarranted and undesired publicity".[22] Leaving aside the exact nature of this "right" for the moment, its sociological sources appear relatively clear, even

---

[17] Strömhelm, Working Paper on the Right of Privacy, Stockholm, (1967), for the Nordic Conference of Jurists, pp. 1-7. A detailed account of this process is contained in an article by Shils, Privacy: Its Constitution and Vicissitudes (1968), 31 L. and Cont. Prob. 281, at pp. 286-296. See also Spiro, Privacy in Comparative Perspective (1971), 13 Nomos 121, at pp. 138-139.

[18] Other than Sweden.

[19] *Op. cit.*, footnote 17, at pp. 137-139.

[20] Although certain lapses have occurred, the roles of Chief Justice Scroggs and "Hanging Judge" Jeffries are merely two of the more notable English illustrations.

[21] Cooley, Torts (2nd ed., 1895), p. 188.

[22] *Kerby* v. *Hal Roach Studios* (1942), 127 P. 2d 577 (Cal. C.A.).

though not accepted as a proper reason for reinforcing it by all commentators.[23] An English author, Madgwick,[24] summarizes it along the following lines: "Ever since man's emergence as a social animal his right to be private has been one of his essential guarantees of liberty. In this sense he may be considered free to the precise extent that he is let alone in that inner core of his being which concerns only himself, to think and act unfettered by either legal restraint or private curiosity. . . . In today's rapidly changing society a part of man's life must be reserved to himself and it is a form of tyranny to attempt to invade and capture another's privacy which is more than a negative state. This last is significant because if privacy is a positive state occurring in the ordinary course of human relations, the burden of justifying any invasions must logically fall on the invader."[25]

The same writer defines the right to privacy as the right of the individual to be in a state of privacy to whatever extent he might wish and an invasion of privacy as anything which in any way interferes with his right.[26] This definition is open to the objection that it is inherently vague, being based on the subjective perceptions and desires of the individual concerned. As a working definition for legal purposes, it would be practically useless since it could not be utilized without further defining each individual's expectations subject to the constraints of law and public policy.

The most significant work undertaken in recent years dealing with this matter is by Alan Westin in his paper, "Science, Privacy and Freedom: Issues and Proposals for the 1970's",[27] and his powerful treatise, *Privacy and Freedom*.[28] In his paper, Westin begins by stating that the nature and degree of privacy accorded to individuals and organizations depends in the first instance on

---

[23] Among writers who regard undue emphasis on the right to privacy as confusing the real values involved or an attempt to bolster bourgeois values are: Leach, A Runaway World (1967), Reith Lectures, London (1968); Bettelheim, The Right to Privacy is a Myth, Saturday Evening Post, July 27th, 1968, p. 9; Mead, Our Right to Privacy, Redbook, April 1965, p. 16; Hechs, The Limits of Privacy (1959), 28 Am. Scholar 192; Arndt, The Cult of Privacy (1949), 21 Australian Q. 69; and Halmos, Solitude and Privacy (1952).

[24] Privacy Under Attack (1968). See also the more recent work by Madgwick and Smythe, The Invasion of Privacy (1974).

[25] Privacy Under Attack, *ibid.*, p. 2.

[26] *Ibid.*, p. 4.

[27] (1966), 66 Col. L. Rev. 1003.

[28] *Op. cit.*, footnote 3.

the political system and culture patterns of the society involved:[29]

> Totalitarian systems deny most privacy claims of individuals and non-governmental organizations to assure complete dedication to the ideals and programs of the state, while the totalitarian state's own governmental operations are conducted in secrecy. Democratic societies provide substantial amounts of privacy to allow each person widespread freedom to work, think and act without surveillance by public or private authorities and to provide similar breathing room for organizations; but they try to strike a delicate balance between disclosure and privacy in government itself.

Westin takes the view[30] that privacy in the sense of "being let alone" actually embraces four different psychological and physical relations between an individual and those around him. These he defines as the states of:

(a) Solitude. This is the state where an individual is separated from the group and freed from the observations of others. It is the most complete state of privacy attainable although even here the subject's peace of mind may be intruded by physical stimuli, supernatural belief or primordial psychological condition.

(b) Intimacy. This is the state where the individual is acting as part of a small group — the family, society, *etc.* Here corporate seclusion may be attained.

(c) Anonymity. This occurs where the individual, although doing public things in public places, finds freedom from identification and surveillance. Another form is the anonymous expression of views whereby the individual may publicly air his views but have his identity remain unknown.

(d) Reserve. Which expresses the individual's need to withhold information, to create mental distance to protect his personality.

Having described what the notion of privacy encompasses, Westin goes on to outline its functions.[31] These are:

(a) The reinforcement of personal autonomy based on the belief in the uniqueness of the individual and his basic dignity and worth as a human being. Individuality stems from the need for autonomy.

(b) It grants emotional release in various situations, for example, from playing social roles or complying with social norms.

(c) Privacy provides the opportunity for self-evaluation which is necessary to process daily experiences and organize future experiences.

(d) The state of privacy also ensures limited and protected communication which is required to provide the individual with the opportunity to share confidences and intimacies with those he trusts.

---

[29] *Op. cit.*, footnote 27, at p. 1050. In the words of a Canadian writer, "Privacy ... is not just an individual interest, but is first and foremost a political value of the highest order.": Ryan, Privacy, Orthodoxy and Democracy (1973), 51 Can. Bar Rev. 84, at p. 86.

[30] *Ibid.*, at pp. 1020-1021.

[31] *Ibid.*, at pp. 1022-1028.

In sum, then, privacy as a state or condition is a means for self-realization.

Although Westin's contribution to the understanding of the concept of privacy is immense, his definition of privacy[32] has been subjected to heavy criticism. An Australian commentator, Morison,[33] points out that it omits the class of cases wherein communications are made *to* a person, such as unsolicited telephone calls. More trenchant objection was levelled at Westin's definition by Professor Lusky[34] who argues that a definition of privacy should not include such value-loaded terms as "right" or "claim". Privacy in his view is not a claim and, if it is a moral right it is too vague and, if a legal right, of little normative value because it leaves too many unanswered questions. Instead, privacy should be regarded as a condition.[35]

Lusky also criticizes Westin's definition because it fails to distinguish between informational communications that are objectionable only because of their false or misleading character and those that, however accurate and complete, report facts that cannot be decently retailed. In the light of the past failure of numerous attempts to define privacy for legal purposes one would expect academics to turn their minds in other directions. But the philosopher stone still entices and the most recent contribution to the vast literature on this subject is by Professor Parker in a paper entitled, "A Definition of Privacy".[36]

The immediate spur to Parker's exhaustive treatment of this topic was the decision of the United States Supreme Court in *United States* v. *White*[37] in which it was held that constitutionally justifiable expectations of privacy do not include the expectation that conversations are not being simultaneously transmitted to an unknown audience by the person to whom one is speaking.

---

[32] *Op. cit.*, footnote 3, p. 7.

[33] Report on the Law of Privacy (1973), N.S.W. Government Printer. Dr. Morison recognizing the difficulty of defining "privacy" takes the view that attempts are either too wide or too narrow. But he does adopt a working definition that is not value-loaded; "the condition of an individual when he is free from interference with his intimate personal interests by others": Report, p. 13.

[34] Invasion of Privacy: A Clarification of Concepts (1972), 72 Col. L. Rev. 693.

[35] Lusky's view that privacy is a condition or state whereby an individual is free from certain types of interference by others is taken up and adopted by Morison in his Report, *op. cit.*, footnote 33.

[36] (1974), 27 Rutgers L. Rev. 275.

[37] (1971), 401 U.S. 745.

Parker recognizes that there is no consensus in the legal and philosophical literature as to a definition of privacy and proceeds to outline the three criteria he believes such a definition would have to meet:

(a) It would fit the data, that is the shared intuitions of when privacy is or is not gained or lost.

(b) The test of simplicity.

(c) Applicability by lawyers and courts. The definition must be capable of being given in charges to juries, in opinions and complaints.

But, since the criteria will sometimes be in mutual conflict, they will have to be compromised by each other in any definition. Therefore the more comprehensive the definition the less need for compromise.

With regard to the criteria of "fitting the data" and "applicability by the courts", Parker, considers that an adequate definition of privacy must permit a separate discussion of five questions: (a) whether a person has lost or gained privacy, (b) whether he *should* lose or gain privacy, (c) whether he *knows* he has lost or gained privacy, (d) whether he approves or disapproves of any such loss or gain, and (e) how he experiences that loss or gain. He considers that definition in terms of "power" or "control" allows such a separate discussion.[38]

Parker believes that the essence of the concept of privacy is control over who can sense us: "Privacy is control over when and by whom the various parts of us can be sensed by others."[39] "Sensed" in this context means seen, heard, touched, smelled or tasted. "Parts of us" means the parts of our bodies, our voices and the products of our bodies, and includes objects closely associated with us. Accordingly, the definition is physically oriented.[40]

Having defined privacy, Parker turns to demolish two criticisms that he anticipates may be levelled at it. The first is

---

[38] See, *e.g.*, Miller, The Assault on Privacy (1971), p. 25, where privacy is defined as "the individual's ability to control the circulation of information relating to him". Parker does not regard this as a complete definition because not every loss or gain of information is a loss or gain of privacy: *op. cit.*, footnote 36, at p. 279.

[39] *Ibid.*, at p. 281.

[40] Parker rejects definitions of privacy in terms of a psychological state because they cannot cover the situation where there has been privacy loss and no corresponding change in mental state because the loss is unknown: *ibid.*, at p. 278.

that the definition is objectionable as being too narrow, not covering, for example, the situation where an agent questions one's neighbours about one's affairs and discovers information that one did not want disclosed. Another case would be where a national data bank has gathered information from various sources to construct a detailed personal file revealing facts that one would never have disclosed voluntarily.[41]

These objections are met with the argument that what seems to be a loss of privacy *is in reality a loss of the value of privacy.* Privacy value may be diminished in three ways: (a) when information about oneself is gathered,[42] (b) the gathering of information about an individual lessens the value of his privacy by rendering it less secure, and (c) the existence of the threat posed by (b) devalues one's privacy because the individual never knows if it is still intact. According to this analysis the existence of a data bank is a loss of the value of the privacy of the subjects examined and not a loss of privacy *per se.*

Parker then illustrates his distinction with reference to two classes of cases.[43] In the first an "unbugged" police informer discloses information passed on to him and such information flow is not deemed an invasion of privacy, whereas in the second case the informer is "bugged" and the information is simultaneously picked up by police. Again, specifically in *United States* v. *White,*[44] the courts have held no invasion of privacy has occurred. Parker argues that this latter conclusion is erroneous and it really is a case of invasion of privacy because the individual has lost control over who can sense him. The first class of case on the other hand is rightly decided because it merely involves loss of control over information and therefore a loss of the value of privacy rather than privacy itself.

Whatever the merit of the distinction drawn by Parker, between privacy invasion and loss of privacy value, one thing is clear. His "applicability principle" has been seriously compromised. How such a distinction could be sensibly put to a jury in a charge by a court escapes me. Take the situation where a govern-

---

[41] *Ibid.*, at pp. 284-288.

[42] This is because one of the important uses of privacy is to *control* the flow of such information. Thus one may still have his privacy (his control over when and by whom one can be sensed by others) but to the extent that he cannot use it to control the flow of information about himself that privacy is less valuable to him.

[43] In the United States, decisions based on the Fourth Amendment to the Constitution had drawn the same distinction.

[44] *Supra.*, footnote 37.

ment agent has collected information concerning X, which is to be stored in a national information data bank, and that part of it is incorrect. According to Parker there is no privacy loss but merely a loss of the value of privacy. If this is so then perhaps the value of privacy is more significant than privacy itself![45]

After reviewing the preceding attempts to define privacy one is left with the objections to each. It must have been a sense of frustration with such fruitless endeavours at construction of a comprehensive definition that drove the eminent American scholar, Prosser,[46] to take an entirely different direction which is characterized as the "functional approach". This is the view that the law of privacy is directed at four distinct kinds of invasion of four separate interests tied together by a common name: intrusions upon the plaintiff's physical seclusion or solitude,[47] public disclosure of private facts,[48] publicity which places the plaintiff in a false light[49] and appropriation for the defendant's benefit of the plaintiff's name or likeness.

Prosser based his "interest categories" on the United States decisions and statutes. More recently, Westin has persuasively argued[50] that two further categories may be added as a result of evolving technology. These are psychological surveillance[51] and data surveillance.[52]

---

[45] Parker has clearly elucidated many of the hazy edges of the notion of privacy and his contribution to the literature must be regarded as the most useful and innovative over the past few years. But it is predicted that additional analyses of privacy will not be long in forthcoming and that the last word on the definition of privacy has not yet been spoken.

[46] Privacy (1960), 48 Cal. L. Rev. 383, and The Law of Torts (4th ed., 1971), pp. 807 *et seq.* The same approach is apparent in the American Restatement of Torts (2d) (1965), Ch. 28A, para. 652A.

[47] For example, peering through a partly open window watching the occupants of a room engaging in intimacies.

[48] Such a case was the basis of the seminal article by Brandeis and Warren, The Right to Privacy (1890), 4 Harv. L. Rev. 193, where the "yellow press" publicized the wedding of Mr. Warren's daughter. A strong example is *Melvin* v. *Reid* (1931), 112 Cal. App. 285, where the producers of a film on the life of a reformed prostitute who had been acquitted of murder were held liable to her. The film, "The Red Kimono", was made seven years after the events portrayed.

[49] See, for example, *Tolley* v. *Fry*, [1931] A.C. 333, where an amateur golfer had his amateur status threatened by a misleading advertisement. This case was decided in libel rather than invasion of privacy.

[50] *Op. cit.*, footnote 3, Ch. 6.

[51] This includes the use of personality testing programmes for job suitability, the resort to the polygraph in adducing evidence and narco analysis in law enforcement.

[52] This is the unreasonable compilation and use of data collections concerning individuals and groups in the community.

How then should the "right to privacy" be regarded? Perhaps the most sensible approach, in the light of the difficulty of definition, is to adopt the suggestion of one commentator[53] that:

> It may be useful as a legal concept to regard the "right to privacy" as a principle, having a high order of generality, than a rule which will govern specific cases.[54]

In such a way the right to privacy will reveal directions and be elastic. The rules will be articulated by statutes, case law and constitution, whereas the principle will be derived from moral and psychological imperatives. Accordingly the "right to be let alone" is not a rule but a principle which merely gives guidance in a specific case.

If this view of the right to privacy is taken, together with Prosser's "interest analysis", a coherent and workable law of privacy can develop, as indeed it has in the United States. The three general privacy statutes enacted in this country appear to bear out this approach, whether by accident or design. In British Columbia,[55] Manitoba[56] and Saskatchewan[57] there has been no attempt to define privacy as such, although certain factors are stated to be relevant when the tribunal of fact decides whether or not a privacy invasion has occurred.

This "open-textured" legislative approach, which is not very different from the judicial development of the law of negligence, seems most appropriate. The tribunal will exercise its own sense of what is proper in the circumstances in deciding whether there has or has not been a breach of privacy subject to the legislative directions and strictures.[58] It may not be entirely satisfactory from a theoretician's perspective but from the viewpoint of efficiency and simplicity[59] it is arguably best. In any event, until such time as a definition of privacy is constructed that incorporates the

---

[53] Freund, Privacy: One Concept or Many (1971), 13 Nomos 182.

[54] *Ibid.*, at p. 197. It may be better still to regard the "right to privacy" as a *set of principles*, since so many disparate interests are encompassed by it. Different principles may underlie separate interests that may in turn be differently dealt with by discrete rules spelled out by statute, *etc.*

[55] *Supra*, footnote 1.

[56] *Ibid.*

[57] *Ibid.*

[58] This has been referred to as the "mores test": Yang, Privacy in English and American Law (1966), 15 Int. & Comp. L.Q. 175, at p. 184.

