The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps

Jeremy Warner*

THE ISSUE OF DATA RETENTION is one that has become prominent in recent times, particularly with the recent extension of Canadian privacy legislation to cover the private sector. This paper investigates the origins of the prohibition on data retention under European and Canadian law and its subsequent development in Europe and Canada with an emphasis on the trends, disparities and other consequences generated by the prohibition since 1968, the date of the first Council of Europe recommendations in relation to data protection in general. In Europe, ever since the first proposal for harmonized data protection laws was made by the Council of Europe in 1973, one of the fundamental principles of data protection law has been that of data retention or data conservation—that is, the obligation of the data user or controller to keep data for a limited period of time only. The 1995 EU Directive on Data Protection contains an express data-retention principle. The OECD Guidelines, which were used to develop Canada's privacy standard and subsequent privacy legislation, are less explicit. In Canada, Part 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA) establishes Principle 5 on data retention or data conservation, which is closely allied with its European counterpart. The connections between each of these discrete legal instruments are obscured by the legal backgrounds to each of PIPEDA and the EU Directive. The paper examines the data-retention principle under PIPEDA, analyzing the extent to which this principle has been influenced by the European legal developments and the extent to which other factors were important in shaping this fundamental rule.

LA QUESTION DE LA RÉTENTION DES DONNÉES est devenue un sujet de l'heure récemment, en particulier avec l'extension récente de la loi canadienne relative à la protection de la vie privée au secteur privé. Cet article examine les origines de la prohibition de la rétention des données en droit européen et canadien et son évolution subséquente en Europe et au Canada, en insistant sur les tendances, les disparités et les autres conséquences de cette prohibition depuis 1968, date à laquelle le Conseil de l'Europe a fait ses premières recommandations relativement à la protection des données en général. En Europe, depuis que le Conseil de l'Europe a proposé pour la première fois en 1973 l'harmonisation des lois relatives à la protection des données, l'un des principes fondamentaux de cette protection est la rétention ou la conservation des données, c'est-à-dire l'obligation que l'utilisateur ou le contrôleur de données ne conservent les données que pour une période limitée seulement. La Directive de l'UE sur la protection des données personnelles de 1995 énonce un principe exprès en matière de la rétention des données. Les lignes directrices de l'OCDE, utilisées pour développer les normes canadiennes et les dispositions législatives en matière de la protection de la vie privée, sont moins explicites. Au Canada, la partie I de la Loi sur la protection des renseignements personnels et les documents électroniques énonce le principe 5 sur la rétention ou la conservation des données, qui est très similaire au principe européen. Les rapports entre ces instruments juridiques distincts ne sont pas toujours clairs étant donné leurs antécédents respectifs. L'article étudie le principe canadien de la rétention des données, en cherchant à cerner l'influence de l'évolution du droit européen et les autres facteurs importants qui ont modelé cette règle fondamentale.

---

* Lecturer in Information Technology Law at the University of Strathclyde, Glasgow, Scotland. The author would like to acknowledge with thanks the comments provided by Professor Donald Nicolson and the comments of peer reviewers in the preparation of this paper. Any errors or omissions are, of course, the sole responsibility of the author.

77 1. INTRODUCTION

80 2. THE LEGAL BACKGROUND TO THE DATA RETENTION PRINCIPLE UNDER EUROPEAN LAW

80 *2.1. Early development of the principle of data retention in Europe*
83 *2.2. Consolidation of the European concept of data retention*

83 2.2.1. From the Convention to the Directive
88 2.2.2. The European Union Directive

90 3. THE LEGAL BACKGROUND TO THE DATA RETENTION PRINCIPLE UNDER THE OECD AND UN GUIDELINES

90 *3.1. Data Retention and the OECD Guidelines*
91 *3.2. Data Retention and the UN Guidelines*
92 *3.3. Analysis of the Influence of OECD/UN Guidelines on PIPEDA and on provincial privacy legislation*

92 4. THE CANADIAN PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

92 *4.1. Introducton to PIPEDA*
94 *4.2. The views of the European Commission on PIPEDA*
97 *4.3. Data retention under PIPEDA*
100 *4.4. Implementation of the data-retention principle in Canada's provincial legislation*

103 5. CONCLUSIONS

The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps

Jeremy Warner

I. INTRODUCTION

THE ISSUE OF DATA RETENTION recently hit the news in the United Kingdom in spectacular fashion when a regional police force, which had at one time held a police file on someone who was eventually convicted of two high-profile murders, stated that "data protection laws meant it could not keep records of unproven claims against [that person]."[1] In Europe, the most topical issue involving data retention has been the proposals from law-enforcement authorities in favour of mandatory systematic retention of communications data, namely email communications and mobile-phone data for use in criminal investigations.

These proposals stem from the data-preservation requirements of the Council of Europe *Convention on Cybercrime*.[2] These requirements have also been the subject of discussion in Canada within the context of the recent *Lawful Access Consultation Document*[3] under the aegis of the Department of Justice. These topical issues relate to the proposed legal obligations to retain records, in addition to the existing multifarious obligations to retain data in the context of, for example, taxation and health and safety at work. The function of this paper is to examine the growth and development of legal restrictions on the retention

---

1. "Data protection guidance pledge" *BBC News* (January 14, 2004), <http://news.bbc.co.uk/1/hi/uk/3395071.stm>. This issue was subsequently examined in detail as part of the Bichard Inquiry, an independent inquiry into the way in which information was handled by the police. See The Bichard Inquiry Report for further details at <http://www.bichardinquiry.org.uk>.
2. This convention (Council of Europe, Committee of Ministers, *Convention on Cybercrime*, CETS No. 185 (2004), <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>), which opened for signatures on November 23, 2001, is an international treaty, with a particular focus on the substantive elements of computer crime and the legal mechanisms to investigate and prosecute those crimes. As of April 7, 2004, thirty-seven states had signed the Convention, including Canada, and five states had ratified the Convention, including three member states of the Council of Europe. The Convention entered into force on July 1, 2004. Articles 16 and 17 deal with the expedited preservation of stored computer and traffic data.
3. The consultation document (Department of Justice Canada, *Lawful Access—Consultation Document* (Ottawa: Department of Justice Canada, 2002), <http://canada.justice.gc.ca/en/cons/la_al/index.html>.) was opened for submissions in August 2002 and was closed in December 2002. A summary of the submissions received was made available in August 2003.

of records—the right to oblivion—rather than the requirement of retention or preservation of records.

While the retention of records is a habit shared throughout the world, restrictions on data retention are becoming increasingly widespread. In particular, Canadian legislation has introduced restrictions on the retention of records in the private sector,[4] which came into effect on January 1, 2004. This extension of the law in Canada is the latest in a long line of international legal developments in relation to data retention and it is the aim of this paper to analyze the Canadian law on data retention within that context. The topical nature of the changes in Canadian law provide an excellent opportunity to reflect on the influence that historical international legal developments have had on the development of data protection law in Canada, with particular focus on the issue of data retention.

European data protection law has offered a basis rooted in the fundamental human right to privacy for the introduction of these data-retention obligations. The European Union *Council Directive 95/46/EC*[5] provides in recital 2 that "…data-processing systems must…respect…[the] fundamental rights and freedoms [of individuals], notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals."[6] The reference in this context to trade expansion is important, because the individual rights that the principle of data retention seeks to protect are subject to the countervailing interests of trade and social progress. Furthermore, the interests of national security and of the prevention and detection of crime must also be balanced with individual rights and freedoms. The European Data Protection Commissioners issued a statement in 2002 in relation to proposals from law-enforcement authorities in favour of mandatory systematic retention of communications data for one year. They stated that "…such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8[7] of the European Convention on Human Rights…."[8]

This perspective is supported by the Council of Europe. In the *Explanatory Report for the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, the instrument upon which the data-retention principle under the Directive was based, it is stated that:

---

4. Restrictions have applied to public/federal entities since the relevant legislation was adopted in 2000.
5. EC, *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [the Directive].
6. *Ibid.*, s. 2.
7. Council of Europe, Committee of Ministers, *Convention for the Protection of Human Rights and Fundamental Freedoms*, CETS No. 005 (1950), <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.
8. Foundation for Information Policy Research, Statement Release, "Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data" (September 11, 2001), <http://www.fipr.org/press/020911DataCommissioners.html>.