[59] Although not a definition the "open-textured" approach arguably fulfills the definition-criteria set out by Parker, *op. cit.*, footnote 36. That is, it fits the data to the extent that statutory factors of relevance are set out, it is simple and can be applied by lawyers and courts.

distinct and discrete legally protected interests we understand to fall under that term, the present "functional" direction appears to be the only way to stumble.

Our task now must be to attempt to elicit what legal measures are available for invasions of privacy and gauge their adequacy in the light of modern technology and social institutions. In order to appreciate the status of privacy protection by law in Canada today, it is convenient to deal with the subject from two different perspectives. These are: to what extent do traditional legal sources protect privacy, and how far has this position been altered by recent statutory modification?

II. *Privacy and Traditional Legal Responses.*

1. *The Common Law.*[60]

At a superficial level the common law of privacy is simple to summarize: there is no protection for personal privacy *per se*, at least outside the United States.[61] As Fleming has expressed the position:[62]

> The right of privacy has not so far, at least under that name, received explicit recognition by British courts. For one thing, the traditional technique in tort law has been to formulate liability in terms of reprehensible conduct rather than of specified interests entitled to protection against harmful invasion. For another, our courts have been content to grope forward, cautiously along the grooves of established legal concepts, like nuisance and libel, rather than make a bold commitment to an entirely new head of liability.

This adequately states the common law's recognition of a right of privacy in the Commonwealth. There is no general legal right; instead where that term is used it is taken to be a statement of principle in support of some other already recognized right or cause of action. This is in sharp contrast to the United States where many states recognize a right to privacy which is articulated and protected by the common law. Ironically, the American position was reached after being originally formulated in Warren

---

[60] An excellent account of the common law on this matter is found in The Preliminary Report on Privacy and the Law in [1971] Proc. Conf. of Comm. Uniformity Legis. 262-293.

[61] Rowan, Privacy and the Law (1973 Lectures of the Law Society of Upper Canada), p. 259, at p. 261; Neill, The Protection of Privacy (1962), 25 Mod. L. Rev. 393, at p. 394; Dworkin, The Common Law Protection of Privacy (1965), 2 Tas. U. L. Rev. 418; and Swanton, Protection of Privacy (1974), 48 A.L.J. 91. For a comprehensive account of the United States Law see Harrison, The Problem of Privacy in the Computer Age: An Annotated Bibliography (1969).

[62] The Law of Torts (4th ed., 1971), pp. 526-527.

and Brandeis' seminal article, "The Right to Privacy",[63] in 1890, which based its arguments and conclusions almost entirely on early English authorities. Why then the stark, judicial dichotomy?

The answer must surely be that referred to by Fleming:[64] the Anglo-Canadian courts lack boldness in establishing new causes of action. This may be rationalized in terms of the generally accepted view of the constitutional position of our courts, namely, that their function is to apply and not create law. Much judicial lip-service is paid to this opinion of the courts' role in society:

> The Law of tort has fallen into great confusion, but in the main; what acts and omissions result in responsibility and what do not, are matters defined by long established rules from which judges ought not wittingly to depart and no light is shed upon a given case by large generalizations about them.[65]

If this perspective of the courts' role in the law-making process had prevailed at an earlier date we would today be deprived of such causes of action as now fall under *Rylands* v. *Fletcher*[66] and *Wilkinson* v. *Downton*.[67]

In Canada there has recently been a shift towards judicial adventurism revealed in the progression of a case that was ultimately found against the plaintiff in the Ontario Court of Appeal. In *Krouse* v. *Chrysler Canada Ltd*,[68] the plaintiff sued for damages alleging that his privacy had been invaded. He was a professional football player whose likeness was used by the defendant in promoting its products (by a "spotter" competition) without his permission. The defendant brought a motion to strike out the statement of claim as showing no reasonable cause of action. This motion was refused by Parker J. who took the view:[69]

> It may be that the action is novel, but it has not been shown to me that the court in this jurisdiction [Ontario] would not recognize a right of privacy.

The case went to trial[70] and the plaintiff succeeded, not however on the basis of an invasion of his privacy, but because

---

[63] *Op. cit.*, footnote 48.

[64] *Op. cit.*, footnote 62.

[65] Dixon J., in *Victoria Park Racing and Recreation Grounds Co. Ltd* v. *Taylor et al.* (1937), 58 C.L.R. 479, at p. 505.

[66] (1868), L.R. 3 H.L. 330.

[67] [1897] 2 Q.B. 57.

[68] (1970), 12 D.L.R. (3d) 463 (Ont. H. C.). See Binchy, Torts (1974), 6 Ottawa L. Rev. 511, at pp. 555-557.

[69] *Ibid.*, at p. 464.

[70] (1972), 25 D.L.R. (3d) 49 (Ont. H. C.).

of appropriation of likeness for commercial purposes and passing-off, two property-related and relatively choate torts. But in delivering judgment, Haines J. indicated that:[71]

> [W]ere it necessary for me to decide this point [whether or not an action in invasion of privacy could be maintained] to determine the action, this novelty would not be an excuse in and of itself, for me to deny the plaintiff relief.

On appeal to the Court of Appeal, however, the decision was reversed and the privacy issue was not argued in that court.[72] We will return to this case later and examine the reasons for Krouse's failure to recover.

Although there is a marked absence of litigation[73] brought in "invasion of privacy" as such there are numerous causes of action recognized at common law and equity that do protect privacy interests.[74] In the main these are available where privacy and property or reputational interests intersect and these have been granted a measure of legal protection. The following description of various causes of action illustrates this general proposition.

(1) *Trespass to land*

Very often trespass to land is a necessary method of invading the privacy of another and an action is maintainable under this head. A trespass is "an unauthorized entry upon the soil of another";[75] whether or not intention is an essential element is still an open issue.[76] But there are three major limits placed on trespass to land as a cause of action. First, there must be actual physical penetration of the plaintiff's airspace, sub-soil or surface.[77] Also,

---

[71] *Ibid.*, at p. 56.

[72] (1974), 1 O.R. (2d) 225 (C.A.).

[73] One Canadian commentator, Cornfield, noted that at the time of writing (1967) there were only four Commonwealth articles on privacy: The Right of Privacy in Canada (1967), 25 U. of T. Fac. L. Rev. 103. In the same year Dworkin published his classic paper, The Common Law Protection of Privacy, *supra*, footnote 61.

[74] Winfield, The Right to Privacy (1931), 47 L.Q. Rev. 23; Report of the Committee on Privacy, hereinafter referred to as Younger Committee Report (1972), Cmnd 5012, App. 1; Dworkin, *op. cit.*, *ibid.*; Storey, The Infringement of Privacy and its Remedies (1973), 47 A.L.J. 498; Morison, Report of the Law of Privacy, *op. cit.*, footnote 33, pp. 15-27.

[75] Blackstone's Commentaries, Vol. 3, p. 209.

[76] Fleming, *op. cit.*, footnote 62, p. 38.

[77] Unless the defendant's acts arise out of unreasonable user of a public thoroughfare: *Hickman* v. *Maisey*, [1900] 1 Q.B. 752 (C.A.).

the plaintiff must establish that he is the occupier of the land affected. Finally, although an action may be brought without proof of damage, if no real damage is established only a nominal award will follow.

The problem of damages can be overcome by applying for punitive damages in appropriate cases. These may be described as "a sum of money awarded in excess of any material loss by way of solatium for an insult or other outrage of the plaintiff's feelings that is involved in the injury complained of"[78] and are designed to punish the defendant. For example, in *Loudon* v. *Ryder*,[79] a case of trespass and assault, the plaintiff received substantial punitive or exemplary damages in excess of her actual damage, where the defendant broke into her apartment and tried to turn her out. Although doubt may now be cast on the ability of an English court to make such an award in the light of *Rookes v. Barnard*,[80] it is fairly clear that in Canada our courts have such jurisdiction.[81]

Indeed such a case is *Parkes et al.* v. *Howard Johnson Restaurants Ltd et al.*[82] where a defendant landlord, wishing to be rid of the plaintiff tenant, tried to force the tenant to leave by smashing a padlock, removing doors, interrupting the elevator service, cutting off the heating and interfering with the electricity supply. In this case, having distinguished *Rookes* v. *Barnard*, the court held that it was appropriate to grant punitive damages and awarded the sum of $4,000.00.

Rowan has suggested[83] that the courts may one day grant a remedy for mental suffering caused by trespass which may even be extended to an occupier's family. A first step in this direction may perhaps be seen in the decision of the Victoria Supreme Court in *Grieg* v. *Grieg*.[84] There, a microphone had been installed in the plaintiff's flat and damages were awarded to compensate

---

[78] Salmond on Torts (15th ed., 1969), p. 716.

[79] [1953] 2 Q.B. 1225.

[80] [1964] A.C. 1129.

[81] *McElroy* v. *Cowper-Smith and Woodman*, [1967] S.C.R. 425 (S.C.C.); *Bahner* v. *Marwest Hotel Company Ltd, Muir et al.* (1969), 6 D.L.R. (3d) 322 (S.C.B.C.); (1970), 12 D.L.R. (3d) 646 (C.A.B.C.); *Pretu* v. *Donald Tidey and Co. Ltd* (1966), 53 D.L.R. (2d) 509 (Ont. C.A.); *cf. Banks* v. *Campbell* (1974), 45 D.L.R. (3d) 603 (N.S.S.C.).

[82] (1970), 74 W.W.R. 255 (B.C.S.C.).

[83] *Op. cit.*, footnote 61, at p. 267.

[84] [1966] V.R. 329.

the plaintiff's "hurt feelings" resulting from the invasion of his privacy[85] through the trespass.

As well as punitive damages, aggravated damages may properly be claimed in certain situations of trespass to land. This class of damages is described as being awardable "when the motives and conduct of the defendant aggravate the injury of the plaintiff".[86] Insult and injured feelings are a proper subject for compensation. In such cases the award is regarded as being part of the actual injury sustained by the plaintiff and thus not directly concerned with punishment of the defendant. Such damages are at large and part of the claim for an award of general damages.[87]

But although trespass to land may afford a modicum of protection where an invasion of privacy occurs through physical entry to a plaintiff's "land", as, for example, spying on him or planting listening devices, it cannot be resorted to where no such entry has occurred. Thus it is of no assistance where the listening device consists of a splice in a telephone cable a block away or where the surveillance is by telescope from private property.[88]

(2) *Trespass to chattels*

This tort comprises a deliberate, unauthorized interference with a chattel in the possession of another. The interference must be direct and actual damage need not be proved.[89] In some very isolated cases, trespass to chattels may afford a measure of privacy-protection. Usually, compensation to be meaningful will have to be based on punitive or aggravated damages in the absence of loss or destruction of the chattel or where the chattel itself is of little value.

An illustration would be the case of a person picking up a letter addressed to another, in that other's home, opening and reading it. This would constitute a trespass to chattels but the real damage to the plaintiff is not in the torn envelope but in his

---

[85] See, too, the example of *Sheen* v. *Clegg*, Daily Telegraph, dated June 22nd, 1961, where damages in trespass were awarded where the defendant had installed a microphone over the plaintiff's marriage bed. It is referred to by Harum, Right of Privacy in Europe, [1970] Am. Bar Assoc. J. 673, at p. 674.

[86] Salmond on Torts, *op. cit.*, footnote 78, p. 716.

[87] Punitive damages, on the other hand, are regarded as special damage and must be particularly pleaded by the plaintiff. This is really anomalous because by their nature they, too, are incapable of precise calculation.

[88] See Dworkin, *op. cit.*, footnote 61, at pp. 422 *et seq.* for a full list of the gaps in the common law.

[89] Fleming, *op. cit.*, footnote 62, at pp. 49-50.

loss of privacy. If the defendant managed to read a letter lying on the plaintiff's table, without touching it, there would be no trespass at all, merely an unactionable invasion at common law of the victim's privacy.[90]

Accordingly, this tort is of limited application in the sphere of protecting privacy interests.

(3) *Trespass to the person*[91]

The torts falling under this head, too, provide little direct protection for privacy:

> If trespass to the person had developed differently — if, that is to say, it had come to include in the concept of a person something of his intangible personal dignity and feelings, as distinguished from his personal person, it could have become a powerful means for protecting privacy. But physical interference with a person — or threats of it — are essential to the action of trespass to the person. The latter will not therefore cover many invasions of privacy — such as spying on a person — which do not involve any physical interference with him or threats of such interference. However, the action of trespass to the person is an appropriate and effective remedy for some cases of invasion of privacy, as where a person is compelled under protest to submit to a medical examination.[92]

(4) *Nuisance*[93]

Private nuisance is usually associated with some indirect invasion of the plaintiff's occupational interest in land which unreasonably interferes with his enjoyment of it. Subject to one exception it is largely confined to physical interference, which reveals its basic limitation for our purpose. This exception relates to watching and besetting a man's house or business with the purpose of compelling him to pursue, or not to pursue a particular course of conduct.[94]

An interesting illustration of "watching and besetting" is *Poole and Poole v. Ragen and The Toronto Harbour Commissioners*.[95] There the plaintiffs successfully brought an action for damages and an injunction to restrain the defendants from inter-

---

[90] This assumes the situation to be one where it was not reasonable or justifiable for the defendant to interfere with or read the letter.

[91] Encompassing the torts of battery, assault and false imprisonment.

[92] Younger Committee Report, *op. cit.*, footnote 74, p. 291.

[93] Younger Committee Report, *ibid.*

[94] *J. Lyons and Sons* v. *Wilkins*, [1898] 1 Ch. D. 255, at p. 267, per Lindley M.R., and the Younger Committee Report, *ibid.*, p. 292.

[95] [1958] O.W.N. 77 (H. C.); *cf. 286880 Ontario Ltd* v. *Park et al.* (1975), 6 O.R. (2d) 311 (H. C.), where an injunction was refused on the facts.

fering with their right of navigation in Toronto harbour.[96] They alleged that the Toronto Harbour Police followed their boat back and forth across the harbour for a period of three months. In finding in favour of the plaintiffs, and granting an injunction and damages in the amount of $2,000.00, McLennan J. said:

> The test whether conduct is a nuisance or not is the effect of such conduct on the average reasonable man. In my opinion the conduct of the Harbour Police was something more than mere personal inconvenience and interference with enjoyment of one's quiet and one's personal freedom or anything that discomposes or injuriously affects the senses or the nerves.... I think it would be an affront to the dignity of any man or woman and was such to these plaintiffs and, unless justified, it is an actionable nuisance....[97]

If this case sets up the proposition that unreasonable surveillance causing injury to another will constitute a nuisance, either private or public, then it is of the utmost importance in an evolving common law protection of privacy.

It must be compared, however, with the decision of the High Court of Australia in *Victoria Park Racing and Recreation Grounds Co. Ltd* v. *Taylor et al.*[98] There it was held that the erection of a viewing platform alongside a race course with the purpose of broadcasting the running of races did not constitute an invasion of the privacy of the race course proprietor nor did it constitute an actionable nuisance.[99] Perhaps the *Poole* decision can be distinguished on the ground that it is closer to the traditional notion of "watching and besetting", over a long period of time in a threatening, albeit covert, manner. Whereas in the *Victoria Park* case there was no threat actual or implied, merely the use of a technique to make commercial gain that damaged the plaintiff's own commercial goals, namely to ensure that the Parkway was attended by paying customers.

A more realistic view is taken by Dworkin,[100] who considers that the majority in the *Victoria Park* case merely adopted a narrow and inflexible view of the limits of nuisance, one that is no longer maintainable in the light of modern technology permit-

---

[96] This was a public nuisance action, the plaintiff's "injuries" being clearly different from that suffered by the other harbour users.

[97] *Supra*, footnote 95.

[98] *Supra*, footnote 65; reference should also be made to the case of "The Balham Dentist" who unsuccessfully sued his neighbours to prevent them from observing him treating his patients by medium of specially arranged mirrors in their property: Dworkin, *op. cit.*, footnote 61, at p. 423.