> "Information power" brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerised data files: payroll, social security records, medical files, etc. It is essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored. For this reason, they should … refrain from storing information which is not necessary for the given purpose….[9]

In the context of data retention in particular, Resolution 74 (29) provided that "individuals have a legitimate interest in seeing certain kinds of information concerning them, particularly that which is harmful to them, wiped off or rendered inoperative after a certain time has passed."[10] The Council of Europe has also recognized the "threat to privacy if information relating to any individual is allowed to accumulate as the years go by."[11] In this new age of the "Information Society," restrictions on keeping personal information have a resounding impact on the operations of all organizations dependent on information about individuals. Accordingly, data retention is one of the core principles of personal data processing necessary to ensure respect for the fundamental rights and freedoms of individuals—notably the right to privacy—and, in particular, to strengthen those rights and freedoms by restricting the right of data users to accumulate personal data freely without any time limitation.

Data retention has been subject to quasi-legal restrictions in Europe since the late 1960s. The first proposal for harmonized data-protection laws in Europe was made by the Council of Europe in 1973.[12] Since then, one of the fundamental principles protecting individual rights in this area has been that of data retention or data conservation. In essence, this places a negative obligation on data users or controllers to keep data only for a limited period of time. The data-retention principle receives its impetus from the view that data protection does not justify storage simply on the basis that one never knows whether some data "… might perhaps come in handy in any unforeseeable future."[13] In 1990, in response to the growing demand for a harmonized approach to data protection in Europe, the European Commission proposed the Directive to deal with issue

---

9. Council of Europe, Committee of Ministers, *Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Texts Adopted, ETS No. 108 (1981), <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm>, para. 2.
10. Council of Europe, Committee of Ministers, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, Texts Adopted (1974), <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20(74)%2029.asp>, para. 21.
11. Council of Europe, Committee of Ministers, *Explanatory Memorandum to Recommendation No. R (81) 1 on regulations for automated medical banks*, Texts Adopted (1981).
12. Council of Europe, Committee of Ministers, *Resolution 73(22) on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, Texts Adopted (1973), <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20(73)%2022.asp>.
13. Council of Europe, Project Group on Data Protection, *Second evaluation of the relevance of Recommendation R (87)15 regulating the use of personal data in the police sector, done in 1998*, (1999) at s. 5.2.3, <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/Reports/J-Report%202%20R(87)%2015.asp>.

of processing personal data. From that proposal to the point where the European Parliament adopted the Directive,[14] the European Union institutions refined the data-retention principle to a simple statement. The simplicity of the principle set out in the Directive is to its advantage, and the benefits of this approach are discussed below.

Canada's current data-retention law is found in the *Personal Information Protection and Electronic Documents Act*.[15] It is acknowledged that federal and provincial privacy legislation has existed in relation to the public sector, and specifically in relation to health records, since 1982[16] and that *PIPEDA* is not the starting point for Canadian data-protection law, which has a history spanning several decades.[17] That being said, the recent coming into force of *PIPEDA*'s provisions relating to the private sector is an important step in the evolution of Canadian privacy legislation. Even though this paper focuses on data retention I will also briefly discuss this statute as a whole and its shortcomings in the context of data retention. It is trite to comment that *PIPEDA* was heavily influenced by the Directive, which is a matter that this paper shall establish. However, the nature and extent of that influence is uncertain, particularly in view of the competing influence of US privacy developments and of other international commitments in the 1980s.

In the first part of this paper I will examine the nature and extent of the prohibition on data retention under European data-protection law, with an analysis of the meaning of the principle with reference to European and international developments in this field. I will investigate the origins of the prohibition on data retention under European law and its subsequent development in Europe, examining the trends, disparities and impact of the prohibition as it has developed since 1968. The paper will conclude with an examination of the influence of European law and of other international instruments on the formation of the data-retention principle under *PIPEDA*, together with a systematic and comparative analysis of data retention under *PIPEDA* and under provincial legislation in Canada.

*

2. THE LEGAL BACKGROUND TO THE DATA RETENTION PRINCIPLE UNDER EUROPEAN LAW

2.1. Early development of the principle of data retention in Europe

THE DATA-RETENTION PRINCIPLE, or the data-conservation principle as it is sometimes known, has its origins in *Recommendation 509 of the Council of Europe on human rights and modern scientific and technological developments*, which was

14. *Supra* note 5.
15. S.C. 2000, c. 5 [*PIPEDA*], <http://laws.justice.gc.ca/en/P-8.6/92607.html>.
16. It is beyond the scope of this paper to examine these instruments. For further information see Tina Piper, "The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's 'Technological Society'" (2000) 23 Dal. L.J. 253 at p. 264.
17. See John MacDonnell, "Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?" (2001) 39 Alta. L. Rev. 346 at pp. 362–64.

adopted in 1968.[18] This acknowledged "… the serious dangers for the rights of the individual"[19] which were, in its view, inherent in some aspects of modern technology. Soon after this early statement in relation to local-government data processing,[20] it was stated that there was a need for "data banks" to be restricted to the necessary minimum of information required for specific purposes such as taxation and the allocation of benefits. Such vague and piecemeal coverage failed to address the reality of the data-processing future.

Data retention continued to be developed at the European level in the early 1970s. In fact, further European developments followed the publication in the United States of a voluntary code of *Fair Information Practices*.[21] The code has been criticized in terms of its effectiveness, in particular by the Center for Democracy & Technology:

> Despite the clear language and intent of the 1973 principles, in practice they have failed to adequately protect the privacy of personal information. The Privacy Act of 1974, which codified the 1973 principles, has been undermined by legislative loopholes, lukewarm implementation by government agencies, and broad interpretation by courts.[22]

Recent proposals to update the code in 1994 and 1995[23] were also heavily criticized, especially because of the perceived inadequacies of the acquisition principle which states that: "Users of personal information should ... obtain and keep only information that could be reasonably expected to support current or planned activities and use the information only for those or compatible purposes."[24] This has a connection with data retention in terms of linking the retention of data to current or planned activities. These principles do not otherwise include a discrete data-retention principle. Nevertheless, they have been described by MacDonnell as the principles upon which many European nations subsequently based their data-protection laws.[25]

The Annex to Resolution 73 (22),[26] Principle 4, which the Council of Europe intended to apply to the storage of personal information in electronic

---

18. Council of Europe, C.A., 19th Ordinary Sess. (Third Part) *Recommendation 509 (1968) on human rights and modern scientific and technological developments* (1968), <http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/ta68/EREC509.htm>.
19. *Ibid.*, para. 2.
20. See Council of Europe, C.A., 21st Ordinary Sess. (First Part), *Recommendation 557 on the use of computers in local government* (1969), <http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/ta69/EREC557.htm>. See also Council of Europe, Committee of Ministers, *Resolution (73) 2 of the Committee of Ministers to Member States on Ways and Means of Encouraging the Use of Computers in Local Government,* Texts Adopted, Res. (73)2 (1973).
21. MacDonnell, *supra* note 17 at 358.
22. Center for Democracy and Technology, "CDT submits these comments on the draft 'Principles for Providing and Using Personal Information'" (1995) Legislative Comment, <http://www.cdt.org/privacy/comments_iitf.html>.
23. The Working Group on Privacy, part of the Information Infrastructure Task Force (IITF) in the United States, issued its initial draft "Principles for Providing and Using Personal Information," on May 25, 1994 (59 Fed. Reg. 27206, No. 100) and its second draft on January 25, 1995 (60 Fed. Reg. 4362, No. 13).
24. *Supra* note 22.
25. MacDonnell, *supra* note 17 at p. 358.
26. *Supra* note 12, Annex.

data banks, requires rules to be "… laid down to specify the periods beyond which certain categories of information should no longer be kept or used."[27] This annex, however, contained several fundamental flaws. First, no guidance was provided as to what form those "rules" should take, which was hardly a portent of harmonized European rules on the subject. Second, while hindsight makes this comment easier to make, it must have been clear even in 1973 that specific periods could not be laid down for the retention of different categories of data without taking account of the specific individuals or organizations holding that data and of the reasons for which that data was being held. In fact, this problem was acknowledged by the Committee of Ministers in the Explanatory Report attached to Resolution 73 (22).[28] Third, it was not clear from the language used whether the time limit was to apply to the passive storage of data or to the active use of data or to both. Principle 7 supplemented Principle 4 insofar as it provided that data users had an obligation to "erase [*sic*] obsolete information,"[29] meaning that data users would have to examine not only the age of data stored by them but also whether stored data was obsolete from the outset.