[99] On this last point, however, the court was divided 3-2.

[100] *Op. cit.*, footnote 61, at pp. 423-424.

ting almost limitless surveillance and interference with the plaintiff's person or property whether real or personal.

Assuming, however, that *Poole* reveals the true direction of the law of nuisance and that Dworkin's desire to liberalize its confines is shared by the courts then this tort is one that could give considerable impetus to privacy protection.

(5) *Defamation*

If a defamatory statement is published about another an action may lie.[101] But such an action is hedged with substantive restrictions that in large measure bar protection for pure privacy interests. Truth is an absolute defence as are privilege and fair comment on a matter of public interest. The plaintiff in the *Red Kimono* case[102] for example, would have been faced with the defence of justification (truth) had the fact-pattern occurred at that time in Canada and an action brought in libel.

On the other side of the coin, there are instances of privacy interests gaining protection under this tort. In *Tolley* v. *Fry*[103] the plaintiff succeeded in libel where his status as an amateur golfer was jeopardized as the result of a misleading advertisement which seemed to suggest that he had granted the use of his likeness for commercial gain.

In the United States, there seems to have been a tendency for the evolving law of privacy to absorb and replace that of defamation rather than for defamation to expand to embrace privacy interests.[104] It would appear, then, that defamation cannot be seriously regarded as an action that could be developed to protect the "right to privacy" unless its present boundaries were substantially expanded.

(6) *Injurious falsehood*

A plaintiff may bring an action, and incidentally protect his privacy, for a false statement that has been dishonestly or improperly made and calculated to cause pecuniary damage to him.[105] Such a statement will be actionable even if it is not

---

[101] See Fleming, *op. cit.*, footnote 62, pp. 455-525.

[102] *Melvin* v. *Reed, supra*, footnote 48.

[103] *Supra*, footnote 49. On the other hand in *Sim* v. *Heinz Co.*, [1959] 1 W.L.R. 313, an injunction was refused the applicant, a well-known actor whose voice had been imitated in an advertisement, because he could not establish "irreparable harm".

[104] Wade, Defamation and the Right to Privacy (1962), 15 Vand. L. Rev. 1093.

[105] Fleming, *op. cit.*, footnote 62, pp. 621-626.

defamatory as long as the plaintiff suffers actual loss of prospective advantage. In *Shepherd* v. *Wakeman*[106] recovery was made where the defendant wrote to the plaintiff's fiance claiming that she was his (the defendant's) wife resulting in the impending marriage being broken off.

(7) *Wilful infliction of nervous suffering*[107]

Where a person wilfully does an act calculated to cause harm to another and thereby infringes his legal right to personal safety, and thereby causes physical harm through mental distress, a cause of action may lie.[108] Thus in *Wilkinson* v. *Downton*[109] a practical joker who had falsely informed the plaintiff that her husband had been severely injured in an accident was held liable to her. Again, in *Janvier* v. *Sweeney*[110] the plaintiff, a French woman, recovered damages where the defendants had posed as police officers searching for evidence of espionage activities by her in order to obtain compromising letters.

The limiting feature of this cause of action seems still to be that manifestations of physical harm must accompany the mental suffering.[111] This tort, if not confined to personal safety and expanded to injured dignity as well as mental suffering as such, could cut a heavy swathe through the variegated privacy interests that currently are unprotected. For such a tort to be effective the requirement of accompanying physical harm would naturally have to be dropped. At the present time, however, there is no indication that the tort will develop along these lines.

(8) *The law of contract*

Sometimes breach of contract can be the vehicle for protecting privacy interests. In *Pollard* v. *Photographic Company*,[112] the defendant took a photograph of the plaintiff in his studio and later used the negative for his own purposes. The plaintiff suc-

---

[106] (1662), 1 Sid. 79.

[107] Fleming, *op. cit.*, footnote 62, pp. 32-36.

[108] *Wilkinson* v. *Downton*, *supra*, footnote 67.

[109] *Ibid.*

[110] [1919] 2 K.B. 316.

[111] Some writers argue that such physical harm may not now be a necessary condition for recovery: Williams, Tort Liability for Nervous Shock in Canada, in Linden (ed.), Studies in Canadian Tort Law (1968), pp. 139 *et seq.* Whereas others argue that even if physical manifestations of harm are a necessary condition to recovery this requirement should be abandoned: Dworkin, *op. cit.*, footnote 61, at p. 444, and Glasbeek, Outraged Dignity — Do we Need A New Tort? (1968), 6 Alta L. Rev. 77.

[112] (1888), 40 Ch. D. 345.

ceeded in an action for breach of contract and for an injunction to prevent the continued unauthorized use of the negative. It was held that there was an implied term of the contract that the defendant would not use copies of the photograph for his own purposes.

The same result may accrue from a breach of copyright as occurred in *Williams* v. *Settle*[113] another case involving a photographer who used a photograph for his own purposes.

(9) *Passing-off and appropriation*

"If a person in selling or offering for sale his goods or services makes a false representation calculated or likely to deceive the public, to the effect that the goods or services are the goods or services of the plaintiff or that the plaintiff is somehow connected with the goods or services, then he may be liable for the tort of passing-off or unfair trading."[114] At one time this form of action was not considered to be particularly wide in scope because it was necessary to show that there was a common field of endeavour between the plaintiff and defendant in order for a plaintiff to succeed.[115]

However, in *Henderson* v. *Radio Corporation Pty Ltd*[116] the New South Wales Court of Appeal held that to establish passing-off it was not necessary that the plaintiff and defendant share a common field of activity. The court held that if this was necessary ". . . any business might falsely represent that his goods were produced by another provided that other was not engaged or not reasonably likely to be engaged, in producing similar goods".[117] It considered that this was not a sound principle and allowed the plaintiff a remedy.

The development of this tort is very desirable if the common law is to keep pace with changing conditions. As Dr. Pannam[118] aptly described the matter, "it is outrageous to think that a person could appropriate the business reputation of another and then thumb his nose at all legal attempts to restrain him".

---

[113] [1960] 1 W.L.R. 1072.

[114] Rowan, *op. cit.*, footnote 61, at p. 275; see also Pannam, Unauthorized Use of Names or Photographs in Advertisements (1966), 40 Aust. L.J. 4.

[115] *McCulloch* v. *Lewis A. May (Produce Distributors) Ltd*, [1947] 2 All E.R. 845.

[116] [1960] S.R. (N.S.W.) 576.

[117] *Ibid.*, at p. 593.

[118] *Op. cit.*, footnote 114, at p. 8.

In Ontario, however, the *Henderson* case was recently distinguished and the Ontario Court of Appeal reaffirmed the narrow position outlined above. In *Krouse* v. *Chrysler Canada Ltd*[119] it was held:[120]

> Traditionally the Courts have restricted this doctrine to proceedings where the plaintiff and defendant are competing in a common trade or are each commercially associated in a common sector of the commercial world.

On the facts of the case, the court went on to the view that the respondent had no claim in passing-off because:[121]

> . . . the buying public would not buy the products of the appellant on the assumption that they had been designed or manufactured by the respondent, nor would the public be understood to have accepted the spotter as being something designed and produced by the respondent. Finally, the spotter was not produced by the appellants to be passed off on the public in competition with a similar product marketed by the respondent.

On the other hand, the *Henderson* case has been followed in the British Columbia Supreme Court. In *Falconbridge Nickel Mines Limited* v. *Falconbridge Land Development Co. Ltd*,[122] Macfarlane J. said, while granting an injunction:[123]

> Counsel for the plaintiff concedes that the plaintiff and defendant are not competitors, but contends, and in my opinion rightly, that the plaintiff need not establish an overlap of business activity. . . .

Krouse was not referred to in this judgment and the question remains: how will the other provincial courts treat passing-off? Will they follow *Krouse* or *Falconbridge*? The issue is not a critical one in those provinces with general privacy statutes since even if the passing-off action is not maintainable an action in invasion of privacy is likely to lie. But in the other provinces the decision to follow *Krouse* instead of *Falconbridge* would stultify the remedial effects of this tort.

As well as passing-off, there is also an emerging tort of appropriation of personality. Fleming describes it as any unconsented appropriation for commercial purposes of someone else's attributes of personality, such as his name, picture, or even

---

119 *Supra*, footnote 72.

120 *Ibid.*, at p. 234, per Estey J.A.

121 *Ibid.*, at p. 236, per Estey J.A.

122 [1974] 5 W.W.R. 385.

123 *Ibid.*, at p. 388.

voice, provided it has or is likely to cause him injury in his property, business, or profession.[124]

There is now some considerable weight to the view that this tort exists as the result of *Krouse*, where the Ontario Court of Appeal, although not finding a remedy on the facts, concluded:[125]

> [F]rom the foregoing examination of the authorities in the several fields of tort related to the allegations made herein... the common law does contemplate a concept in the law of torts which may be broadly classified as an appropriation of one's personality.

(10) *Breach of confidence*[126]

Under the court's equitable jurisdiction to prevent any abuse of confidence, a certain measure of protection of privacy can be attained. In fact the Younger Committee *Report*[127] states that this remedy protects privacy as such more than any other and recommended that the Law Commission examine this branch of the law with a view to its clarification and statement in legislative form.[128]

However, all would not agree with this view. In his report to the New South Wales Parliament, Dr. Morison[129] disagreed with the recommendations of the Younger Committee because he felt that the courts were still in an exploratory stage concerning this cause of action and the time was therefore not ripe for codification.

The leading case in this area is *Prince Albert* v. *Strange*[130] where the defendant was prevented from publishing both etchings made by Prince Albert and a list of the etchings which the defendant had prepared based on information which he knew was originally disclosed in breach of confidence. This case is important for two reasons: the plaintiff had no copyright, and the defendant

---

[124] *Op. cit.*, footnote 62, p. 629. See also Mathieson, Comment (1961), 39 Can. Bar Rev. 402.

[125] (1974), 1 O.R. (2d) 225, at p. 238, per Estey J.A.

[126] See Dworkin, Confidence in the Law (1971), Univ. of Southampton; Jones, Restitution of Benefits Obtained in Breach of Another's Confidence (1970), 86 L.Q. Rev. 483; Forrai, Confidential Information — A General Survey (1971), 6 Sydney L. Rev. 382; North, Breach of Confidence: Is there a New Tort? (1972), 12 J.S.P.T.L. 149.

[127] *Op. cit.*, footnote 74, p. 295.

[128] *Ibid.*, at p. 194. See The Law Commission Working Paper No. 58, Breach of Confidence (1974), London, H.M.S.O.

[129] Morison, *op. cit.*, footnote 33, pp. 27-28.

[130] (1849), 1 Mac. B.G. 25.

had not been a party to the breach of confidence. Another important case is *Argyll* v. *Argyll*.[131] There a wife successfully obtained an injunction to prevent disclosure of matters arising out of her marriage. It was held that her former husband could not make such disclosure in a series of newspaper features he was proposing to publish. The court based its decision on *public policy* since she had no *property interest* in the material concerned.

The court's jurisdiction today seems to be based on the duty to be of good faith rather than concern to protect proprietary or contractual matters. This was made clear in *Fraser* v. *Evans*[132] where the plaintiff was a public relations consultant under an obligation of confidentiality to the Greek government, to whom he made a report. The report, from sources in Greece, came into possession of a British newspaper. The plaintiff applied for an injunction to restrain publication, which was refused. Although he was under an obligation of confidence it was not reciprocal. During the course of his judgment Lord Denning M.R. said:[133]

> No person is permitted to divulge to the world information which he has received in confidence, unless he has just cause or excuse for doing so. Even if he comes by it innocently, nevertheless once he gets to know that it was given in confidence, he can be restrained for breaking that confidence. But the party complaining must be the person who is entitled to the confidence and to have it respected. He must be the person to whom the duty of good faith is owed.

From this short outline of the common law and its effect on protection of privacy, it can be seen that apart from special instances there is little chance of a body of coherent rules being developed. Instead the legislatures must be regarded as the bodies to turn to if privacy as a vital social state is to be reinforced by legal action.

2. *Miscellaneous Statutory Remedies.*

Various discrete statutory provisions, both provincial and federal, have granted measures of reinforcement to the right to privacy in the past.

---

[131] [1967] Ch. 302.

[132] [1969] 1 Q.B. 349 (C.A.).

[133] *Ibid.*, at p. 361. For an interesting Canadian illustration see *Slavutych* v. *Baker et al.* (1975), 55 D.L.R. (3d) 224, where the Supreme Court of Canada ruled that where a document concerning a colleague had been solicited from a tenured university professor on the clear understanding that it was to be used only for a particular limited purpose, such document could not subsequently be used against the professor in dismissal proceedings as evidence of his inability to form objective judgments. See also *Bell* v. *University of Auckland*, [1969] N.Z.L.R. 1029.

Sometimes the statute in question has been interpreted in a patently strained way to achieve the desired result. This occurred in *Re MacIsaac and Beretranos et al.*[134] where a landlord repeatedly entered onto rented premises in breach of section 46 of the former British Columbia Landlord and Tenant Act.[135] The trial judge found that section 46 created a statutory right of privacy and awarded the applicant $200.00 damages. One of the grounds for so finding was that there was no penalty imposed if the landlord violated the section.

This decision achieved a desirable result for what are obviously wrong reasons. The trial judge, Levy Prov. Ct J., was of the opinion:[136]

> In legislating s. 46, the provincial legislature must have considered the common law right to privacy, and the need to incorporate that right in a statute, thereby creating a statutory tort.

The only basis for this conclusion was the article in the 1890 *Harvard Law Review* by Warren and Brandeis;[137] questionable authority at best! Instead, an action for breach of contract could properly have been maintained since a breach of section 46 was also a breach of a tenant's right to quiet enjoyment of the property, a contractual right under the Act.

There are a variety of criminal and quasi-criminal provisions that are designed to protect privacy interests or do so incidentally. It is an indictable offence to publish a defamatory libel.[138] Unlike the tort of defamation, where truth is an absolute defence, the crime of defamatory libel is only susceptible to the defence of truth if the matter and manner of publication *was also for the public benefit* at the time of publication.

A number of other such offences occur in the Criminal Code; for example, section 171 deals with miscellaneous disturbance and loitering offences, and section 173 regarding loitering

---

[134] (1972), 25 D.L.R. (3d) 610 (Prov. Ct B.C.).

[135] R.S.B.C., 1960, c. 207. S. 46 reads: "Except (a) In cases of emergency; or (b) with the consent of the tenant given at the time of entry; or (c) where the tenant abandons the premises the landlord shall not exercise a right to enter the rented premises unless he has first given written notice to the tenant of at least twenty-four hours before the time of entry, and the time of entry shall be between the hours of eight in the forenoon and nine o'clock in the afternoon as specified in the notice."

[136] *Supra,* footnote 134, at p. 614.

[137] *Supra,* footnote 48. See Pratt, The Warren and Brandeis Argument for a Right to Privacy, [1975] Public Law 161.

[138] Criminal Code, R.S.C., 1970, c. 34, as am., s. 264.

and prowling at night on another's property near a dwelling house and section 177 concerning the spread of false news are merely illustrative.

A striking example of how the criminal process may be used to protect privacy is revealed in the case of *R.* v. *Chapman and Grange.*[139] There, the two accused were charged with conspiracy under section 432(2)(a) of the Criminal Code in that they entered into an agreement to effect an unlawful purpose, namely, to divulge the purport or substance of a conversation or message, having acquired knowledge of the conversation or message over a telephone line when the conversation or message was not intended for them. In short: conspiracy to wiretap and pass on the information so obtained.

The accused had "bugged" a union headquarters building and had acted on and divulged the information that they had obtained. The wording of the indictment was the same as that contained in a penal provision of the Ontario Telephone Act.[140] The accused were convicted and appealed. One of their main arguments was that the Ontario provision, section 112, was *ultra vires* since it was criminal law and that as eavesdropping was not an offence at common law the conspiracy had not been made out.