Although not specifically excluded in the context of Resolution 73 (22), it was intended that the prohibition on data retention would not apply to information that remained indefinitely valid, such as "names, birth dates, diplomas or other qualifications acquired by a person."[30] However, the Resolution suggested that data users implement the rule by programming computers to erase the pertinent information automatically when the terminal date was reached.[31] The Committee also categorically denied that it was recognizing a formal "right of oblivion" for data, but instead claimed that it was seeking to protect individuals from the unreasonably long retention of possibly harmful data.[32]

The Resolution applied to any information relating to living natural persons but only if it was stored in "electronic data processing systems used to handle … and to disseminate [that] information."[33] On that basis, the impact of the Resolution was limited, particularly in view of the fact that dissemination of computerized information was not commonplace in industry at the time. To a large extent, Resolution 74 (29) mirrors these words in relation to processing in the public sector.[34] The only difference is that, by way of clarification, the 1974 version states that the rules should specify "time limits" rather than periods "beyond which information should not be kept or used."[35]

In the context of *PIPEDA*, the three criticisms discussed in relation to Resolution 73 (22) apply to some extent.[36] No guidance is provided on the form

27. *Ibid.*, para. 4.
28. *Ibid.*, Explanatory Report. In its explanatory report attached to the Resolution, the Committee of Ministers explained that Principle 4 was not specific, on the basis that rules on data retention could either be laid down by law or by the user of the relevant data bank and that the form which those rules took would depend to a large extent on the character of the information being stored and disseminated.
29. *Ibid.*, Annex, para. 7.
30. *Ibid.*, Explanatory Report, para. 23.
31. *Ibid.*
32. *Ibid.* Explanatory Report, para. 24.
33. *Ibid.*, Annex.
34. *Supra* note 10.
35. *Ibid.*, Annex, para. 4.
36. See above critique of Resolution 73 (22).

of the guidelines and procedures to be used in establishing retention periods; this has already created difficulties for provincial legislatures interpreting the provisions. Furthermore, it is not made explicit in section 4.5 of *PIPEDA* that retention periods will vary depending on the nature of the information in question. Finally, however, *PIPEDA* does answer the third criticism of the early European efforts in relation to data retention: data retention under *PIPEDA* requires fixed periods of time to apply to the retention of information, not to the use of information.

The 1974 Resolution also acknowledged that the public sector could have legitimate grounds for requiring the retention of data beyond these time limits. Accordingly, the Council of Europe recognized exceptions where the information was used for statistical, scientific or historical purposes and where such use required the data to be "conserved" for an indefinite duration, subject to precautions being taken to protect individual rights to privacy. These exceptions were specifically directed at public authorities and governments, which, as guarantors of continuity, "have a special duty to preserve certain information for posterity."[37]

It is a feature of the development of European data-protection law that the private and public sectors were treated separately before they were eventually treated equally for the purposes of data-protection law. However, the early observations that hailed the public sector as the guarantor of continuity—meaning that there had to be somebody with one eye on the future interests of society while accessing information from the past—have never been voiced in relation to the private sector.[38] *PIPEDA* does not do so either. Private databases have been growing in number over the last twenty years and the information contained in those databases may be of the type that ought to be preserved for posterity. This raises the question of whether there is any support for extending the duty of guarantor of continuity into the private sector? And, if so, to what extent would that duty affect the basic restrictions on data retention discussed in this paper?

The foundation stone for the principle of data retention was laid in the 1970s by recommendations of the Council of Europe. Not only was it clear by the middle of the decade that some form of prohibition on the retention, conservation or use of data was required, but also that the Council of Europe had by this time established its principal justification for seeking harmonized rules with respect to this matter—namely, that individuals needed to be protected from the harm that could result from the retention of data for an unreasonable length of time. The same justification applies in the context of *PIPEDA* and data retention today.

2.2. Consolidation of the European concept of data retention

2.2.1. From the Convention to the Directive

The Council of Europe *Convention on Data Protection* ("the Convention") covered the "automatic processing" of personal data, including automated data storage and computer processing and the alteration, erasure, retrieval and dis-

37. *Supra* note 10, Explanatory Memorandum, para. 22.

38. Except to the limited extent in relation to historical and statistical research where the information is to be anonymized.

semination of data, in both the private and the public sectors.[39] Article 5 of the Convention provided that personal data should be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."[40] This marked an important change in emphasis for the principle of data retention. The principle still required erasure or deletion of personal data but focused on the form of the data being retained. Data that was held or preserved in a form that did not allow identification of data subjects could be retained indefinitely. Even if the data subjects could be identified, the time limit or period during which the data could be stored or processed was as long as was required for the purpose for which the data was stored or processed. This also marked another important development: a rule had been promulgated that provided organizations with a clear basis upon which to set retention periods, namely the purposes for which they were processing the data in question.

Each of these points has been incorporated within *PIPEDA*. First, there is the recommendation in section 4.5.3 in relation to rendering information anonymous. This also follows the recommendations contained in the *OECD Guidelines* that were finalized at approximately the same time as the Convention.[41] Second, the crucial link between retention and the purposes of processing is set out in section 4.5 of *PIPEDA*.

In providing guidance on the terms of the Convention, the Council of Europe noted that this did not mean that "data should after some time be irrevocably separated from the name of the person to whom they relate" but rather that "it should not be possible to link readily the data and the identifiers."[42] Previous recommendations had been leading toward a broad and effective prohibition on data retention that supported the protection of privacy interests. This statement, by allowing organizations to avoid the prohibition where it was not possible to link data and individuals readily, went a long way towards undermining that protection. It suggested that data could be retained indefinitely as long as it was not immediately or "readily" possible to link individuals with the data held on them. Future developments of European law on data retention, culminating in the Directive, would move away from the approach of ready identification set out in the Convention, preferring a more absolute and less subjective test of identification.[43]

---

39. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, E.T.S. No. 108, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&CL=ENG>.

40. *Ibid.*, Article 5e.

41. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications Service, 2001), <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

42. *Supra* note 9.

43. See *e.g.* EC, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] O.J. L. 201 at Article 8, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>, dealing with the retention of communications data only. However, these developments do not modify the data retention principle in the Directive.

Of the recommendations adopted by the Committee of Ministers immediately following the Convention, several introduced significant developments on the "data-retention" theme. Recommendation No. R (81) 1 applied to the operation of medical data banks and included a requirement for the operators of such data banks to publicize and adhere to a set of regulations that should include a section on the "long-term conservation of data."[44] It also provided that, generally, "data relatable to an individual should be kept on record only during a period reasonably useful for reaching their main purpose(s)."[45] However, an exception was recommended for situations where, in the interests of public health, medical science, or for historical or statistical purposes, it would be justifiable "to conserve medical data that have no longer any immediate use" before and after the death of the relevant data subject.[46]

For the first time, it was recommended that the usefulness of data should be a factor to be considered in defining retention periods and that information about the retention policy used by an organization was to be made available. In *PIPEDA* and in more recent European data-protection laws, the consideration of usefulness has been replaced with a consideration of the necessity for the retention of data to fulfil specified purposes. Such a concept of necessity is not far removed from the early-1980s concept of usefulness. On the other hand, a central criticism of the recommendations on data retention in *PIPEDA* is that section 4.5.2 does not directly recommend publication of retention policies by organizations—something that was demonstrably part of European data-protection thinking in the early 1980s.

The principle of data retention continued, after 1984, to be developed in a piecemeal fashion at the European level. Recommendations were made by the Committee of Ministers of the Council of Europe covering areas as specific and diverse as social security,[47] police records,[48] employment,[49] credit-card processing,[50] telecommunications[51] and medical records.[52] Throughout these rec-

---

44. Council of Europe, Committee of Ministers, *Recommendation No. R (81) 1 of the Committee of Ministers to Member States on Regulations for Automated Medical Data Banks*, Texts Adopted, Rec. (81) 1 (1981), <https://wcm.coe.int/ViewDoc.jsp?id=680983&Lang=en>, s. 3.1(j) of Appendix to Recommendation No. R(81) 1.

45. *Ibid.*, para. 7.1.

46. *Ibid.*, para. 7.2.

47. Council of Europe, Committee of Ministers, *Recommendation No. R (86) 1 of the Committee of Ministers to Member States on the Protection of Personal Data used for Social Security Purposes*, Texts Adopted, Rec. (86) 1 (1986), <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Recommendation%20(86)%201.asp#TopOfPage>.

48. Council of Europe, Committee of Ministers, *Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector*, Texts Adopted, Rec. (87) 15 (1987), <https://wcm.coe.int/ViewDoc.jsp?id=704881&Lang=en>.

49. Council of Europe, Committee of Ministers, *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, Texts Adopted, Rec. (89) 2 (1989), <https://wcm.coe.int/ViewDoc.jsp?id=710373&Lang=en>.

50. Council of Europe, Committee of Ministers, *Recommendation No. R (90) 19 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Payment and Other Related Operations*, Texts Adopted, Rec. (90) 19 (1990), <https://wcm.coe.int/ViewDoc.jsp?id=603199&Lang=en>.

51. Council of Europe, Committee of Ministers, *Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services*, Texts Adopted, Rec. (95) 4 (1995), <https://wcm.coe.int/ViewDoc.jsp?id=529167&Lang=en>.

52. Council of Europe, Committee of Ministers, *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*, Texts Adopted, Rec. (97) 5 (1997), <https://wcm.coe.int/ViewDoc.jsp?id=571075&Lang=en>.

ommendations, there were a number of recurring themes.

First, the connection, which was established by the Convention, was maintained between the reason for the data being processed and the permitted retention period for that data. A clear link was established during this period between the purposes behind the processing that was taking place and the length of time over which that data could lawfully be retained. For example, Recommendation No. R (86) 1 looked at the length of time that was justified for the accomplishment of the relevant task and which was not prejudicial to the interests of the individual data subject. Similarly, Recommendation No. R (87) 15 stated that the data should be deleted if no longer necessary for the purposes for which they were stored, such that there would no longer be a need to retain data following the conclusion of an inquiry into a particular criminal case. Recommendation No. R (89) 2 proposed limiting the storage of personal data by an employer to a period no longer than is justified for the recruitment of employees, the fulfilment of the contract of employment or management, or the planning and organization of work, or in order to satisfy the interests of a present or former employee; Recommendations No. R (90) 19 and No. R (97) 5 continued in a similar vein. Recommendation No. R (95) 4 stated that data needed for billing purposes, such as itemized billing data, should not be stored for any longer than is strictly necessary for settling an account with the data subject, although this could be extended where such data needs to be kept for a reasonable period in order to deal with billing complaints, or to satisfy legal obligations, of the operator or service provider.

During the period after the Convention, the trend was very much one of linking the retention period increasingly closely with the underlying processing justifications. The developments also continued to move towards some necessity or requirement for the data to be kept rather than simply for the sake of convenience or usefulness. This indicated that future rules on data retention would become increasingly focused, discrete and discordant. For those interested in individual rights to self-determination of processing activities carried out in relation to their personal data, a particularly outrageous development was the hint that there could be situations where data could lawfully be retained beyond that period of time necessary for relevant processing purposes where there was an additional interest in doing so, such as service-provider interests or where it was adjudged to be in the individual data subject's interests to do so.

In connection with the provincial legislation developed since *PIPEDA*, the legislation introduced in British Columbia and Alberta has illustrated that this theme continues to apply to data-protection law. In each jurisdiction, the provincial legislation allows information to be retained beyond that time period necessary for relevant processing purposes if there are legal or business purposes that justify such retention. These appear to be broad and subjective exceptions to the general rule under *PIPEDA* and, if accepted as "substantially similar" to *PIPEDA*, threaten the consistent application of the fundamental principle of data retention in Canada. If this approach is followed, and provincial legislation is allowed to apply

in lieu of *PIPEDA* despite these shortcomings, there is a risk to Canada's status as one of the few third countries to meet with European Commission approval.[53]

As a second theme, it became clear that fixed retention periods would need to be designated by each individual or each type of data user. For example, Recommendation No. R (86) 1 specifically required that storage periods be specified for each category of benefit and that directed storage periods be fixed for different categories of data depending on the data in question.[54] Similarly, Recommendation No. R (90) 19 suggested that further consideration was required in relation to the benefits of setting specific time limits for the retention or conservation of data.[55] In an interesting development, while looking at data concerning job applicants which is kept to defend potential legal proceedings such as those involving allegations of applicants being rejected on grounds of sex, race or religion, or that incorrect recruitment and interview procedures were followed, it is stated that: "The data should only be stored for a reasonable period. The circumstances will determine the length of the period. It goes without saying that, should legal proceedings not occur, the data are to be deleted."[56] The close link between the specific individual and the fixed retention period which should apply to their data is inherent in this statement. Recommendation No. R (87) 15 provided that such data should only be kept for a reasonable period of time.

These first two developmental themes are linked. Not only were data-retention rules to depend on the purposes of the processing in question, but also any fixed retention periods established following these rules would need to depend on the particular type of data in question. Thrown into the proverbial ring was the additional complication that there could be circumstances in which the retention period established for any given data could be a "reasonable" period of time. By its nature, such a retention period would depend on the particular data to which it related and on the other circumstances surrounding the relevant retention.

A third theme relates to the suggestion that organizations and local authorities should establish review procedures in line with their fixed retention periods. In particular, the *Evaluation of the relevance of Recommendation No. R (87) 15* adopted in 1999 found that "the law should be explicit about the duration of storage of criminal intelligence."[57] It also proposed a fixed number of years after the last addition of data to that record, followed by a periodic review

---

53. See Part IV (ii), below, in relation to the views of the European Commission on *PIPEDA*.

54. For example, data required for the operation of a company pension scheme would be retained long after the employee had retired.

55. For example, where personal data is used to process payment instructions by cheque, giro orders or payment cards, data users had to consider the merits of retaining data after any such means of payment had been refused and, where the payment has proceeded, the extent to which there was a need to retain that data for the purpose of defending legal actions or for furnishing proof of transactions carried out by the data subject.

56. Council of Europe, Committee of Ministers, *Explanatory Memorandum to Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, Texts Adopted, Exp.Rec. (89) 2 at para. 102.

57. Council of Europe, Committee of Ministers, *European Committee on Legal Co-operation (CDCJ) Final Activity Report—Evaluation of the Relevance of Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector in the Light of New Developments in this Field*, Documents, CM (99)28 (1999) at Appendix D, para. 5.2.3, <https://wcm.coe.int/ViewDoc.jsp?id=401937&Lang=en>.

and deletion, where appropriate, or a stricter system of obligatory deletion after a certain lapse of time. For the first time, the rules being proposed at a European level were raising awareness of the need for a systematic approach to compliance with the prohibition on data retention.[58] As discussed below, *PIPEDA* fails to provide the necessary guidance on specific data-retention periods to be applied by organizations processing personal information.

The fourth and final theme contained within the Council of Europe recommendations is raised by Recommendation No. R (95) 4, which proposed that information on the period over which communications data would be stored should be provided to data subjects, and that data subjects should have the right to require data to be deleted where it has been retained for an excessive period of time. This final development furthered the concept of user empowerment in the debate about data retention—a matter that was more fully enshrined in the Directive.

2.2.2. The European Union Directive

Following discussion in the European Commission about the perceived lack of harmonized laws on data protection within the EU, based partly on the fact that relatively few Member States had up to that point signed on to the Convention, the European Parliament adopted the Directive.[59] Article 6 required EU Member States to introduce provisions into their national laws directing that personal data be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they were further processed. Appropriate safeguards were to be laid down for personal data stored over longer periods for historical, statistical or scientific purposes.

Before the Directive, the direction that the prohibition on data retention or conservation had taken was divided along several different channels, with the earliest developments dealing with the retention of specific types of personal data or with specific types of processing activity. The first attempt to outline a general rule on data retention came with the Convention, based on the purposes of processing, necessity of storage and retention periods, and linked to the requirement for the data subjects to be identifiable from that data. The elements of that general rule were maintained throughout the 1980s and early 1990s and culminated with the requirements of the Directive. The idea of user empowerment by means of information given to individual data subjects about retention policies was also introduced. However, during this period several additional themes can be identified.

It was suggested that the retention of data had to be justified on the basis of usefulness or that the retention periods fixed by organizations should be reasonable. Data retention became more closely associated with specific processing industries or organizations rather than being focused on the purposes behind each type of processing, with different rules on retention applying to different types of processing. It was recommended that any data-retention periods

---

58. See Jeremy Warner, "Data Culling: The Scope of the Fifth Data Protection Principle" (2002) 37 Scot. L. Times 303.

59. See *supra* note 5.

established by data users should depend on the category of data being processed. Lastly, the requirement for organizations to implement retention, review and deletion policies was introduced into the debate. Although not explicitly proposed in terms of the Directive, these themes have continued to have an influence on modern thinking about data retention. They are represented in *PIPEDA* in sections 4.5.2 and 4.5.3 with the recommendations to develop policies and procedures documenting retention periods for information.

However, there were a number of areas concerning the data-retention principle that have never been resolved. First, the question that was highlighted in the *Annex to Resolution 73 (22)*,[60] namely whether specific retention periods need to be applied to both the period of time during which data can be retained and the period of time during which data can be used by the data controller. The Directive applies a time limit to the period during which data can lawfully be kept. Similarly, the Convention focused on the period of time that the relevant data could be "preserved" and European developments in the 1980s looked at the "storage" of data. *PIPEDA* itself is concerned solely with the period of retention of data. However, early statements of the principle looked at the length of time over which data could be kept or used and, in Canada, the provincial legislation in Quebec[61] places a time limit on the period during which information may be used, rather than simply being retained. Is the data-retention principle intended to apply not only to the storage or retention of data in the widest sense but also to active use? It is a matter that European data-protection law has dealt with inconsistently, and this inconsistency has been repeated in Canada.