The Ontario Court of Appeal held section 112 to be *intra vires* and since it rendered wiretaps and disclosure unlawful (as provincial offences) it was a *crime* of conspiracy for two or more persons to agree to effect this, thus through a combination of a provincial statute and the Criminal Code elements of privacy received protection.[141]

A more interesting case is *Re Copeland and Adamson et al.*[142] There a policy statement of the Board of Commissioners of Police for Metropolitan Toronto was issued empowering peace officers to employ audio surveillance if they had the approval of the chief of police and where reasonable and probable cause existed for the belief that a criminal offence was or would be committed.

---

[139] (1973), 20 C.R.N.S. 141 (Ont. C.A.).

[140] R.S.O., 1970, c. 457.

[141] A nice constitutional question of paramountcy will no doubt now arise as a result of the federal Protection of Privacy Act, *supra*, footnote 2, discussed *infra*.

[142] (1972), 28 D.L.R. (3d) 26.

The applicant, a lawyer, brought a motion for an order of *mandamus* to direct the chief of police to desist from such practice because it violated section 112 of the Ontario Telephone Act,[143] section 25 of the incorporating Bell Telephone Company of Canada Act,[144] and section 1(a) of the Canadian Bill of Rights.[145]

The application was dismissed. There was no violation of section 112 of the Telephone Act because that section contained a saving clause allowing a person to divulge the contents of a message if authorized to do so. Nor was there a violation of the Bell Telephone Act because wire-tapping does not impede the conversation between the parties, and the argument under the Bill of Rights was rejected on the ground that the section is only declaratory of rights and provides no means to enforce them. Furthermore, at common law, a person had no legally enforceable right to privacy of his conversation, even if held on a telephone, and the right to enjoyment of property would not include such a right.

Although denying the applicant's motion in *Copeland* the court did express sympathy with the applicant's position:[146]

> It would appear therefore that there is a pressing need for legislation in Canada providing protection to the individual against such abuses and regulating the area within which such devices may be lawfully used.

Today, this matter would be governed by the substantive provisions of the Criminal Code contained in Part IV.1 that deal specifically with invasion of privacy by electronic eavesdropping and set up safeguards to prevent them from occurring.[147]

A further line of cases of recent origin reveal that privacy is an interest that is judicially recognized as being in need of protection and that the courts will attempt to achieve this by expanding existing remedies where this can be reasonably done. These cases deal with the "right to counsel" that an accused has pursuant to section 2(c)(ii) of the Canadian Bill of Rights.[148]

In *R.* v. *Penner*[149] the accused was arrested on suspicion of impaired driving and a demand for a sample of his breath was

---

[143] *Supra*, footnote 140.

[144] S.C., 1880, c. 67.

[145] R.S.C., 1970, Appendix III. S. 1(a) deals with the right to enjoyment of property.

[146] *Supra*, footnote 142, at p. 37, per Grant J.

[147] These provisions are discussed in Part 4, *infra*.

[148] *Supra*, footnote 145.

[149] [1973] 6 W.W.R. 94, 12 C.C.C. (2d) 468 (Man. C.A.).

made pursuant to section 235(2) of the Criminal Code, while at the police station the accused asked if he might telephone his lawyer. This request was granted but a further request to telephone in private was refused. It was found as a fact that the police were able to overhear the accused's conversation and that it would have been possible to observe the accused on the telephone without overhearing him. In quashing the conviction of the accused for refusing to provide a sample of his breath, Hall J.A. stated:[150]

> In my view the right to retain and instruct counsel carries with it the essential element of privacy, and the failure to grant it in the circumstances of this case was a substantial interference, with such right. It affords a reasonable excuse for failure of the accused to comply with the demand.

The decision in *Penner* has been reinforced by the same court in *R.* v. *Makismchuk*.[151] There the Manitoba Court of Appeal held that the right to privacy, which is included in the right to counsel, is an inherent right and it is not necessary to ask for such privacy. It is sufficient if he asks to retain and instruct counsel.[152]

These criminal and quasi-criminal provisions are quite discrete and very often result from expansive constructions placed on them by the courts. Apart from the "Protection of Privacy" portion of the Criminal Code (Part IV.1) they are not intrinsically concerned with privacy. The privacy interests protected are merely adjunctive to the primary thrust of the enactments. They do provide, however, a vehicle for the courts to protect privacy interests regarded as being of a high order of social value where such a liberal interpretation is not inconsistent with their objects and does no violence to the language used.

III. *Canadian Provincial Experiments in Privacy Protection.*

As a result of the common law's failure to accommodate itself to what was perceived as an imminent threat to important privacy interests a number of legislative schemes have been adopted as palliatives. The initiative was taken by the provinces pursuant to their jurisdiction over property and civil rights[153] and more

---

[150] *Ibid.*, at p. 96 (W.W.R.); see also *R.* v. *Balkan*, [1973] 6 W.W.R. 617; *R.* v. *Levy* (1973), 21 C.R.N.S. 292; *R.* v. *Straightnose*, [1974] 2 W.W.R. 662; *R.* v. *Walkington*, [1974] 2 W.W.R. 454; and *R.* v. *Doherty* (1974), 25 C.R.N.S. 289 (N.S.C.A.).

[151] [1974] 2 W.W.R. 668, 15 C.C.C. (2d) 208.

[152] Compare *Makismchuk*, *ibid.*, with *R.* v. *Stasiuk* (1974), 25 C.R.N.S. (Sask. Dist. Ct) where it was held that the accused must *ask* for such private communication with his counsel.

[153] S. 92 (13) of the British North America Act, 30 & 31 Vict., c. 3 (U.K.).

recently by the federal government under its criminal law-making powers.[154] This part is concerned only with the provincial experiments and they can be classified under two heads: general privacy-protection legislation and specialist legislation controlling the gathering and use of personal data.[155]

1. *The Early Years.*

In November 1966, an officer of the Pulp and Paper Workers of Canada publicly alleged that electronic listening and recording devices had been used to "bug" rooms in a Vancouver hotel where the union was holding its convention. A private detective, who had formerly been with the Royal Canadian Mounted Police had been engaged by the rival International Pulp and Sulphite Workers Union to plant the bugging devices and two officers of the Security and Intelligence Branch of the Royal Canadian Mounted Police were actively involved in the affair.

As a result of this incident, on November 9th, 1966,[156] Judge Rey Sargent was appointed a Commissioner under the Public Inquiries Act[157] to inquire into this invasion of privacy and report his findings and recommendations.[158] However, after ten days of hearings, the validity of the Order in Council setting up his jurisdiction was attacked and it was struck down as being an improper exercise of the Public Inquiries Act.[159] The Commission of Inquiry was reinstated by Order in Council dated January 3rd, 1967[160] with the terms of reference considerably wider than they had been:[161]

---

[154] S. 91 (27), *ibid.*

[155] Three provinces have enacted legislation of both types: British Columbia (1968 and 1974), Manitoba (1970 and 1971), and Saskatchewan (1972 and 1974). In the United Kingdom there have been four unsuccessful attempts at enacting privacy legislation. For the text of all British Parliamentary and Draft Right of Privacy Bills see the Report of The Committee on Privacy, *op. cit.*, footnote 74, Appendix F. See too, Dworkin, The Younger Committee Report on Privacy (1973), 36 Mod. L. Rev. 399, and Taylor, Privacy and the Public (1971), 34 Mod. L. Rev. 288, for the reasons for such legislative failure.

[156] Order in Council, [1966] B.C. Gazette 2727.

[157] R.S.B.C., 1960, c. 315.

[158] Sargent, Report of the Commission of Inquiry into Invasion of Privacy, Aug. 9th, 1967, pp. 1-2 (B.C.), hereinafter cited as B.C. Commission Report.

[159] *R. ex rel. McPhee* v. *Sargent* (1967), 60 D.L.R. (2d) 641.

[160] [1967] B.C. Gazette 48-49.

[161] B.C. Commission Report, *op. cit.*, footnote 158, p. 2.

> [I]t deemed expedient to cause inquiry to be made into ... the nature and extent of the use of electronic and other listening and recording devices and records thereof for the purpose of invading the privacy of persons or organizations and ... the nature and extent of the apparent use of such devices and records by ... private detectives ... or their clients and the justification, if any, for and the background of such use, with a view to determining whether any legislative enactment or amendment or extension of the substantive law is necessary for the preservation of privacy as a civil right.

This was the first formal inquiry into the right to privacy in Canada and the Commission *Report* was published in August 1967. Although the *Report* contained no summary of conclusions the major recommendations were:[162]

> 1. Legislation is necessary to regulate the use and prevent the abuse of electronic devices. Federal legislation is preferable. However, there is nothing to prevent at the present time the Provincial Legislature from enacting legislation which would render it a Provincial offence to eavesdrop, and it is my suggestion that the ancient English crime of eavesdropping be revised and recast to meet our modern problems.
> 2. I also suggest that the possession of equipment which is capable of infringing privacy or receiving or monitoring police calls be made a crime with the onus on the accused to prove that he did not have it in his possession for that purpose.
> 3. "Appropriate legislation" should be enacted to give a civil right of action for the invasion of privacy.... Draft bills already presented to the Provincial Legislature relating to the invasion of privacy could be used as the starting point for such legislation.
> 4. Private detectives finding need to use electronic devices would have to apply to a judge of the County Court and show cause in each case.
> 5. Federal Authorities should have the untrammelled right to use electronic or other devices as may be necessary for the peace, protection and good government of Canada.
> 6. The police should have the right to use these devices where necessary to carry out their duty. The Criminal Code procedure for obtaining a search warrant on application to a justice is considered and rejected in favour of a procedure based on the writ of assistance system authorized by certain federal statutes.... I have come to the conclusion that for efficient and prompt use the Federal system of writs of assistance to responsible officers be issued by the Chief Justice of the Supreme Court of British Columbia upon the nomination by the Attorney General of British Columbia.
>
> This appointee would be an officer mature and skilled and on him would devolve the responsibility for authorizing the use of these devices and also the onus for their abuse.

Although this *Report* has been severely criticized,[163] nevertheless it marked the beginning of an awareness in this country

---

[162] Atrens, Comment on the Report of the Commission of Inquiry into the Invasion of Privacy (1968), 10 Crim. L.Q. 138, at pp. 141-142.

[163] Ryan, The Invasion of Privacy by Electronic Listening Devices in Canada (1970), 8 Col. I. Dr. Comp. 87; and Atrens, *op. cit.*, *ibid.*

that there was a need for protection of privacy. A direct consequence of the Commission *Report*, whether or not reflecting its content, was the passage of the British Columbia Privacy Act[164] in 1968 which was the first legislation of its kind in Canada and the Commonwealth.

Also in 1968 the Ontario Law Reform Commission presented a study on invasion of privacy to the Attorney General for that province.[165] This *Report* recommended, *inter alia*, the creation of both an offence and a tort of invasion of privacy. As well, the report made extensive recommendations respecting electronic surveillance devices, credit reporting and disclosure of personal information, computer banks, and the suggestion that the right to privacy be included as a fundamental right in proposed human rights legislation.[166] The *Report* also recommended that the Ontario government establish a Royal Commission to investigate invasion of privacy in depth.

On May 2nd, 1969, the Legislative Assembly of Alberta appointed a special legislative committee to examine all matters relating to the invasion of privacy. The resulting *Report*[167] was unfortunately quite superficial and had nothing to add to the existing literature. Its only concrete recommendations were in the area of credit reporting.[168] However, the *Report* did state that "if this Committee has contributed to a growing awareness of the amount of information being gathered about each citizen, and the manner in which this information can be manipulated either for good or evil, the Committee's work will have been worthwhile".[169] This statement of concern is of considerable political significance. There is an urgent need for Canadian society to become aware of the potential threats to its institutions and culture by the saturation effects of numerous privacy invasions that may appear trivial in themselves. If present invasion of privacy is characterized as a snowball starting down a mountain, we may not become aware of its danger until it has reached the base and caused irreversible damage.

---

[164] *Supra*, footnote 1.

[165] Ontario Law Reform Commission, Report on Protection of Privacy in Ontario (Preliminary Study) (1968).

[166] *Ibid.*, pp. 73-74, and discussed at pp. 75-100.

[167] Special Legislative Committee on Invasion of Privacy, A Report to the Alberta Legislature (1970).

[168] *Ibid.*, pp. 54-56.

[169] *Ibid.*, p. 6.

2. *The General Privacy Acts.*

At the present time there are three[170] Privacy Acts in force in Canada in the provinces of British Columbia,[171] Manitoba[172] and Saskatchewan.[173]

In British Columbia the statute creates a tort, actionable without proof of damage, for the unreasonable violation of the privacy of another person, wilfully and without claim of right.[174] It also creates a second statutory tort, actionable without proof of damage, for using the name or portrait of another person for advertising or promotional purposes without his consent.[175] Privacy is not defined but section 2(3) states that privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass, and section 2(2) sets out a number of factors that the court must regard in deciding the issue.[176] The same subsection makes it clear that the *fact* of invasion of privacy is *objectively* measured; then the defendant's liability will turn on his state of mind and so on.

The statute also creates a significant exception by specifying conditions whereby activities will not constitute invasions of privacy.[177] These include consent by the plaintiff, an act or conduct incidental to the lawful defence of the person or property, an act authorized or required by law, and, most important, the acts of a peace officer acting in the course of his duty for the prevention, investigation or discovery of crime and the conduct of any public officer engaged in an investigation under provincial law, so long as his actions are proportionate to the gravity of the crime or matter subject to investigation and were not committed in the course of trespass.

---

[170] In 1972, Bill 60, An Act Respecting Personal Privacy, was introduced into the Nova Scotia Legislature. This Bill was in identical terms to the B.C. Privacy Act but it did not go beyond 1st Reading.

[171] *Supra,* footnote 1.

[172] *Ibid.*

[173] *Ibid.*

[174] *Ibid.*, s. 2(1).

[175] *Ibid.*, s. 4(1).

[176] S. 2(2): "The nature and degree of privacy to which a person is entitled in any situation . . . is that which is reasonable in the circumstances, due regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of another, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties."

[177] *Ibid.*, s. 3. Privilege is also a defence.

Although hailed as "one of the most significant recent developments in the law of torts"[178] in 1968, the passage of six years has shown the Privacy Act to be a "non-development". To date there has been only one reported decision: *Davis* v. *McArthur*.[179]

There a private investigator was sued for damages as the result of his actions in obtaining evidence for pending divorce proceedings. The defendant was employed by the plaintiff's wife to investigate his conduct, and pursuant to this, together with his former partner, periodically checked his movements over a period of six months. During this time the defendant became aware that the plaintiff was also being observed by someone else and that he appeared to be aware of it.

The plaintiff and his wife agreed to separate in November 1968 but she allowed him the use of her car over the Christmas period. At her request the defendant attached a device to the rear of the car which emitted a steady signal that could be located by a receiver on the appropriate frequency. This was referred to throughout the trial as a "bumper beeper". While using the car the plaintiff slammed the trunk lid and the "bumper beeper" fell off. The plaintiff's first alarmed reaction was that the device was a bomb, but he later disconnected the batteries and was apparently not unduly concerned.

An action was brought by the plaintiff against the defendant pursuant to section 2 of the Privacy Act, counsel submitting that the "bumper beeper" was a method of electronic eavesdropping within the compass of section 2(3). Seaton J. rejected this argument, pointing out that the apparatus was merely a homing device and not one whereby a person could secretly overhear a private conversation.[180] It was also held that there was no trespass within the meaning of section 2(3). However, the defendant's actions constituted surveillance, which was specifically referred to in section 3(2) as a *means* of causing an actionable invasion of privacy.[181]

---

[178] Atrens, Comment on the Privacy Act (1968), 26 Advocate 183.

[179] (1970), 72 W.W.R. 69, 10 D.L.R. (3d) 250 (B.C.S.C.); reversed (1971), 17 D.L.R. (3d) 760, [1971] 2 W.W.R. 142 (C.A.).