Second, the *Explanatory Report on the Convention*[62] proposed that data could be retained indefinitely as long as it was not immediately or "readily" possible to link individuals with the data held on them. In defining "personal data", the Directive links that concept to the identification of a natural person—a concept which has been interpreted differently in different member states of the European Union.[63] The concepts of identification and anonymity have been interpreted differently throughout Europe in the absence of clear guidance on the subject. Without further explanation of the meaning of the term "anonymous" as used in section 4.5 of *PIPEDA*, the inconsistency witnessed across Europe in the implementation of the Directive is likely to be reflected among provincial statutes seeking to expand on the term as used in *PIPEDA*.

Third, in the early 1980s it was proposed that, in certain circumstances, data could be retained provided that it was reasonably useful to do so for certain processing purposes. Following the Convention, European data-protection law based data-retention periods on the period of time necessary for data to be

---

60. *Supra* note 12.

61. The Quebec legislation is an example of legislation that has been approved by the Canadian government as being "substantially similar" to *PIPEDA*. See the *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1, <http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1.html>.

62. *Supra* note 9.

63. European Commission, *Report from the European Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)* (Luxembourg: European Union Publications Office, 2003) at para. 3, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=52003DC0265&model=guichett>.

retained pursuant to specified processing purposes. Subsequent developments have been broadly aligned with that principle. The wording of *PIPEDA* permits no right of retention where mere usefulness, reasonableness or convenience is the only justification for keeping data. However, elements of usefulness and reasonableness have found their way into the provincial legislation introduced by British Columbia.

The Convention and the Recommendations of the Council of Europe that immediately followed that instrument share many aspects with *PIPEDA* and with the provincial legislation enacted to conform to *PIPEDA*. It is notable that the Council's attempts to expand on the basic principle of data retention were not consolidated as part of the principle when it was included in the Directive. This historical perspective may provide a window on the future of Canadian data-retention law. Given the conflicting development of provincial legislation in the short time since *PIPEDA* was enacted, it is submitted that a data-retention principle that is general and simplistic is likely to generate greater consistency in application and greater flexibility for organizations seeking to comply with the law, notwithstanding the criticisms that we have seen directed at such an approach. Attempts to expand on the principle and to provide an all-encompassing and exhaustive set of requirements for compliance will likely lead to inconsistency in application and rigid approaches to data retention which are not in keeping with the dynamic and wide-ranging practice of data processing in the private sector.

*

3. THE LEGAL BACKGROUND TO THE DATA-RETENTION PRINCIPLE UNDER THE OECD AND UN GUIDELINES

3.1. Data Retention and the OECD Guidelines

IT HAS BEEN REPORTED that "Canada formally adhered to the 1980 *OECD Guidelines* on the Protection of Privacy and Transborder Flows of Personal Data on June 29, 1984."[64] The *OECD Guidelines*[65] have been described as "the best known set of FIPs"[66] and as "among the first multinational efforts in this area."[67] It is surprising therefore to note that the Guidelines themselves do not contain any explicit statement on data retention.[68] However, data retention is discussed in the Explanatory Memorandum, which provides that:

---

64. EC, *Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data provided by the Canadian Personal Information Protection and Electronic Documents Act*, [2002] O.J. L. 002 at Recital 8, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002D0002&model=guichett>.
65. *Supra* note 41.
66. Fair Information Practices (FIPs).
67. *Supra* note 17 at p. 358.
68. *Supra* note 41.

> … when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.[69]

This explanatory extract is provided in relation to the Purpose Specification principle.[70]

As discussed below, the data-retention principle under *PIPEDA* incorporates elements drawn from the *OECD Guidelines*. In particular, section 4.5.3 contains an explicit reference to destruction, erasure or rendering anonymous that can be attributed to the influence of the *OECD Guidelines*. Nevertheless, *PIPEDA* establishes an explicit data-retention principle, whereas the *OECD Guidelines* do not. In this respect, there are strong grounds for suggesting that data retention under *PIPEDA* has been influenced more by the European model of data protection than by the core guidance set out in the *OECD Guidelines*.

3.2. Data Retention and the UN Guidelines

There are also grounds for suggesting that the influence of the *United Nations Guidelines Concerning Computerized Personal Data Files*[71] (the *UN Guidelines*) is manifested in *PIPEDA*. In particular, it has been reported that "Canada was [also] among the countries that supported the [UN] Guidelines … which were adopted by the General Assembly on 14 December 1990."[72] Within the context of data retention, Principle 3 of the UN Guidelines provides that:

> The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:
> …
> (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

Data retention is a secondary concern under the *UN Guidelines*. The rendering of information about the purpose of collection and use of information to data subjects is the primary concern in Principle 3, which serves the secondary purpose of making it possible to ensure that data-retention obligations are observed. Otherwise, the language used in Principle 3 of the *UN Guidelines* is similar to the data-retention principle in its simplest form expressed in the Directive and in section 4.5 of *PIPEDA*. Each of these instruments focuses on the

---

69. *Ibid.* at p. 44.
70. *Ibid.* at Part Two, para. 9:
> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use should be limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
71. *Guidelines for the Regulation of Computerized Personal Data Files*, GA Res. 44/132, UN GAOR, 44th Sess., Supp. No. 49, UN Doc. A/44/49 (1989) at 211, <http://www1.umn.edu/humanrts/instree/q2grcpd.htm>.
72. *Supra* note 64 at Recital 8.

period for which data or information is kept and each tie the retention period to the achievement of purposes for which the data or information was collected or was to be used.

These similarities are not, it is submitted, sufficient to establish any clear connection between the data-retention principle under *PIPEDA* and the same concept under the *UN Guidelines*. There is also no circumstantial evidence suggestive of a strong influence being exerted by the *UN Guidelines* over the form of *PIPEDA*, unlike the position in relation to the Directive. The *UN Guidelines* are not binding on Canada and there is no sanction for failure to adhere to the principles.

3.3. Analysis of the Influence of OECD/UN Guidelines on PIPEDA and on provincial privacy legislation

The strong similarities between the language used in the *OECD Guidelines* and in *PIPEDA* in relation to data retention are sufficient to indicate a strong possibility of influence. However, given the subsequent development of European data-protection law—in particular the reported influence of the *OECD Guidelines* on that development—this influence is more likely to have been indirect than direct. The role of the *UN Guidelines* is, however, less clear. The language and parameters of the data-retention principle embodied in the *OECD Guidelines* and in the *UN Guidelines* respectively are reflected to an extent in *PIPEDA*. *Prima facie*, in the absence of any indication to the contrary, there is little else to support the view that these instruments shaped data retention under *PIPEDA*. Accordingly, it is submitted that one must look to the European model of data-protection law, its origins and its subsequent development, in order to gain further insight into the meaning of data retention under *PIPEDA*.

*

4. THE CANADIAN PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

4.1. Introduction to PIPEDA

IT HAS BEEN COMMENTED that the enactment of *PIPEDA* established "basic, legally enforceable privacy protections"[73] and that it did so through the medium of "time-tested privacy principles that have been adopted around the world."[74] It is submitted that the principle of data retention is one of most far-reaching of these basic protections and time-tested principles. As we shall see, *PIPEDA* has also attracted criticism over its level of generality[75] and over ineffective oversight and enforcement mechanisms[76]—deficiencies that will continue to have a profound effect on the application of the data-retention principle in Canada.

---

73. *Supra* note 17 at p. 358.
74. Michael Geist , "Name names, or privacy law toothless" *Toronto Star* (17 November 2003), <http://www.michaelgeist.ca/resc/html_bkup/nov172003.html>.
75. Teresa Scassa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2000-2001) 32 Ottawa L. Rev. 1 at pp. 5–19.
76. Christopher Berzins, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" (2002) 27 Queen's L.J. 609.

PIPEDA was enacted on April 13, 2000 in order, amongst other things, "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances,"[77] those circumstances namely being commercial activities and the operation of a federal work, undertaking or business, either inter-provincially or internationally. *PIPEDA* has been the subject of extensive scrutiny by the European Commission Working Party and by the European Commission itself. In 2001, a European Commission Decision[78] reported as follows:

> As from 1 January 2004, the Canadian Act [*PIPEDA*] will extend to every organisation that collects, uses or discloses personal information in the course of a commercial activity, whether or not the organisation is a federally regulated business. The Canadian Act [*PIPEDA*] does not apply to organisations to which the Federal Privacy Act applies or that are regulated by the public sector at a provincial level, nor to non-profit organisations and charitable activities unless they are of a commercial nature. Similarly, it does not cover employment data used for non-commercial purposes other than that relating to employees in the federally regulated private sector. The Canadian Federal Privacy Commissioner may provide further information on such cases.[79]

Before considering the relative merits of the data-retention principle under *PIPEDA*, it is relevant to note that *PIPEDA* applies to all activities, commercial or otherwise, in a federal and international context but only to commercial activities in a provincial context.

PIPEDA only applied at the federal level until January 1, 2004, from when it has also applied to the private sector, except to the extent that "substantially similar" provincial legislation has been enacted in relation to the private sector. Section 26(2) of *PIPEDA* gives the Governor in Council, effectively the federal cabinet, the power "if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, to exempt the organization, activity or class from the application of this part in respect of the collection, use or disclosure of personal information that occurs within that province."[80] There is therefore a relationship of mutual exclusivity between the federal legislation, namely *PIPEDA*, and "substantially similar" provincial legislation. Section 26(2) further restricts the application of *PIPEDA* by excluding its application where provincial legislation dealing with the commercial activities discussed above has been enacted on a footing that is found by the Governor in Council to be substantially similar to that of *PIPEDA*. The extent to which provincial legislation has been enacted is to be

---

77. *Supra* note 15, Preamble to *PIPEDA*.
78. European Commission, *Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, (2002) O.J. L 2/13.
79. *Supra* note 64 at Recital 5.
80. *Supra* note 15.

the subject of yearly review by the Privacy Commissioner.[81]

No measured consideration of the data-retention principle can be carried out without regard for the general problems associated with *PIPEDA*. Notwithstanding the above-mentioned criticism of its generality and of its enforcement and oversight mechanisms, *PIPEDA* also contains substantial limitations. The first is its limited extension to the private sector—it does not apply to not-for-profit organizations, for example. The second is its relationship with provincial legislation—it does not apply where, for example, provincial legislation has been enacted to deal with privacy in the private sector in a manner that is ruled to be substantially similar to *PIPEDA* by the federal cabinet, as has occurred in the province of Quebec.

4.2. The views of the European Commission on PIPEDA

The Directive contains a general prohibition[82] on the transfer of personal data outside the European Economic Area.[83] One of the exceptions to this general prohibition applies to transfers of personal data to third countries that are the subject of a European Commission finding of adequacy.[84] At the time of writing, the European Commission has made several findings affirming the adequacy of protection provided by the legal and regulatory regimes in place in each of Argentina,[85] Guernsey,[86] Hungary,[87] Isle of Man[88] Switzerland[89] and the United States (specific only to organizations that have accepted the safe harbour privacy principles)[90] and, specifically, for the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of

---

81. *Ibid.*, s. 25(1), which provides that:

    > The Commissioner shall, as soon as practicable after the end of each calendar year, submit to Parliament a report concerning the application of this Part [Part I deals exclusively with personal-information protection], the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation.

82. Articles 25 and 26 of the Directive, *supra* note 5.

83. The European Economic Area (EEA) is comprised of the EU member states together with Norway, Iceland and Liechtenstein.

84. Article 25(6) of the Directive, *supra* note 5.

85. EC, *Commission Decision 2003/490 of 30 June 2003 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Argentina*, [1998] O.J. L 168/19, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_168/l_16820030705en00190022.pdf>.

86. EC, *Commission Decision 2003/821 of 21 November 2003 on the adequate protection of personal data in Guernsey*, [2003] O.J. L 308/27, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_308/l_ 30820031125 en00270028.pdf>.

87. EC, *Commission Decision 2000/519 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Hungary*, [2000] O.J. L 215/4, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00040006.pdf>.

88. EC, *Commission Decision 2004/411 of 28 April 2004 on the adequate protection of personal data in the Isle of Man*, [2004] O.J. L 151/48.

89. EC, *Commission Decision 2000/518 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Switzerland*, [2000] O.J. L 215/1, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00010003.pdf>.

90. EC, *Commission Decision 520/2000 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles*, [2000] O.J. L 215/7, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000D0520&model=guichett>.

Customs and Border Protection.[91] Each of these Commission findings of adequacy was preceded by an opinion from the European Commission Working Party on Data Protection[92] to the effect that, following scrutiny of the regime in question by the Working Party, that regime provided adequate protection within the terms of the Directive. The opinion of the Working Party is therefore of critical importance in paving the way for a Commission finding of adequacy.

The Working Party issued an opinion on the adequacy of *PIPEDA* in 2001.[93] In its conclusions, it reported that *PIPEDA*

> only applies to private sector organisations that collect, use or discloses personal information in the course of commercial activities. Moreover, the Act [*PIPEDA*] will enter into force in three stages, full implementation being scheduled only for 2004.[94]

In connection with the mutually exclusive relationship between federal *PIPEDA* and provincial equivalents, the Working Party recommended that the European Commission in particular should "look into the process leading to the definition of 'substantially similar' and to ascertain whether it is appropriate to individually recognise provincial laws as providing an adequate level of protection or if the same objective can be attained at the federal level through an Order in Council."[95] It recommended that "any adequacy finding for the Personal Information and Electronic Documents Act should reflect the limitations in scope and the implementation timetable."[96] While the latter concern regarding the implementation timetable has now subsided, the concerns relating to the limitations in scope of *PIPEDA* remain a source of continuing concern for the European Commission.

In reaching its conclusion as to whether it was appropriate to issue a Commission finding of adequacy, the Commission Decision asserted that *PIPEDA* "covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests and to recognize certain information which exists in the public domain."[97] Accordingly, following the Working Party's Opinion, the European Commission adopted Decision 2002/2/EC,[98] indicating that Canada was considered to provide an adequate level of protection for personal data transferred from the European Community to recipients sub-

---

91. EC, *Commission Decision 2004/535 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection*, [2004] O.J.L. 235/11, <http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf>.
92. The Working Party was established by Article 29 of the Directive as an independent EU advisory body on data protection and privacy. Its tasks are laid down primarily in Article 30 of the Directive.
93. EC, Article 29 Data Protection Working Party, *Opinion 2/2001 on the adequacy of the Canadian Personal Information Protection and Electronic Documents Act.*, 5109/00/EN, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002D0002&model=guichett>.
94. *Ibid* at 7.
95. *Ibid.*
96. *Ibid.*
97. *Supra* note 64, Recital 9.
98. *Supra* note 64.

ject to *PIPEDA*. For the purposes of examining the data-retention principle under *PIPEDA* and similar provincial legislation in Canada, it is sufficient to note that the Commission's finding that *PIPEDA* provides adequate protection enables the free movement of personal data between EU member states and Canada. This alone was a guiding incentive for the Canadian legislature to enact *PIPEDA* in a form appropriate to ensure that a Commission finding of adequacy could be given in relation to the act.

A Commission finding of adequacy is made in relation to the level of data protection in a third country in general. Although data retention is not central in determining whether a Commission finding of adequacy is issued, it is submitted that data retention will be a factor that will be considered by the Working Party and the European Commission in considering the level of protection in any third country. To support this view, it is necessary to consider the working document on assessing adequacy of protection in third countries that was adopted by the Working Party in 1998,[99] following the publication of a discussion paper on the same subject matter in 1987.[100] In both documents, the Working Party concluded that:

> Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a "core" of data protection "content" principles and "procedural/enforcement" requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements.[101]

However, the data-retention principle embodied in the Directive was not itself included by the Working Party within the set of basic content principles that the Working Party suggested should be included in any third country's data-protection requirements.

While the Working Party's suggestions indicate that the inclusion of a data-retention principle would not be mandatory in assessing the adequacy of protection provided by any third-country legal regime, it is difficult to argue with any real conviction that the absence of a data-retention principle on broadly similar terms to the equivalent protection provided by the Directive would have been more acceptable to the Working Party and the European Commission. It is arguable that the European Commission would not have reached the same conclusion on the level of adequacy provided under *PIPEDA* if it did not contain such a data-retention principle. Consequently, there is a strong argument to say that data retention in its current form under *PIPEDA* was influenced by the Directive. Accepting that the provisions of *PIPEDA* on data retention were influenced by

---

99. EC, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* Doc. D/5025/98, <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf>.

100. EC, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *First orientations on Transfers of Personal Data to Third Countries—Possible ways forward in assessing adequacy*, Doc. D/5020/97, <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1997/wp4_en.pdf>.

101. *Ibid.* at 5-6 and *Supra* note 99 at p. 5.

the Directive permits a direct connection to be established between the growing experience of the Canadian legislators in tackling data retention and the experience of the law-makers of the European Community and the Council of Europe in refining the concept of data retention over the last thirty years.