[180] (1969), 10 D.L.R. (3d) 250, at p. 252. His Honour pointed out that there are several meanings of the right to privacy ("the right to be let alone", "seclusion", *etc.*) but that under the Privacy Act the respective rights and duties are not fixed and extremely elastic: *ibid.*, at p. 254.

[181] *Ibid.*, at p. 252.

In order to sustain his action, the plaintiff had to establish, pursuant to section 2(1), that the violation was "wilful". Seaton J. construed this term to mean ". . . intentionally, knowingly and purposely without justifiable excuse . . . as distinct from a negligent act".[182] Accordingly, either intention or subjective recklessness is required to be established by the plaintiff. The defendant took the position that he had a claim of right as a private investigator. This was rejected because the term "claim [or colour] of right" relates to an honest belief in a state of facts which, if it existed, would at law justify or excuse the act done.[183] Here there was no mistake of fact by the defendant. In particular, Seaton J. took the view that the Private Detective's Licensing Act[184] was a regulatory measure and did not make either an invasion of a person's property or an invasion of a person's privacy justifiable.

It neither gave the defendant a claim of right within section 2(1) nor authorization within section 3(1)(c) so as to grant a complete defence. However, this did not render the defendant's status of private investigator completely irrelevant. A private investigator may in some cases do things which would not constitute a breach of privacy whereas it may be such a breach if someone does it out of sheer inquisitiveness. This means that although every alleged invasion of privacy is a question of fact, one of the most significant factors is the motive of the defendant.[185]

The other significant factors were: the wife's right to have the enquiries made; the conduct of the plaintiff (which, over a long period, would not excite suspicion); the extent of the surveillance in thoroughness and duration; and the effect it would

---

[182] *Ibid.*, at p. 253. The learned judge also took the view that the plaintiff had to establish the defendant's absence of any claim of right. This must be open to question in the light of such authorities as *R.* v. *Turner* (1816), 5 M. & S. 206, where Bayley J. stated: ". . . [If] a negative averment be made by one party, which is peculiarly within the knowledge of the other, the party within whose knowledge it lies, and who asserts the affirmative is to prove it, and not he who asserts the negative." Of course an allegation of absence of claim of right is such a negative averment.

[183] *Ibid.*, at p. 254, following *R.* v. *Johnston* (1904), 8 C.C.C. 123, 7 O.L.R. 525, and *R.* v. *Fetzer* (1900), 19 N.Z.L.R. 428.

[184] R.S.B.C., 1960, c. 297.

[185] This general proposition was affirmed by the Court of Appeal. See *Davis* v. *McArthur* (1971), 17 D.L.R. (3d) 760, at p. 764 where Tysoe J.A. stated: ". . . I respectfully agree with the learned trial Judge . . . that the defendant's role as private investigator does not give a claim of right within s. 2(1) or authorization within s. 3(1) (c) so as to afford a complete defence, but it does not follow that his position as a private investigator is not relevant."

have upon a person. The learned judge felt that if the court regarded only the defendant's actions, they may have been reasonable having regard to the interest of the wife in obtaining divorce evidence. But the defendant was aware that the plaintiff knew he was being constantly watched (not by the defendant) during a time of considerable emotional stress, that is, during the break-up of his marriage.

Seaton J. concluded:[186]

> [T]he defendant know[s] or ought to have known that the plaintiff's privacy was being so thoroughly invaded as to cause a reasonable man to be worried, apprehensive and emotionally upset. When the conduct of a private investigator reaches that point I have no hesitation in saying that he is violating the privacy of the person he is investigating.

Section 2(2) of the Privacy Act sets out the test of an invasion of privacy in terms of reasonableness, and what the defendant did was viewed by the court as unreasonable in the circumstances. According to Seaton J.'s reasoning, however, the decision may have been different had the defendant not been aware of the other person "shadowing" the plaintiff.[187] So, although the affixing of the "bumper beeper" to the car was not in itself an invasion of privacy,[188] when it was placed in the context of the plaintiff's marital crisis and the apparent surveillance by another, the whole set of circumstances rendered the defendant's actions within the Privacy Act. The sum of one thousand dollars was awarded the plaintiff as damages.

The defendant appealed the decision, which was reversed in the Court of Appeal.[189] Delivering judgment for that court, Tysoe J.A. pointed out that the right to privacy is, *inter alia,* the right to be let alone or to be free from unwarranted publicity. Tysoe J.A. expressed the view that the trial judge had placed too much importance on the earlier surveillance since, although it would be relevant in determining the reasonableness of the defendant's conduct, its nature and extent were not disclosed in the evidence. Of more significance, though, was the trial judge's reliance on the ill-health suffered by the plaintiff (who had consulted a doctor, presumably *after* the "bumper beeper" incident) as evidence of a breach of the Privacy Act. It could

---

[186] *Supra,* footnote 180, at p. 256.

[187] Unless, of course, the defendant was "unreasonable" in not having that knowledge.

[188] It would probably have been such an invasion if the car had belonged to the plaintiff and not his wife, as well as a trespass to chattels.

[189] (1971), 17 D.L.R. (3d) 760.

properly have been taken into account in assessing the damages but not in deciding whether or not a breach of the Privacy Act had occurred. Only where there is a pre-existing state of ill-health on the plaintiff's part (as in the case of an invalid) is it likely to be relevant to the substantive question, "Has there been an invasion of privacy?" In the words of Tysoe J.A.:[190]

> The evidence does not indicate that the respondent was other than a normal healthy man who was living and carrying on his work in the manner one would expect of such a man. The knowledge that he is being watched is likely to be upsetting to anyone, but in my respectful opinion the evidence that, as it turned out, this respondent was affected as he was, is not relevant to the question of the nature and degree of privacy to which he was entitled or whether there was a violation of that right of privacy. My view is that in this case that evidence goes only to the matter of damages.

The Court of Appeal adopted the view that the appellant had acted reasonably in the light of four factors:[191]

(1) He was the wife's agent acting in her legitimate interests [*his* motive was legitimate?];
(2) His observation did not attract public attention;
(3) His observation was not offensively executed; and
(4) His observation was not unduly close or continuous.

Accordingly, the appeal was allowed and the action dismissed.

Under the Manitoba statute[192] the tort is described differently. There a person commits a tort against another when he substantially, unreasonably and without claim of right violates the privacy of another and the action may be brought without proof of damage.[193] Section 3 describes examples of invasions of privacy quite precisely and includes the second tort under the British Columbia Act. The defences open to a defendant under the British Columbia Act are all available under the Manitoba Act but with one addition.[194] Section 5(b) makes it a defence for the defendant to show that he neither knew nor reasonably should have known that his act, conduct or publication constituting a violation of privacy would have violated the privacy of any person. Thus a defendant may show that he neither knew that an invasion of privacy would result from his act and that he was not negligent

---

190 *Ibid.*, at p. 763.

191 *Ibid.*

192 *Supra*, footnote 1.

193 *Ibid.*, s. 2.

194 *Ibid.*, s. 5.

in failing to perceive that an invasion would ensue. Unlike Manitoba both the British Columbia and Saskatchewan Acts exclude negligence as a basis of liability.[195] One provision of the Manitoba Act which may be important and does not appear in either the British Columbia or Saskatchewan Acts is section 7 which declares that no evidence obtained by virtue or in consequence of a violation of privacy in respect of which an action may be brought under the Act is admissible in any civil proceedings.

To date there have been no reported cases under the Manitoba Privacy Act.

In Saskatchewan[196] the statutory tort of invasion of privacy is in general terms identical to the British Columbia Act. Section 3 also lists examples of violations of privacy as does the Manitoba Act, but a major improvement of the Saskatchewan Act over that of Manitoba is that in the Manitoba Act the section states that privacy *may* be violated by the enumerated methods. In contrast, the Saskatchewan Act states that *proof* of the same enumerated methods is *prima facie* evidence of a violation of privacy.

Both this legislation and the Manitoba Act grant the court a wide discretion as to remedies including damages, injunction, accounting of profits, an order to restore articles or documents and any other relief which appears necessary. Such a provision is absent from the British Columbia legislation.

Under section 6 of the Saskatchewan Act in determining whether there has been an invasion of privacy, the court must consider the nature and degree of privacy to which a person is entitled in any situation having due regard for the lawful interests of others. Furthermore, the nature and incidence of the act, the effect of the act, the relationship of the parties and the conduct of the parties before *and after* the act, must also be considered. Similar provisions are found in section 2(2) of the British Columbia Act and section 4(2) of the Manitoba Act. However, a unique feature of the Manitoba Act is that these provisions are to be considered by the court only when assessing damages.

---

[195] For a debate over this difference see The Protection of Privacy Act, [1972] Proc. Conf. Comm. Uniformity Legis. 202. The discussion centred on the distinction between intentional and unintentional invasion. Both British Columbia and Manitoba agreed that unintentional invasion should be excluded and did not discuss negligence. It seems, however, that under the Manitoba Act, negligent invasion of privacy *may* be a tort.

[196] *Supra*, footnote 1.

Therefore the court need not look at these factors when granting an injunction or any other remedy as provided for in section 4(1).

Another feature of the Saskatchewan Act[197] is that a publication of any matter is not a violation if the matter is on reasonable grounds believed to be *of* public interest. The Manitoba Act[198] requires belief to relate to publication *in* the public interest if it is to be a defence. Much of which is *of* public interest need not be *in* the public interest to reveal. In British Columbia,[199] on the other hand, a defence lies only if the publication *is* of public interest whatever the belief of the defendant.

An important feature of the Privacy Acts, and one which is common to each, is that an action for invasion of privacy must be instituted in the Supreme Court of each province. This may be the reason for the paucity of case-law under them. In six years the British Columbia experience has revealed only one reported decision. The high cost of litigation in the Supreme Court in addition to the added embarrassment of having the invasion made public are probably enough to deter many people with a legitimate cause of action. These factors become more stringent when one considers the type of damages a plaintiff is likely to recover for invasions. Unless punitive damages are awarded the sum is not likely to be very large. It can be argued, then, that these Acts do not grant real protection to the privacy interests they were set up to safeguard, at least, at the most visible level. It may be alternatively conjectured that the existence of the Acts has resulted in a type of "preventive-legal" situation whereby people regulate their activities to take account of them. But at this stage of their evolution, the Acts have yet to reveal their efficacy.

Finally, it should be noted that privacy is given some protection under article 1053[200] of the Quebec Civil Code which reads:

> Every person capable of discerning right from wrong is responsible for the damage by his fault of another, whether by positive act, imprudence, neglect or want of care.

---

[197] *Ibid.*, s. 2(a).

[198] *Supra*, footnote 1, s. 5(f) (1).

[199] *Supra*, footnote 1, s. 2(a). For an excellent discussion of the meaning of the term "public interest" see *London Artists Ltd* v. *Littler*, [1969] 2 Q.B. 375 (C.A.).

[200] See Glenn, Civil Responsibility—Right to Privacy in Quebec (1974), 52 Can. Bar Rev. 297. For a summary of the French law of privacy see Strömhelm, *op. cit.*, footnote 17. He points out, pp. 7 *et seq.*, that since the early nineteenth century French courts have applied art. 1382 of the Civil Code, which provides, in general terms, that anyone who inflicts an injury on another is bound to redress the wrong, to impose civil liability

In the case of *Robbins* v. *Canadian Broadcasting Corp.*,[201] the plaintiff, a doctor, had written to the producer of a television programme criticizing some features of the programme. On a succeeding edition of the same programme the name and address of the plaintiff were displayed on the screen and viewers were invited to write or telephone the plaintiff to "cheer him up". As a result, the plaintiff was subjected to a large volume of offensive letters, telephone calls, and C.O.D. gifts so that he was obliged to disconnect his telephone and suffered serious inconvenience and worry. The Quebec Superior Court found a remedy under article 1053 for the plaintiff because the defendant's servants had committed a "fault". Unfortunately, the court found there was "no need to attempt any precise definition of this fault".[202] However, in assessing damages, the court did say the "Plaintiff also has a claim for humiliation and invasion of privacy".[203] The important point of the case is that the decision did not rest on a property interest—it protected privacy *per se.*

3. *Personal Information Storage Systems.*

In very recent years there has been an increasing interest in invasion of privacy resulting from the collection and use of personal data. In 1968 the Legal Research Institute of the University of Manitoba prepared a *Report*[204] which recommended the control of commercial personal information reporting agencies. Other studies with recommendations similar to the Manitoba *Report* followed.[205]

The Manitoba *Report*[206] examined the role and practices of the commercial reporting profession in Canada and concluded

---

on acts, that involve the invasion of privacy. This is particularly true of cases concerning the violation of the secrecy of confidential letters, abuse of a person's name, and unwarranted publication of a person's image. No general theory of privacy existed and when it developed it was influenced by German views expressed in the concept of *droits de la personnalité* ("persönlichkeitsrechte").

[201] (1957), 12 D.L.R. (2d) 37.

[202] *Ibid.*, at p. 40.

[203] *Ibid.*, at p. 42.

[204] Gibson and Sharp, Privacy and Commercial Reporting Agencies, Legal Research Institute, University of Manitoba, Winnipeg (1968).

[205] Department of Communications, Conference on Computers: Privacy and Freedom on Information (Queens University, 1970); Sharp, Credit Reporting and Privacy, the Law in Canada and the U.S.A. (1970); Privacy and Computers, A report of a joint Dept of Communications and Dept of Justice Task Force (Ottawa, 1972).

[206] This study draws heavily on Commercial Credit Bureaus: Hearings before a Sub-Committee of the Committee on Government Operations, House of Representatives, 90th Congress, 2nd Sess. (1968).

that there were two major types of reporting agencies. The first is the "file" agency. In this type of operation the major credit grantors in an area agree to make available to each other through the reporting agency the payment records and other credit information of those to whom they have granted credit. This type of operation is primarily concerned with credit information on a continuing basis:

> In some file-type operations the credit grantors simply supply specific information from their own files on request, but it is more common now for them to provide an automatic continuing input of data to central files maintained by the reporting agency.[207]

This information is usually supplemented by information relating to bankruptcies, divorces, criminal convictions, promotions, and so on. Although no credit bureaus in Canada are wholly computerized, they are probably very near to it due to pressure to provide a more complete and up to date service.[208] However, even now the credit bureaus are highly mechanized with automated files and direct telephones enabling checks of prospective customers in minutes.

The second form of reporting agency is the "investigative agency". When a request for information is received by this form of agency, one of its employees investigates usually by telephone or by interviewing. This information is supplemented by data from public records as in the file-type operation. The purposes for which information is sought range from insurance applications and credit to employment and bonding. The sources of information include employers, neighbours, bankers, and so on. Two examples of the investigative type agency are Retail Credit Company of Cananda Ltd[209] and Dun & Bradstreet of Canada Ltd.[210]

The dangers the Manitoba Institute believed were threatening the privacy of individuals through credit reporting were (a) the danger of inaccurate or misleading information being reported, and (b) the danger of accurate information being used for unjustifiable purposes. The conclusions and recommendations of the Institute were:[211]

---

[207] Gibson and Sharp, *op. cit.*, footnote 204, p. 9.

[208] Privacy and Computers, *op. cit.*, footnote 205, p. 63.

[209] A wholly owned subsidiary of Retail Credit Company, an American corporation.

[210] This company specializes in investigating businesses, rather than individuals.

[211] This summary is taken from Gibson and Sharp, *op. cit.*, footnote 204, p. 31.

1. Commercial reporting should not be prohibited.
2. The commercial reporting profession should be regulated by means of licensing legislation.
3. Arrangements by which customers of reporting agencies agree not to disclose the identity of the agency to the subjects of a report should be prohibited.
4. More publicity should be given to the existence, functions and correction procedures of reporting agencies.
5. The defence of qualified privilege should be extended to the commercial reporting professions.
6. Reporting agencies should be required to notify the subjects of all reports that a report has been made, and may be examined at the office of the agency. They should also be required, when subjects insist, to forward to the recipients of the original reports, notice that the subjects dispute certain items. Sources need not be disclosed unless the licensing authority so orders.
7. Permission of the subject should not be required before a report can be made.
8. Disclosure of information to officials of a foreign government should be prohibited but disclosure to Canadian government authorities should not be prohibited, at least until the question of creating a general law of privacy has been studied more thoroughly.