4.3. Data retention under PIPEDA

Part 1 of *PIPEDA* establishes Principle 5 on data retention or data conservation, which is closely allied with the data-retention principle under the Directive. The sections on the data-retention principle follow the wording used in the Canadian Standards Association *Model Code for the Protection of Personal Information*,[102] which itself was originally based on the *OECD Guidelines*.[103] The Working Party confirmed this, reporting that: "The privacy provisions in Schedule 1 of the Act [*PIPEDA*] are those of the CSA *Model Code for the Protection of Personal Information*, recognised as the Canadian national standard in 1996."[104]

Principle 4.5 provides that:

> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.[105]

It is the last sentence of section 4.5 that sets out the Canadian data-retention principle under *PIPEDA*. The fundamental principle follows the terms of the European data-retention principle closely. In particular, the Canadian data-retention principle (a) focuses on data retention, rather than usage; (b) applies a test of necessity to that retention; and (c) is connected to the purposes or fulfilment of the purposes for which the data were collected. From the evidence of the Privacy Commissioner's findings under *PIPEDA*,[106] the Privacy Commissioner will expect a reasonably strong link between the ongoing retention of data and the purposes for which the data was collected.[107]

---

102. Canadian Standards Association, *Model Code for the Protection of Personal Information*, CSA Standard CAN/CSA-Q830, <http://www.privacyexchange.org/buscodes/standard/canadianstandards.html>.

103. *Supra* note 41.

104. *Supra* note 93.

105. *Supra* note 15, s. 4(5).

106. The Privacy Commissioner's findings under *PIPEDA* are available at <http://www.privcom.gc.ca/cf-dc/2004/index2-4_e.asp>.

107. Case #6 considered a bank that had retained credit-card application data after the application had been turned down. The Commissioner considered it unreasonable that the data would remain accessible indefinitely and, accordingly, found that the bank had contravened section 4.5 (see <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010723_02_e.asp>). Case #139 concerned a bank that had retained data provided by the father of a loan/credit applicant after the loan had been denied. The Commissioner found that the information had not been collected for a proper purpose and therefore that the data had been retained for too long a period (see <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_8_e.asp>). Case #255 concerned the retention of photographic images and pass-application data by a Canadian airport authority that had been obtained from Canada Customs and Revenue Agency employees needing security clearance to work at that airport. The investigation showed that the data had been kept in case the individual returned to work at the airport at some time in the future. The Commissioner found that the practice of keeping the data did not fulfil any purpose and that there had been a contravention of Principle 4.5 (see <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031224_e.asp>). In case #157, the Commissioner found that there was a strong link between a six-year retention period and the purposes for which the data had been collected (which were to provide credit grantors with current information on the financial performance of credit applicants) and that, accordingly, there was no contravention of Principle 4.5, (see <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_2_e.asp>).

In addition, section 4.5.2 provides that:

> Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

The use of the word "should" in this context rather than the word "shall" is important. Given the interpretive section of *PIPEDA*,[108] which provides that the use of the word "should" denotes a recommendation rather than an obligation, this word choice seems to weaken the legislation by introducing "an unhelpful degree of uncertainty."[109] Clearly, with reference to *PIPEDA*'s data-retention principle, this crucially reduces the strength of the obligation to comply with the requirements of data retention under that piece of legislation. It is submitted that this approach does little to "allay concerns about indefinite retention of personal information,"[110] which have been cited as the justification for the inclusion of specific data-retention protections, despite the positive approach to enforcement of these recommendations that has been adopted by the Privacy Commissioner to date.[111]

Section 4.5.2 therefore contains recommendations as set out above that appear to do no more than elaborate on the requirements of section 4.5.[112] In elaborating on the basic principle of data retention, they reflect the recommendations of the Council of Europe in 1973 regarding the laying down of specific retention periods. However, they do not reflect later developments of this branch of data retention in Europe. As noted above, parallels may be drawn with Council of Europe Recommendation No. R (81) 155 where the publication of retention periods was required as part of the data-retention principle in relation to specific types of medical data. The merit of requiring publication of retention guidelines and procedures is that this requirement conforms to the principle of transparency of data processing in the eyes of data subjects that is central to data-protection regulation. The omission of publicity and transparency from

---

108. *Supra* note 15, s. 5(2).

109. *Supra* note 17 at p. 375.

110. *Supra* note 16 at p. 267.

111. See Case #52, <http://www.privcom.gc.ca/cf-dc/cf-dc_020613_e.asp>, and Case #255 <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020613_e.asp>, where the Commissioner found that the organizations in question had failed to meet their respective obligations to have retention and deletion policies in place. Case #52 involved a company that had collected data from participants in online contests, while case #255 involved an airport authority. Equally, the Commissioner found that there was no sustainable complaint under section 4.5.2 in relation to case #157, <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_2_e.asp>, where a credit-reporting agency had a six-year retention policy.

112. The strength of the bond between section 4.5 and section 4.5.2 is illustrated in the findings of the Privacy Commissioner in case #216. The airport under investigation had a one-year retention period that applied to audiocassette recordings of runway inspections. To that extent, the airport appeared *prima facie* to have complied with the requirements of section 4.5.2. However, the Commissioner sustained the complaint under both section 4.5 and section 4.5.2 because the airport had lost or destroyed the audiocassette—apparently due to human error—before the expiry of that time period and had therefore not respected its own directive, <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030801_07_e.asp>.

PIPEDA's explicit recommendations in relation to data retention is noteworthy as an additional area in which that act has failed to provide adequate protection for individual rights to privacy in the processing of their personal data. Criticism of the Canadian data-retention principle has also been based on its failure to specify "strict standards" on minimum and maximum retention periods.[113] The criticism of specific retention period setting is well founded as discussed above.[114]

Finally, section 4.5.3 provides that:

> Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

These recommendations appear to be directly influenced by the wording from the Explanatory Memorandum to the *OECD Guidelines* discussed above. The wording of section 4.5.3 is evidence that the Directive was not the only international instrument in this field to influence the form of *PIPEDA*. In the context of prior European legal developments, the inclusion of the alternative of rendering information anonymous is also borrowed from the Convention. The meaning of the term "anonymous" is not expanded upon in *PIPEDA*, and, given the significant number of different interpretations of anonymity[115] in the context of data and the different meanings given to the identification of data subjects under European law, this does not commend itself in terms of legislative clarity.

Further criticism of the Canadian data-retention principle has focused on the incorrect equating of the rendering of information anonymous and the destruction of that data.[116] The criticism of this aspect of *PIPEDA* is, it is submitted, less convincing. The effective rendering of information anonymous such that the information is no longer capable of being identified with an individual is a sound alternative to destruction or erasure of that information. If information is effectively "anonymized," it ceases to be subject to *PIPEDA* as it no longer constitutes "personal information" for the purposes of the legislation.[117]

However, the data-retention principle as implemented in full in *PIPEDA* has been developed beyond the simplicity of the data-retention principle as found in the Directive. In addition, the introduction of "substantially similar" legislation in the provinces of Alberta, British Columbia and Quebec has led to a

---

113. Tina Piper, "The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's 'Technological Society'," (2000) 23 Dal. L.J. 253 at p. 283. Note also that in case #157 the Privacy Commissioner found at para. 10 that *PIPEDA* "did not *presume* to set out specific minimum or maximum periods" [emphasis added], <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_2_e.asp>.

114. In the United Kingdom, a feature of the guidance provided by the UK Information Commissioner on data retention has been a willingness to specify retention periods in relation to specific types of data. See generally Warner, *supra* note 58.

115. These different interpretations include non-perceptibility of the subject, legally relevant anonymity, legally non-relevant anonymity, legally non-relevant identity and legally relevant identity. It is legally relevant and non-relevant identity that seem most suitable for the purposes of application or non-application of data-retention requirements. See M. Van Dellen, "Anonymity on the Internet: What Does the Concept of Anonymity Mean?" (2002) 9(1) EDI L.R. 1 at pp. 1–6.

116. Piper, *supra* note 113 at p. 283.

117. *Supra* note 15, s. 2(1).

growing diversity of forms for the data-retention principle, each of which deserves individual examination.

4.4. Implementation of the data-retention principle in Canada's provincial legislation

With reference to the substantial similarity of extant provincial privacy legislation, it is notable that only three provincial legislatures have enacted laws in this area since *PIPEDA* was enacted. On September 1, 1994, Quebec introduced the *Protection of Personal Information in the Private Sector Act*,[118] which has been approved by the Canadian federal government as being "substantially similar" to *PIPEDA*. In 2003, British Columbia (*Personal Information Protection Act*[119] introduced on October 6, 2003) and Alberta (*Personal Information Protection Act*[120] introduced on December 4, 2003) introduced pieces of legislation that were finally approved by the federal government as being compatible with *PIPEDA* on October 12, 2004.

In relation to data retention, section 12 of the Quebec act states that "once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to the time limit prescribed by law or by a retention schedule established by government."[121] There is a clear parallel with the Quebec approach and the trend among European data-retention laws to focus on restricting the ongoing use of information, rather than its storage or retention. In doing so, the Quebec legislation risks avoidance of the data-retention principle by the passive use, storage or keeping of information unless a broad and potentially misleading interpretation of the term "use" is applied to the legislation.

In British Columbia's *Personal Information Protection Act*, section 35(2) states that:

> An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that:
> (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
> (b) retention is no longer necessary for legal or business purposes.

This broad retention principle is subject to section 35(1) which provides that "if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it."

The British Columbia approach to data retention clearly involves a narrow, document-specific approach. The reference to the destruction of docu-

---

118. *Supra* note 61 R.S.Q. c. P-39.1.
119. S.B.C. 2003, c. 63.
120. S.A. 2003, c. P-6.5.
121. *Ibid.*, s. 12.

ments is difficult to apply to electronic information, where concepts of erasure and deletion are by no means equivalent to destruction. The legislation also revolves around concepts of reasonableness, which were at one time part of European data-retention thinking but which were omitted from the Directive, and of necessity for legal or business purposes. In relation to legal or business purposes, there would appear to be no need to link the purposes for which data retention is permitted with the purposes for which it was collected.[122]

Section 35(1) develops the basic exception under section 4.5.2 of *PIPEDA* that, where personal information has been used to make a decision about an individual, it may be retained for a reasonable period of time.[123] Accordingly, the British Columbia legislature has designated a specific period of one year as a retention period for such information. This undoubtedly provides more clarity than the *PIPEDA* equivalent. However, there is some doubt whether it will be appropriate in all circumstances, particularly where decisions have long-term implications or legal repercussions. In those circumstances, the retention period of one year will be vastly inadequate and potentially fatal to decision-making review and legal claims alike.

In Alberta, the approach taken in the *Personal Information Protection Act* is contained in section 7(1), which provides that:

> Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,
> (a) collect that information unless the individual consents to the collection of that information…
> …
> (c) use that information unless the individual consents to the use of that information, or
> (d) disclose that information unless the individual consents to the disclosure of that information.[124]

Section 35 then provides that "Notwithstanding that a consent has been withdrawn or varied…an organization may for legal or business purposes retain personal information as long as is reasonable."[125] The result is that Alberta's legislation contains no explicit data-retention principle. Data retention in Alberta is something that is implied in connection with data-subject consent or that applies via *PIPEDA* to the extent that Alberta has not introduced "substantially similar" legislation.

Flaherty has commented that:

---

122. *Supra* note 119 at s.35(2). This is addressed in s. 35(2)(a), but the manner in which s. 35(2) is drafted permits retention beyond the period that is reasonably required to serve the purposes for which the data were collected if it remains necessary to retain that data for legal or business purposes.

123. For those versed in the European data-protection model, it is important to note that the decision does not need to be the subject of automated decision-making.

124. *Supra* note 120.

125. *Ibid.*

> The ideal data protection law should strive for as much explicitness as possible in the identification of privacy interests in order to facilitate, guide, and inform the process of limiting surveillance. It is sometimes argued that the changing nature of challenges to privacy discourages such efforts. Yet, at present, there is a core element of well-defined privacy interests that stands the test of time and is not fully susceptible to changes in technology, ideology, age, income, or social developments. The core of privacy interests remains essentially the same in Western nations, while surveillance threats continue to escalate.[126]

It is submitted that among the core of the privacy interests common to the western nations mentioned by Flaherty is the fundamental principle of restricting data retention. Following Flaherty's recommendations, the principle ought to be as explicit as possible. There is an argument that the Directive and the *OECD Guidelines* are not as explicit as they could be in stating the principle of data retention. *PIPEDA*'s provisions concerning data retention are consistent with the data-retention principle under the Directive and the *OECD Guidelines*, and could on that basis be subject to the same criticism. However, *PIPEDA* seeks to avoid that criticism by elaborating on the requirements of data retention under the European model in terms of retention periods, decision-making and the destruction/anonymization of information. However, critics can point to the broad variance among the existing provincial enactments of *PIPEDA*'s data-retention provisions, as described above, which will undermine effective compliance across Canada, and to the inconsistent interpretations among provincial legislatures introducing "substantially similar" legislation in relation to the private sector. This variance and these inconsistencies are, it is submitted, largely the result of the enactment of weak recommendations in *PIPEDA* and of the failure to require provincial legislatures to follow the wording of *PIPEDA* more closely in implementing "substantially similar" legislation.

Given the approach to data retention under the Alberta, British Columbia and Quebec legislation, which have been approved under *PIPEDA*, a failure to incorporate explicit data-retention provisions may not be fatal to any provincial legislation. It is submitted that the Canadian government, in determining whether there is substantial similarity of provincial legislation with *PIPEDA* ought to consider data retention as one of the core principles that provincial legislation must include to protect fully the privacy of Canadian citizens and their personal information. A failure to do so will lead to the piecemeal introduction of inconsistent privacy legislation relative to the private sector across Canada. Such piecemeal inconsistencies among provincial legislation are likely to be significant in the context of any future European Commission review of the protection achieved under

126. David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989) at p. 378.

PIPEDA, particularly given the warning issued by the Working Party in relation to the process used to identify substantially similar legislation.

*

5. CONCLUSIONS

DATA RETENTION HAS BECOME a significant issue for the "Information Society": laws respecting data retention severely restrict the freedom of organizations to hold information about individuals. The development of the legal prohibition on data retention, subject to the balances and limitations necessary in a democratic society, has been tortuous throughout the last thirty years culminating, with the Directive, in a data-retention principle of simplicity and generality. In Canada, data retention under *PIPEDA* has assumed unprecedented significance. It is in this context that this paper has examined the nature and extent of the prohibition on data retention under Canadian law.

The generality of *PIPEDA*'s provisions and the drawbacks associated with the enforcement and oversight mechanisms within that act are also problems which are associated with the data-retention principle under the same. In addition, the limited application of *PIPEDA* to the certain parts of the so-called private sector and the relationship of mutual exclusivity between *PIPEDA* and substantially similar provincial legislation both serve to restrict the potential impact of data retention on data-processing activities in Canada.

Despite these apparent limitations, data retention under *PIPEDA* has the potential to make a significant difference to data-processing expectations among data users and subjects in Canada; the realization of that potential is beginning to bear fruit through some of the Privacy Commissioner's investigations and findings under *PIPEDA*. The act introduces a basic obligation on data users that personal information shall be retained only for as long as is necessary for the fulfilment of specified purposes, and goes further to recommend "best practices" for data users. In doing so, *PIPEDA* has stated data retention in a more explicit form than has the Directive. In addition, the introduction of allegedly "substantially similar" legislation in the provinces of Alberta, British Columbia and Quebec has led to a growing diversity of forms of the data-retention principle which threatens to undermine the existing favourable status enjoyed by the federal legislation under European data-protection law. Whereas the basic data-retention principle in *PIPEDA* conforms to the Directive's provisions, the development of provincial legislation which is inconsistent with the federal approach has the potential to threaten the favourable status of the federal act under European data-protection law.

The Directive was not the only possible influence on the form of data-retention principle under *PIPEDA*. In fact, there is some merit in the argument that the competing influences of the United States's privacy developments and of other international commitments—primarily the *OECD Guidelines* and the *UN Guidelines*—also had an effect on *PIPEDA*'s provisions. In particular, a comparison of *PIPEDA*'s provisions and the *OECD Guidelines* demonstrates that both instruments share common approaches to retention periods and to the retention of decision-making information as well as to the provision of guidance on

destruction/anonymization of information. However, none of these international developments make data retention an explicit and fundamental principle of data processing in the way that the Directive and *PIPEDA* approach data retention.

The origins of the principle of data retention—namely the Council of Europe recommendations culminating in the Convention—provide a meaningful insight into the issues and challenges that are likely to shape the development of *PIPEDA* and of provincial legislation on data retention. In particular, the formal declaration from the Council of Europe that individuals need to be protected from the harm that could result from the retention of data for unreasonable lengths of time confirms the solid basis for new data-retention rules in Canada. The Convention and the recommendations of the Council of Europe that immediately followed it share many characteristics with *PIPEDA* and with the provincial legislation enacted under it. It is notable that attempts of the Council of Europe to expand the basic principle of data retention were not included in the Directive. This historical analysis suggests that data retention as set out in the Directive is likely to generate greater consistency in application and greater flexibility for organizations complying with the law than attempts to expand the principle.

The data-retention principle under *PIPEDA* includes many of the frailties of the European approach to data retention, which is unsurprising given the influence that European data-protection law has had on current data-protection law in Canada under *PIPEDA*. In refining the European approach to data retention, the Directive clearly reveals a trend away from expanded guidance on retention periods and justifications for retaining data. Learning from European experience is an effective way for Canadian legislators to fast-track the development of law on data retention. To that extent, it is submitted that Canadian laws on data retention should be streamlined to provide a no-frills, clear and simple core principle