To a certain extent, misuse of information by credit reporting agencies can be controlled by the law pertaining to defamation and breach of confidence.[211a] However, seven provinces in Canada have now legislated with regard to protecting privacy interests affected by such agencies.

At first glance this branch of privacy seems to be a most peculiar point to begin creating a framework of legal protection. But it is consistent with the way in which the common law itself has developed. The common law has long recognized and protected a person's property interests and interests in reputation and physical integrity from unwarranted attack. Thus, where privacy interests intersect with these other interests, attacks on them may be incidentally protected. We have such illustrations as appropriation of likeness or trade name for profit where damages and injunctive remedies can be claimed. Indeed, the highly developed American law of privacy has used as an authoritative basis for its doctrines the English decision of *Gee* v. *Pritchard*[212] where an injunction was granted to prevent disclosure of confidential and private material in letters written to the defendant by the plaintiff. The defendant had made copies of the letters before returning them and the court held that an injunction lay to protect the defendant's *property* right in the letters.

[211a] An action may also lie for negligent misstatement: *Hedley Byrne* v. *Heller*, [1964] A.C. 465 (H.L.).

[212] (1818), 2 Swan 402.

In the case of personal information storage systems[213] the relationship between the common law's concern to protect property and reputational interests and the Canadian provincial law reformers' desire to regulate their use is striking. The primary rationale for the regulation of data storage systems is simply that existing property and expectation interests would otherwise be placed in jeopardy.

A matter of note is that credit and personal data reporting has been the subject of examination by the Commissioners on Uniformity of Legislation in Canada. At their 1971 conference it was resolved that "the Ontario and Quebec Commissioners undertake a survey of the protection of privacy in the area of credit and personal data reporting and . . . report at the next meeting of the Conference with a draft uniform Act".[214] Ontario's draft Act[215] was very similar to that which was recently legislated by that province.[216] Quebec's draft Act,[217] although not the same as Ontario's, was similar in aim and intent. The matter was referred to the Conference the following year. In 1973, Quebec and Ontario again submitted draft Acts,[218] but Ontario suggested that the subject be taken off the agenda until more jurisdictions had legislation of common intent on the subject,[219] and the matter was referred to the 1974 Conference. Despite this lack of agreement the Commissioners have probably had a certain amount of influence on present legislation because three provinces, Ontario, Nova Scotia and British Columbia, have almost identical legislation, and that of Saskatchewan is broadly similar. However, the Manitoba and Newfoundland Acts are distinct from the other four and from each other, whereas Quebec's attempt through four sections of the Consumer Protection Act[220] is sparse and superficial.

Manitoba was the first province to enact legislation governing personal information systems.[221] The Manitoba Personal Investiga-

---

213 Especially computerized systems whereby all privacy concerns are compounded.

214 [1971] Proc. Conf. Comm. Uniformity Legis. 83.

215 The Consumer Reporting Act, [1972] Proc. Conf. Comm. Uniformity Legis. 180.

216 Consumer Reporting Act, S.O., 1973, c. 97.

217 Protection of Privacy (Credit and Personal Data Reporting), [1972] Proc. Conf. Comm. Uniformity Legis. 196.

218 Personal Information Reporting Act (Ontario), [1973] Proc. Conf. Comm. Uniformity Legis. 360. Agences d'information (Québec), p. 372.

219 [1973] Proc. Conf. Comm. Uniformity Legis. 359.

220 S.Q., 1971, c. 74.

221 Personal Investigations Act, S.M., 1971, c. 23.

tions Act does not require licencing of those who conduct investigations but section 3(1) states that no person shall conduct a personal investigation (described generally as any inquiry by any person to obtain factual or investigative information from any source other than the subject dealing with credit, insurance, employment or tenancy) without the express written consent of the subject of the investigation or unless the subject is given written notice by the user of the information that a personal investigation has been conducted. Such notice is given within ten days of the granting or denial of the benefit for which the subject has applied. Section 2 exempts the Act's application to provincial or municipal governments (except in applications by a subject for employment, credit, insurance or tenancy), police officers in their official capacities, reports on corporation containing only factual information about officers or employees and certain investigations (a) by an employee on a subject where potential salary is greater than $12,000.00 per annum, (b) where the subject is invited to participate in ownership of a private company and (c) where the subject applies for life insurance in excess of $25,000.00 and the beneficiary of such insurance is the subject's employer.

Section 4 excludes certain information from any report such as reference to race, religion, bankruptcy of the subject fourteen years or more before the report, statute barred debts or writs, writs issued more than twelve months before the report where the status of the action is unknown, information about judgments unless the name and address of the judgment creditor is included, any adverse factual or investigative information more than seven years old and any investigative information regarding the subject unless reasonable efforts[222] have been made to corroborate it.

Section 5 specifies who may have access to personal reports on subjects and that a subject must be advised in writing by any user of such a report that he has been denied a benefit as a result of the user's use of the personal report. If a subject is denied a benefit as a result of the use of a personal report he may, within thirty days, apply to the user to ascertain the name and address of the reporting agency and the user must inform the subject of his right to protest such information. The reporting agency must supply to the subject, within twenty-four hours of application, the source of all information, the nature of any investigative information and inform the subject of his right to protest.

---

[222] This leaves the question: what are reasonable efforts? The corroborator may be someone who has heard the same gossip.

Section 8 provides that any person may inquire of any reporting agency whether they hold a file on him and, if such a file is kept, the information contained there must be disclosed to him. The subject of any report may protest any information in a personal file and a method is set out whereby the reporting agency or user must attempt to verify such information. Provision is also made to cover the case where the reporting agency is outside Manitoba and the user within. The user must attempt the verification in this situation. This is an important provision as the situation might often arise where the reporting agency is located outside the province. Under section 6 a user and reporting agency cannot agree not to disclose information to a subject. Any such agreement is deemed void.

Finally, pursuant to sections 16 and 19, the Act makes it an offence for a user or reporting agency to fail to comply with the provisions but both are exempt from civil liability unless they knew or ought to have known that any of the information was false, misleading or negligently obtained.

Four pieces of provincial legislation, that of British Columbia,[223] Ontario,[224] Nova Scotia,[225] and Saskatchewan,[226] are very similar and may be conveniently discussed together.[227] In doing so, it must be borne in mind that the Saskatchewan legislation is considerably narrower in scope than the others because it applies only to credit reporting agencies. These are defined as anyone engaged in the *business* of furnishing information to subscribers regarding the financial rating of persons.[228] On the other hand, in British Columbia and Nova Scotia[229] the Acts cover persons who, for gain or profit, furnish consumer reports. Unless the term "gain" in this context is granted a wide construction, these enactments, too, will be subject to severe limitation. In Manitoba, a credit reporting agent does not have to provide credit reports for remuneration as long as he is "engaged" in so doing,[230] and in Ontario, a credit reporting agent is a person who for gain or profit or on a regular co-operative non-profit basis, furnishes consumer

---

223 Personal Information Reporting Act, S.B.C., 1973, c. 139.

224 Consumer Reporting Act, *supra*, footnote 216.

225 Consumer Reporting Act, S.N.S., 1973, c. 4.

226 Credit Reporting Agencies Act, S.S., 1972, c. 23.

227 Newfoundland has also enacted a Collection Agencies Act, S.N., 1973, c. 14, that came into effect on 1st April, 1974.

228 *Supra*, footnote 226, s. 2 (c).

229 B.C., *supra*, footnote 223, s. 1; N.S., *supra*, footnote 225, s. 2(1).

230 *Supra*, footnote 221, s. 2(e).

reports.[231] The Manitoba concept of a credit reporting agency being a person engaged in providing credit reports for remuneration *or otherwise* is apparently the most elastic and encompassing.

All four Acts require reporting agencies to be licensed or registered under the respective legislation, and Ontario requires registration of all personal information reporters. Saskatchewan goes so far as to require credit reporting agencies to be bonded. All enactments have extensive provisions regarding the terms of the licences as well as those setting out procedures for appeal from a denial or cancellation of such licences.

The Acts generally restrict those to whom agencies may divulge information. These include (1) a person who (a) uses the information for extending credit or collecting a debt, (b) uses the information for a tenancy agreement, (c) uses the information for employment purposes (d) uses the information for underwriting insurance (e) uses the information for a direct business transaction with a consumer, or (2) a person who uses the information in accordance with instructions from the consumer or (3) in response to an order from a court. Saskatchewan, however, limits the class to whom information may be given to those granting credit.[232]

All four Acts also provide that the reporting agency shall adopt all procedures reasonable for ensuring accuracy and fairness in reports as well as quite detailed lists of what must not be included in the reports.[233]

With the exception of the Saskatchewan Act, no person may obtain a consumer report without the express consent of the consumer or unless the user of the report gives notice to the consumer that a report will be obtained. The Saskatchewan provisions are not as strong because they merely require disclosure of reports upon the request of the consumer. Similarly, under all the Acts except that of Saskatchewan, where the user of information denies the subject a benefit, notice must be given to the consumer. Under the British Columbia and Nova Scotia Acts, the user must state that a benefit has been denied, that the consumer has a right to disclosure, give the name and address of the

---

[231] *Supra*, footnote 216, s. 1(1) (c).

[232] *Supra*, footnote 226, s. 17.

[233] B.C., *supra*, footnote 223, s. 11; Sask., *supra*, footnote 226, s. 18; Ont., *supra*, footnote 216, s. 9; N.S., *supra*, footnote 225, s. 10. The Saskatchewan provisions are considerably narrower than those of the other three provinces.

reporting agency and the source and nature of information obtained elsewhere than a reporting agency. Furthermore, under these two Acts the denial of a benefit need not be the result of the use of such information. Under the Ontario Act, the denial must be because of use of information and the notice need only contain the name and address of the source and the consumer's right to examine the report. The Saskatchewan Act has no such provision.

All four enactments require disclosure to a consumer, on request, of the nature and substance of information on file respecting the consumer, and all but Saskatchewan require that the sources of such information be disclosed. The fact that Saskatchewan does not require disclosure of sources may well be an important provision because, as Dr. Morison stresses,[234] this itself opens the door to invasion of the privacy of information sources.

It is of interest that the Nova Scotia[235] enactment provides for the settlement of disputed information where the reporting agency is located outside the province. This may well prove to be an area where the other statutes will require amendment, since inter-provincial personal investigation is hardly uncommon.

The most important provisions of these Acts relate to the correction of errors[236] and the creation of a supervisory director or registrar to control their administration. The consumer, when examining his report, is permitted to be accompanied by one other person and the reporting agencies must provide trained staff to properly explain the information in the reports. The consumer may file a statement of protest regarding any information contained in the report and the reporting agency is left with the onus of confirming, completing or correcting information and if correction is necessary, the reporting agency must notify all those who have received the reports. There are also provisions for the registrar under the Acts to make investigations pursuant to complaints. Finally, the Acts make it an offence for anyone to fail to comply with their provisions.

Mention should now be made of the Newfoundland Credit Reporting Agencies Act.[237] The purpose of this legislation is

---

[234] Morison, *op. cit.*, footnote 7, p. 49.

[235] Manitoba also has such a provision, *supra*, footnote 221.

[236] B.C., *supra*, footnote 223, s. 16; Sask., *supra*, footnote 226, s. 25; Man., *supra*, footnote 221, ss 10 and 11; Ont., *supra*, footnote 216, s. 12; N.S., *supra*, footnote 225, s. 13.

[237] Collection Agencies Act, *supra*, footnote 227.

certainly the same as the other Acts which have been discussed but it is directed at regulating the agencies rather than granting rights to the consumer. It requires licensing of credit reporting agencies, and regulates the type of information which may be reported. If the credit risk of a person is being assessed, the consumer must be informed of the investigation together with the name of the credit reporting agency supplying the report—if the consumer asks for such information.[238] Any person may find out if a report has been made on him without cost.[239] The registrar is responsible for enforcing the provisions of the Act although restraining orders may be granted by a judge of the Supreme Court where persons are in breach of the Act or any order made under the Act.

The final statutory provision dealing with personal information is the Quebec Consumer Protection Act.[240] Because of their brevity, these sections are reproduced and self-explanatory:

> DIVISION IV
>
> Information Agents
>
> 43. For the purposes of this division, any person carrying on the business of preparing and distributing to others credit reports respecting the character, reputation or solvency of a person is an information agent.
>
> 44. All information gathered and credit reports prepared by an information agent respecting a person shall be the credit record of such person.
>
> 45. Any person may examine his credit record during business hours and make his comments in writting, which shall be recorded in such record.
>
> 46. However, an information agent is not bound to disclose the source of his information, if it does not appear in the credit record.

It can be seen that these provisions are the most sparse of those set up by legislation and can hardly be regarded as providing more than a modicum of protection.

Only the passage of time will reveal whether or not these statutes concerning the reporting and distribution of personal information are really effective. The need for regulation and protection of privacy interests thereafter threatened by data banks will no doubt increase with the evolution of more sophisticated computers and other modes of compilation and recall. These statutes are essentially concerned with a property interest (credit, renting and insurance) and to that extent are consistent with the traditional thrust of the common law.

---

[238] *Ibid.*, s. 21.

[239] *Ibid.*, s. 22.

[240] *Supra*, footnote 220.

But a more general threat to privacy exists at the level of the public institutional use of mechanical dossiers, particularly within the framework of criminal law enforcement. Pieces of information garnered by different parts of the state apparatus can be easily centralized and computerized for instant recall. Fragmented information may pose no threat to an individual's privacy but where those fragments are joined to reveal a profile, albeit vague, an individual may find his career activities circumscribed, his relationships with others jeopardized and his reputation ruined.

Computers are mere tools and cannot be said to be inherently good or bad. The concerns of those who fear unregulated computerization of personal information by government or otherwise are easily stated. There is always the possibility that the information may be misclassified or based on false information. The creation of a central storage facility instantly accessible to subscribers facilitates access to a wider group than formerly existed. Information released by a computer system tends to take on the quality of accuracy, whereas in fact it may be entirely misleading, inadequate or based on false data.

It cannot be too strongly argued that regulation of all systems of computers concerned with personal information is a vital step in the direction of privacy preservation. Apart from the tentative credit-oriented provincial legislation we have referred to, there is a pressing need to grant access to information contained in other data banks to those who appear in them. There must be the machinery to regulate such data banks and ensure that false information is changed and that abusive practices are stopped.

Toffler[241] perceived the need for the creation of a technological ombudsman to "receive, investigate and act on complaints having to do with the irresponsible application of technology". Surely this need is most pressing in relation to computerized data surveillance, which, after all, is merely a visible facet of the technological explosion.

The statutory schemes we have referred to are, in large measure, a reflection of the concern with which society regards the existence and use of uncontrolled personal information systems. This concern will not be satisfactorily met until all such systems, including law enforcement units, are subject to appropriate regulatory procedures.

---

[241] Future Shock (1970), pp. 390-392.

IV. *The Criminalization of Electronic Surveillance.*[242]

Electronic eavesdropping as a mode of obtaining evidence of criminal activity[243] had been the subject of judicial scrutiny for some years prior to the enactment of the federal Protection of Privacy Act 1973.[244] It had been held by the Ontario Court of Appeal[245] that since the police were under a statutory duty[246] to make proper enquiries and take preventive measures against crime, the use of a wiretap was not an offence against the province's Telephone Act.[247] The Supreme Court of Canada subsequently decided that wiretaps were admissible in evidence as having probative value,[248] and in the Ontario Court of Appeal's view this was the case whatever methods were used to install the "bug".[249] In *R.* v. *Montani,*[250] Mark Prov. J. was able to conclude:[251]

> [P]rior to any legislation being passed banning police wiretapping ... the police have the right to wiretap and that evidence obtained from [it] is admissible....

Between 1964 and 1970 there had been many attempts to introduce legislation controlling wiretapping in Canada. With the exception of three, all of these bills have been introduced by private members and all but one have been unsuccessful.[252] As well as the private members' bills the Minister of Justice has

---

[242] This part is a summary of an article entitled Electronic Eavesdropping and Federal Response: "Cloning a Hybrid" (1975), 10 U.B.C. L. Rev. 36.

[243] Of course it is a method not confined to criminal proceedings but the more critical cases occur in this context.

[244] *Supra,* footnote 2.

[245] *Kennedy* v. *Tomlinson* (1959), 20 D.L.R. (2d) 273.

[246] They were already under such a common law duty.

[247] *Supra,* footnote 140.

[248] *Silvestro* v. *The Queen,* [1965] S.C.R. 155.

[249] *R.* v. *Steinberg,* [1967] 1 O.R. 733 (Ont. C.A.).

[250] (1974), 26 C.R.N.S. 339 (Ont. Prov. Ct).

[251] *Ibid.,* at pp. 341-342. This case decided that voice print (spectographs) analysis was admissible in a preliminary hearing. In *R.* v. *Demeter* (1975), 19 C.C.C. (2d) 321 (Ont. H. C.), Grant J. took the view that electronic surveillance that would be "unlawful" under the Protection of Privacy Act was not unlawful for the purposes of admissibility of evidence so obtained where it took place prior to the enactment of that legislation, even though the trial occurred after the Protection of Privacy Act came into effect. The same result was arrived at in *R.* v. *Lesarge* (1975), 17 Crim. L.Q. 118 (Ont. Co. Ct).

[252] These bills include 1964, C-103; 1966, C-45; 1967, C-18, C-19; 1968, C-17, C-18, C-24, C-78; 1969, C-116; 1970, C-96; 1972, C-83 and 1973, C-120.

introduced three bills to make wiretapping illegal by amendments to the Criminal Code.[253] For the most part these three bills are very similar. The last of these, Bill C-176, was adopted by the House of Commons on December 4th, 1973 and became law on June 30th, 1974.

Bill C-176, otherwise known as the Protection of Privacy Act,[254] was enacted by amending the Criminal Code[255] for the express purpose of creating offences relating to the interception of private communications, the disclosure of private communications and the possession of any device primarily useful for the surreptitious interception of private communications and to establish rules governing the admissibility of evidence thereby obtained. The bill also provides, by amendments to the Crown Liability Act,[256] for civil liability of the Crown in circumstances where a private communication is unlawfully intercepted or disclosed by a servant of the Crown. By amendments to the Official Secrets Act,[257] it makes provision for the interception or seizure of private communications where the interception or seizure is directed towards the prevention or detection of any subversive activity (that is espionage, sabotage) directed against Canada or detrimental to the security of Canada and where the interception or seizure is necessary in the public interest.

1. *The Provisions of the Protection of Privacy Act 1973.*[258]

Under section 178.11 everyone who *wilfully* "intercepts"[259] a "private communication"[260] by "electromagnetic, mechanical or other device"[261] is guilty of an indictable offence and liable to imprisonment for five years. However, no offence is committed if the originator or receiver of the private communication expressly

---

[253] 1971, C-252; 1972, C-6; and 1973, C-176.

[254] *Supra*, footnote 2. See generally, Manning, The Protection of Privacy Act (1974).

[255] *Supra*, footnote 138.

[256] R.S.C., 1970, c. C-38.

[257] R.S.C., 1970, c. O-3.

[258] All section references are to the Criminal Code, unless otherwise indicated.

[259] Defined in s. 178.1 as "listening to recording or acquiring a communication or acquiring the substance, meaning or purport thereof".

[260] Defined in s. 178.1 to mean any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.

[261] Defined under s. 178.1 as meaning any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.

or impliedly consents to the interception[262] or if the person intercepting the communication has an authorization to intercept.[263] If there is more than one originator or receiver of the private communication (that is at least three parties), the consent of one of them is sufficient to validate the interception. This clarifies the case of a police agent being able to consent to electronic surveillance in such circumstances and legitimately intercept or arrange for the interception of what would otherwise be private conversations.

Section 178.12 provides the guidelines for an application for authorization to intercept a private communication in investigating the commission of an offence. It states that an application shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 482 of the Criminal Code and shall be signed by the Attorney General of the province in which the application is made or the Solicitor General of Canada *or* an agent specially designated in writing for the purposes of this section by the Attorney General for the province or the Solictor General of Canada, depending on who may institute proceedings. Such written designation must be made personally by the provincial Attorney General or federal Solicitor General. The application must be accompanied by an affidavit, which may be sworn on the information of a peace officer, deposing to (a) the facts relied upon to justify the belief that an authorization should be given together with particulars of the offence, (b) the type of private communication proposed to be intercepted, (c) the names and addresses, if known, of persons whose communications, if intercepted, would assist the investigation of the offence, (d) the period for which the authorization is required, and (e) whether or not other investigative procedures have been tried and failed, and so on.

The secrecy of the material referred to in sections 178.12 and 178.13(3) is maintained by filing it in a sealed packet in the manner outlined in section 178.14. In such a case the sealed packet cannot be opened for review by way of *certiorari*. Such review is confined to the trial judge and subsequent appeal from his determinations and then only if there is extrinsic evidence of "fraud".[263a]

---

[262] S. 178.11 (2) (a).

[263] S. 178.11 (2) (b).

[263a] *In re Miller and Thomas* (1975), 23 C.C.C. (2d) 257; *cf. Re Stewart and the Queen* (1975), 23 C.C.C. (2d) 180 (Ont. Co. Ct) where it was held that *pre-trial* review was available.

A limiting factor on obtaining authorization is contained in the term "offence" as used throughout the Protection of Privacy Act. It is defined in section 178.1 in such a way as to limit its meaning to an indictable offence with a possible term of imprisonment of ten years or more, or an indictable offence linked with "organized crime".[264] The term "offence", as defined in the first reading of Bill C-176, on April 13th, 1973, meant *any* indictable offence.[265] Whatever one's view of the Act is, it is undoubtedly better for having been passed at a time when a minority government was in power. The alteration of the definition of "offence" was one of the concessions the Liberal government had to make to maintain a parliamentary majority.

But the Protection of Privacy Act is no help in defining what organized crime is. Is it merely two or more people conspiring to commit a number of indictable offences, or has it a more precise meaning? The term "organized crime", is certainly not a term of art judicially defined and it changes its meaning as its context shifts.[266] Probably the meaning that our courts will attribute to it is that which is popularly granted to it, in the United States:[267]

> Organized crime, is used as a synonym for syndicated crime, cartel crime, or confederated crime, not for the many varieties of criminal organization.

Section 178.13 spells out the grounds on which a judge must be satisfied before allowing an authorization to intercept a private communication.[268] It also states that an authorization shall include

---

[264] This vagueness has been criticized by law enforcement agencies. See the first Report of the Solicitor General to Parliament, dated February 10th, 1975, p. 5. The actual wording is: "indictable offence in respect of which there are reasonable and probable grounds to believe that it forms a pattern of similar or related offences, by two or more persons acting in concert, *and* that such pattern is part of the activities of organized crime."

[265] It would therefore have included such offences as theft under $200.00.

[266] For an excellent account of the different meanings attributable to this open-textured term see Cressy, Criminal Organization: Its Elementary Forms (1972), pp. 1-17.

[267] Cressy, Organized Crime and Criminal Organizations (1971), Churchill College Overseas Fellowship Lecture, No. 7, p. 10.

[268] These include satisfaction that other investigative procedures have been tried and have failed; that alternative modes of investigation *are* unlikely to succeed; *and* that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using *only* other investigative procedures. The use of the conjunctive "and" was contained in the third reading of Bill C-176, which was duly enacted. At second reading it was the disjunctive "or". It appears in the final copy

(a) a description of the offence in respect of which private communications may be intercepted (b) the type of communication that may be intercepted (c) the identity, if known, of persons whose communications may be intercepted (d) such terms as the judge considers advisable in the public interest and (e) a statement that the authorization is not valid for a period exceeding thirty days. Finally the section allows the Attorney General[269] or the Solictor General of Canada to designate which persons may intercept communications under the authorization and the method and grounds for renewal of the authorization for a further period of up to thirty days. A unique feature of section 178.13(4) dealing with renewals is that any of the circumstances in subsections (1)(a), (b) or (c) or both will suffice. Whereas if the applicant is relying on those in subsection (1)(a) and (b) in the original application he must have both! Section 178.14 describes the manner in which applications for authorization to intercept personal communications will be kept confidential, in the custody of the court.

Section 178.15 also represents an area of substantial improvement between the first and third readings of this Act. It deals with emergency authorizations and in its original form gave the Attorney General for the provinces or the Canadian Solicitor General *or* an agent authority to authorize interception of communications for thirty-six hours in cases where the urgency of the situation required interception to commence before an authorization could be obtained with reasonable diligence. This proposal was opposed by the opposition and the Rt Hon. John Diefenbaker moved to delete it in total.[270] This motion was amended by

---

of the statute published as "or". Technically, the third reading copy as assented to by Parliament is correct but, it certainly seems inconsistent with the urgency provisions rationale to require officers to attempt other investigative techniques in advance of applying for authorization.

[269]S. 178.13 (2.1) is really unclear as to which Attorney General is being referred to. Since in other provisions the term Attorney General is qualified by the phrase "of the Province" *etc.*, it may be assumed to refer to the federal Attorney General which, grammatically, also flows from a literal reading of the section. But this seems inconsistent with the foregoing procedures whereby a *provincial* Attorney General is the authorizing agency with the federal Solicitor General. It would follow logically that such *provincial* Attorney Generals should have the power to designate who may make interceptions. The latter construction is likely to be the one placed on the provision by the courts, especially as it is consistent with the general definition of Attorney General contained in s. 2 of the Criminal Code.

[270] House of Commons Debates (unrevised, Nov. 23rd, 1973), p. 8088.

a government member[271] and the resulting compromise is the present provision. The section now states that an application for an authorization may be made *ex parte* to a judge of a superior court of criminal jurisdiction or as defined in section 482, designated from time to time by the Chief Justice (of the provincial Supreme Court), by a peace officer specially designated by the provincial Attorney General or Canadian Solicitor General if the urgency of the situation requires interception of private communications to commence before an authorization could reasonably be obtained. The judge, if satisfied that the urgency of the situation so requires, may issue an authorization for thirty-six hours. For evidentiary purposes, an interception made under this section is deemed not to be lawful unless the judge certifies that he would have granted an authorization if application had been made under section 178.12 in the ordinary way. An open question arising out of the provision is whether or not section 178.15(2) creates the possibility of a wiretap being started without authorization and subsequent authorization being applied retroactively by the judge to validate it.

Law enforcement agencies have been critical of the emergency provisions and their concern has been reflected in the first *Report of the Solicitor General of Canada* to Parliament.[272] In it the Hon. Warren Allmand stated:[273]

> The emergency authorization legislation — Sec. 178.15 is having an adverse effect on both ordinary and organized crime investigation. The reason is that the emergency provision is not proving to be a remedy for emergency applications. The time required to obtain an emergency authorization is virtually the same as that under a normal application. Of a total of 141 authorizations only three were received under s. 178.15. To be truly effective emergency conditions require an instantaneous response from the courts.

The second crime created by this Act is contained in section 178.18. It is an indictable offence to possess, sell or purchase any electromagnetic, acoustic, mechanical or other device knowing that the design thereof renders it primarily useful for surreptitious interception of private communications. An offender is liable on conviction to two years imprisonment. Certain persons in possession of such equipment are exempted from this section including a police officer in possession in the course of his

---

[271] *Ibid.* (Nov. 28th, 1973), p. 8245.

[272] Dated February 10th, 1975. For a police view of the Act see Craig, Electronic Surveillance: Setting the Limits (1975), 24 Univ. of N.B. L. J. 29.

[273] *Ibid.*, at p. 6.

employment, a person in possession to make an interception in accordance with an authorization, and a person in possession under the authority of a licence issued by the Solicitor General of Canada. A licence issued to the last named person may contain such terms and conditions as the Solicitor General may prescribe. Any person convicted of possession under section 178.18 may forfeit any device the possession, selling or purchasing for which he was convicted, pursuant to section 178.19.

Another crime created by this Act, under section 178.20, makes it an offence to use, disclose the contents of, or disclose the existence of any private communication without the express or implied consent of the originator or the receiver. This is an indictable offence and a conviction may result in a two year prison term. This provision does not apply to persons giving evidence in criminal or civil proceedings if the communication is admissible under section 178.16, to disclosure in the course of a criminal investigation if the communication was lawfully intercepted, or where disclosure is made to a peace officer and is intended to be in the interests of the administration of justice.

The Solicitor General of Canada is required as soon as possible after the end of the year[274] to prepare a report relating to authorizations and interceptions and lists details that must be included in the report which must be presented to Parliament. The section also requires that provincial Attorney Generals prepare and publish a similar report which is to be made available to the public.

One provision, section 178.23, very nearly aborted the Protection of Privacy Act due to government and Senate opposition. When the bill was read for the first time this section was non-existent. It provides that the Attorney General of the province in which an application for authorization was made or the Canadian Solicitor General, shall notify in writing, within ninety days following the period for which the authorization was given, the person who was the subject of the interception. Following this, the court which issued the authorization must be informed of the notification. It does not apply to a warrant issued under the Official Secrets Act[275] or where the provincial Attorney

---

[274] Year means "calendar year": s. 28 of the Interpretation Act, R.S.C., 1970, c. I-23. The first report was presented to Parliament by the Hon. Warren Allmand, the Solicitor General of Canada, dated February 10th, 1975.

[275] *Supra*, footnote 257.

General or Solicitor General of Canada certifies, within ninety days, to the judge who issued the authorization, that the investigation is continuing and the judge is of the opinion that the interests of justice require that a delay of determinate reasonable length be granted and the judge grants such a delay.

There has been continued pressure from law enforcement agencies to have this provision repealed. But it is difficult to perceive how section 178.21 of the Criminal Code, granting jurisdiction to a court to award punitive damages when convicting an accused for unlawful interception and so on, could be in any measure effective without such a notice provision. If it were otherwise a paradigm "Catch 22" would result: a law enforcement agency may illegally intercept private communications but the victim-object will be unaware that he is even being observed since by its very nature such observation will be covert. Only when the victim-object is appraised of the surveillance can he proceed to assess its legality. Further, only where this is capable of being done can the criminal process be initiated, in the event of illegality, and the punitive damages can only be granted within the framework of such criminal process.

The Solicitor General, in his first *Report* to Parliament noted that law enforcement agencies were of the view that this provision has diminished their effectiveness in dealing with organized crime.[276]

After the second reading of the bill on May 8th, 1973, it was referred to the Standing Committee on Justice and Legal Affairs. As an aside, it is noteworthy that the present Act owes a great deal to that committee for its present state[277] and work done on previous wiretap bills.[278] Indeed, section 178.23 was created by that committee which added the provision by a majority vote.[279] The Minister of Justice opposed its addition and when the House of Commons resumed consideration of the bill as reported with amendments from the Standing Committee, the Minister introduced a motion to amend which would have deleted this section.[280]

---

[276] Dated February 10th, 1975, p. 5.

[277] House of Commons Standing Committee on Justice and Legal Affairs, Proceedings (1973), Nos 13-17, pp. 21-24, 26-29.

[278] *Ibid.* (1972), Nos 8-11; (1970), No. 7; and (1969), Nos 29-30.

[279] *Ibid.* (November 8th, 1973), No. 28, pp. 3-23.

[280] House of Commons Debates (unrevised, November 29th, 1973), p. 8269.

This motion was defeated by a narrow margin with the government members voting in favour.[281] On the same day, December 4th, 1973, the bill was read the third time and passed.[282] However, this was not to be the end of its stormy passage. On the 5th and 11th of December, 1973, the bill was given first[283] and second[284] readings, respectively, in the Senate and referred to that house's Standing Committee on Legal and Constitutional Affairs. The committee interviewed two witnesses, Chief Adamson of the Toronto Police and the Minister of Justice. It must therefore have been no surprise when the committee reported back to the Senate on the 13th of that month and recommended that section 178.23 be deleted. This recommendation was adopted as an amendment and the bill received third reading the same day.[285]

On the 10th of January, 1974, the Minister of Justice introduced a motion that the House of Commons did not concur in the Senate's amendment and in place of the former provision moved that the bill be amended to provide for a "report of progress to a judge within 90 days" instead of *notice* to the person who was the object of the interception.[286] However, it was further moved that this motion should only read that the House of Commons did not concur in the Senate amendment and that this message be sent to the Senate.[287] This motion passed with the government members opposed. On the 14th of January, 1974, the Speaker of the House of Commons announced that the Senate did not insist on its amendment and the bill was given Royal Assent.[288]

---

[281] House of Commons Debates (unrevised, December 4th, 1973), p. 8399.

[282] *Ibid.*, p. 8419.

[283] Senate Debates (unrevised, Dec. 5th, 1973), p. 1245.

[284] *Ibid.* (Dec. 11th, 1973), p. 1329.

[285] *Ibid.* (Dec. 13th, 1973), pp. 1361-1362.

[286] House of Commons Debates (unrevised, Jan. 10th, 1974), p. 9232.

[287] *Ibid.*, p. 9238. This motion was made by Mr. Leggatt, M.P., (New Westminster) and, pp. 9236-38, he made a short review of the Bill's history saying the House of Commons had considered wiretapping for four years with fifteen debating days while the Senate had debated about three hours. Also two House of Commons Standing Committees on Justice and Legal Affairs had interviewed thirty-two witnesses including R.C.M.P. Deputy Commissioners, Canadian Civil Liberties Assoc. representatives, and Ramsey Clarke, former United States Attorney General, while the Senate Committee had interviewed only two witnesses.

[288] House of Commons Debates (unrevised, Jan. 14th, 1974), p. 9303.

One provision of the Protection of Privacy Act which will likely be the subject of protracted litigation in the future is section 178.21.[289] Subsection (1) provides that a court that convicts an accused under section 178.11 or section 178.2 may, upon the application of a person aggrieved, at the time "sentence" is imposed, order the accused to pay to that person an amount not exceeding $5,000.00 as punitive damages. Subsection (3) states that where an amount ordered to be paid under subsection (1) is not paid forthwith, the applicant may, by filing the order, enter as a judgment in the superior court of the province in which the trial was held, the amount ordered to be paid. That judgment is enforceable against the accused in the same manner as if it were a judgment rendered against the accused in that court in civil proceedings. It should also be noted that the definition of "sentence" in section 601 of the Criminal Code is amended by including an order made under section 178.21.

Section 178.16 deals with the admissibility of intercepted communications as evidence and evidence derived from an interception.[290] When the bill was passed on first reading, subsection (1) stated that a private communication that had been intercepted was inadmissible as evidence against the originator unless (a) the interception was lawfully made or (b) the originator or receiver of the private communication consented to the admission; but evidence obtained directly or indirectly as a result of information acquired by interception of a private communication was not inadmissible by reason only that the private communication was itself inadmissible as evidence. However, the Standing Committee on Justice and Legal Affairs amended this subsection[291] to its present form. It now declares that a private communication that has been intercepted and evidence obtained of a communication are both inadmissible as evidence against the originator thereof or the receiver unless the interception was lawfully made or the originator or receiver consents to the admission.

---

[289] This provision raises questions as to its constitutionality and role within the context of the doctrine of *res judicata*. See my article, *op. cit.*, footnote 242, at pp. 52-63.

[290] For a full discussion of this provision see my article, *op. cit.*, *ibid.*, at pp. 46-52. See also Owen, When is an Interception Lawfully Made?, [1975] March Crown's Newsletter 1, who discusses the "spin-off" effects of a wiretap in relation to *R. v. Palneau* (1975), where evidence of rape by the accused was held admissible whereas it was derived from a wiretap authorized on the basis of a suspected "breaking and entry" and conspiracy to break and enter.

[291] House of Commons Standing Committee on Justice and Legal Affairs, Proceedings (Sept. 18th, 1973), No. 26, pp. 24-51.

Had this subsection stood alone the section would have been a welcome change from the common law. However, before the third reading, the Minister of Justice introduced subsection (2)[292] and after two amendments and considerable debate[293] that subsection was passed and became part of the Act. Section 178.16(2) states that in any proceedings where the judge is of the opinion that any private communication or any other evidence that is inadmissible pursuant to subsection (1) is (a) relevant *and* (b) inadmissible by reason only of a defect of form or an irregularity in procedure, not being a substantive defect or irregularity, in the application for or the giving of the authorization under which such private communication was intercepted or by means of which such evidence was obtained *or* (c) that, in the case of evidence, other than the private communication itself, to exclude it as evidence may result in justice not being done, he *may,* notwithstanding subsection (1) admit such private communication or evidence as evidence in such proceedings.

This provision, section 178.16(2), hedges what would otherwise have been a substantial shift in legal policy towards the American "poisoned fruit" doctrine.

The latter part of the Protection of Privacy Act encompasses necessary changes to the Crown Liability Act[294] and the Official Secrets Act.[295] A new section 7 is added to the Crown Liability Act whereby the Crown is liable for all loss or damage caused by or attributable to an intentional interception of a private communication by a servant of the Crown acting in the course of his employment. The Crown would also be liable for punitive damages not exceeding $5,000.00 to each person suffering a loss.[296] The section does not apply if the interception was lawful or made with the consent of the receiver or originator.[297] Again, the Crown is liable for the same damages as above where a servant of the Crown discloses any part of a communication which has been intercepted.[298] The amendment also provides that no award of punitive damages will be made under section 7

---

[292] House of Commons Debates (unrevised, Nov. 27th, 1973), p. 8203.

[293] *Ibid.* (Nov. 27th, 1973), pp. 8203-8212 and (Nov. 28th, 1973), pp. 8229-8242.

[294] *Supra,* footnote 256.

[295] *Supra,* footnote 257.

[296] *Supra,* footnote 256, s. 7.2(1).

[297] *Ibid.,* s. 7.2(2). Random monitoring pursuant to radio spectrum management, too, will not mean liability.

[298] *Ibid.,* s. 7.3(1). There are a number of exceptions: s. 7.3(2) (1).

of the Crown Liability Act where an order has been made under section 178.21 of the Criminal Code for punitive damages.[299]

The amendments to the Official Secrets Act provide that all the amendments to the Criminal Code and Crown Liability Act in the Protection of Privacy Act do not apply to any person who makes an interception pursuant to a warrant and the Solicitor General may issue a warrant authorizing an interception if he is satisfied that the interception is necessary for the prevention or detection of subversive activity (defined) directed against Canada.[300] The contents of a warrant must include the type of communication to be intercepted or seized, the person or persons who are authorized to do so, and the length of time the warrant is to remain in force.[301] Finally, the Solicitor General must make an annual report detailing all warrants issued.[302]

The data available at this time, contained in the federal Solicitor General's *Report*, is insufficient to permit generalization concerning the effect of the Protection of Privacy Act on either law enforcement or civil liberties. The *Report* only deals with those interceptions relating to offences that may be commenced by the federal authority. The bulk of these were drug conspiracies[303] and although the number of arrests and charges are revealed, it is not clear what the conviction results were nor how often it was necessary to adduce wiretap evidence at trial. The same need for clarification is evident in the British Columbia Attorney General's *Report*[304] which contained certain data on the number of charges laid but none on the conviction ratio or the number of times evidence from an interception was adduced in court.

This legislation is undoubtedly of the highest social value to Canadians. It recognizes the role of privacy in our society and sets out to protect it from invasion in specific ways. It regulates the state's use of electronic eavesdropping devices and covert seizure of private communications during a criminal investigation. It is also the only comprehensive penal statute in the Com-

---

[299] *Ibid.*, s. 7.4.

[300] Official Secrets Act, *supra,* footnote 257, s. 16(1) and (2).

[301] *Ibid.*, s. 16(4).

[302] *Ibid.*, s. 16(5).

[303] See the Solicitor General's Report to Parliament, *op. cit.*, footnote 264, p. 3.

[304] The Vancouver Province, dated March, 1975, p. 10.

monwealth dealing with privacy invasion, albeit of a specific character.[305]

V. *Future Directions.*

In his macabre novel; *1984*,[306] George Orwell was asserting that human dignity is ultimately lost where a political state achieves a condition of omniscience and omnipotence. There the leading character, Winstone Smith, became conscious of the telescreen with its never-sleeping ear, but felt that so long as he retained a core-zone of privacy he could still function as a free human being:

> They [the Thought Police] could spy on one day and night, but if you kept your head you could still outwit them. With all their cleverness they had never mastered the secret of finding out what another human being was thinking.

This view was echoed by his friend, Julia, "they can't get inside you".

Of course, Winstone and Julia were quite wrong. They had reckoned without the tenacity and technology of the modern state and the sense of dedication that its functionaries manifest. When captured and taken to the Ministry of Love, Winstone realized after his torture that the Thought Police had watched him like a beetle under a magnifying glass. There was no physical act, no word spoken aloud, that they had not noticed, *no train of thought that they had not been able to infer*. O'Brien, the party-functionary, technocrat and torturer, could be any behavioural scientist when he claimed "We . . . control life . . . we create human nature".[307]

In Winstones' case his "human nature" was altered to the extent that he betrayed Julia to the state. It was not the physical torture that caused it; instead it was threats directed at his primordial fear of rats. The state had penetrated his private space, had acquired key data and was now in a position to manipulate its victim. Knowledge is the key to power in human institutions and the capacity and will to invade core-zones of privacy turns that key. Indeed the turning of that key affects the behaviour of those who know of it as well as the objects.

---

[305] Fifteen American States have legislation and the federal government has enacted the Omnibus Crime Control and Safe Streets Act 1968, Public Law 90-351, 82 Stat. 197 (1968), Title III, Wiretapping and Electronic Surveillance.

[306] (1949, Penguin ed. 1954).

[307] *Ibid.*, p. 216.

The "chill-factor" in human relations is a widely recognized social phenomenon.[308] It has been described as:[309]

> By chilling effect [of surveillance] we refer to any diminution in or inhibition of the expression of legitimate political behaviour in response to governmental practices.

The same comment could be passed of any human institution, such as a corporation or university, vis-à-vis those who exercise power and the constituent members.

Whatever the ultimate goal, political power, commercial gain or prurient interest, the capacity to interfere with others' private spaces is available to each of us. The direction of the law must be to recognize this fact and move towards regulation. This can only be done if we clearly express those interests that ought to properly be protected and assign moral priorities to them. Once this is done, a variety of regulatory models are open to be adopted.

By combining the work of Prosser and Westin, we have a highly developed account of the values concerned and the way in which they can be expressed in terms of legally-protected interests.[310] How then are we to regulate prospective privacy invasion?[311]

The traditional legal response has been to rely on the common law which, as we have seen, is very often unsuited to deal with the rapidly changing techniques of modern technology. As well, discrete statutory enactments criminalizing certain classes of privacy invasion have been undertaken by the various legislatures. Apart from those contained in the Protection of Privacy Act 1973, they appear to have been randomly selected and in existence only by historical mischance.

---

[308] Askin, Surveillance: The Social Science Perspective (1972), 4 Rutgers L. Rev. 59.

[309] *Ibid.*, at p. 63.

[310] This is along the lines in which the German law has developed. Most German jurists regard it as an impossible task to exhaustively define a general right of the personality ("persönlichkeitsrechte") and concentrate on defining the interests it embraces, such as honour and reputation. The free development of the personality is a fundamental right under art. 2, No. 1 of the West German Constitution of 1949.

[311] It must be recognized that in different cultures different emphasis will lie: "There is a different sociological emphasis between France and the United States. In France electronic surveillance plays a minor role under *les droits de la personnalité* and the focus is on protection of the human body, and issues concerning contracts relating to it." Strömhelm, *op. cit.*, footnote 17, p. 12.

An alternative to the judicialization of invasions of privacy is to create a privacy ombudsperson or commissioner. To a certain extent this has already been done in those provinces that have regulated abusive practices relating to personal information systems. If a similar administrative tribunal were to be set up to control invasions of privacy (or even if the same tribunal's functions were expanded), it would provide a cheap and accessible alternative to a costly legal action. It could be granted the power to award remedies, such as damages and injunctions, in appropriate cases.[312] Appeal procedures could be built in whereby appeals are taken to the Supreme Court rather than another administrative tribunal if this is regarded as desirable.

But an even better solution would be to retain judicial examination of alleged invasions of privacy and give jurisdiction to the Small Claims Division of the Provincial Court.[313] The relatively informal procedure there should not deter prospective claimants and the award ceilings such courts have are probably nearer the sort of damages a claimant is likely to receive. Certainly the cost of bringing such an action would no longer be a real bar and it would soon become clear whether or not this factor is the primary deterrent to privacy actions, or, alternatively, whether there *is* a real need for a general privacy statute at all!

Apart from administrative and civil legal reinforcement of privacy values, we can also turn to the criminal law as a means of achieving the same objective. This was consciously done in the federal Protection of Privacy Act, which must be regarded as a paradigm for future penal legislation governing privacy interests.

Not all invasions of privacy should be brought under the criminal law. This system should only be used to support those values that are regarded as being generally held by the community and of primary importance. The hybrid created by the Protection of Privacy Act is quite unique under Anglo-Saxon derived legal systems.[314] By combining the features of criminal sanction and damages in the same trial proceedings, a summary mode of achieving two objectives—protecting certain privacy values and

---

[312] It is recognized that this could raise a constitutional issue: see Laskin, Provincial Administrative Tribunals and Judicial Power (1965), 41 Can. Bar Rev. 446.

[313] This need not be exclusive jurisdiction, but related to the damages claimed.

[314] Although a usual way of dealing with reparation questions under French legal process.

"compensating"[315] the victim—has been developed. This enactment, if regarded as a successful experiment, will undoubtedly provide the statutory physiology for further reform.

Although many provinces lack general privacy legislation, the combined effect of the extant common law, and provincial and federal legislation, grants Canadians a fair measure of protection against invasions of privacy. More so than any other Commonwealth or European country[316] and perhaps as great as the United States where the countervailing interest in "the right to freedom of expression" is much more highly developed.[317]

But there is no room for complacency. A Canadian "Watergate" is not inconceivable despite our various checks on governmental power and the rewards of industrial espionage are so great that it would be naïve to assume that it has ceased merely because the old techniques have been rendered unlawful.[318]

In the last resort privacy, like any other value, must rely on the support it receives from the community. If state agencies and private groups are not subject to social condemnation, as well as legal sanctions, for infractions of the privacy legislation, the advantages of ignoring it will tend to outweigh those of observing it. The community must be alert to attacks on its privacy values and be prepared to expand or modify its systems of regulation as each new threat becomes apparent.

---

[315] This term is conceptually objectionable, since for constitutional purposes it is not compensation but part of the punishment. But in reality is it not a form of reparation for injury which, by its very nature, is hardly capable of rational measurement?

[316] Strömhelm, Right of Privacy and Rights of the Personality, a Comparative Survey (1967).

[317] In Canada too, this interest is sometimes regarded as higher than that of the "Right to Privacy". See Weisstub, The Individual Right to Privacy vs. The Public Right to Knowledge, a paper delivered to the Canadian Association of Philosophers at the University of Toronto, June 1974.

[318] A "Watergate" situation creates a paradox, pointed out to me by Professor Peter North. Where there are strong defamation and privacy laws, the press is likely to be reluctant to engage in fringe investigative reporting and such laws are likely to be relied on by public authorities to prevent scrutiny of their own invasions of the privacy of others.