25. ANONYMITY AND THE LAW IN CANADA

CAROLE LUCOCK AND KATIE BLACK

I. INTRODUCTION

Anonymity can be understood as not being named or identified or as not having identity connected with certain pieces of information. Anonymity thus broadly covers the "availability or unavailability of various kinds of information that may be known or identified about persons"[1] and includes the ability of others to reveal identity.

In Canada, there is no general right to anonymity. Rather, the law focuses on the circumstances and conditions under which a person's identity may or must be revealed or hidden from view. As such, this chapter discusses limited, rather complete, anonymity and examines the contexts and conditions under which the law supports a person not being named or known.

Although anonymity is often associated with the right to privacy, this chapter distinguishes anonymity from privacy. It only touches on privacy principles when they are directly relevant to the discussion of anonymity in Canadian law. As it relates to privacy, anonymity is often viewed as a mechanism for enhancing privacy.

1. G. Marx, "What's in a Name? Some Reflections on the Sociology of Anonymity," *The Information Society* 99, 15:2 (1999): 19.

Canada's legal system is jurisdictionally complex due to its operation within Canada's federated landscape. Legislative power is constitutionally divided between the federal government and ten provincial governments.[2] Given this complexity, we provide a cursory overview of Canadian laws pertaining to anonymity citing jurisdictional legislation and case law as examples. In general, we have tried to capture newer legal developments to illustrate that social and technological changes have had an impact on anonymity and its support in law. Some instances reveal that there has been an erosion of what would have been de facto anonymity, for example, unrecorded transactions, travel, or presence in a public space. Other instances demonstrate there has been a greater willingness to shield identity, for example, the identity of parties and witnesses in criminal and civil law suits, the requirement of the anonymization of data to be used for research purposes, and the disclosure of identity in access to information requests.

II. CONSTITUTIONAL PROVISIONS

A. Knowledge of Citizens Contemplated: Vital Statistics, Citizenship and Census

Canada's founding constitutional documents, the Constitution Act of 1867[3] and the Charter of Rights and Freedoms,[4] clearly permit and arguably require some state knowledge of citizens and noncitizens within Canadian jurisdiction. As such, the constitution cannot be said to have contemplated or provided for complete state-related anonymity.[5]

The Constitution Act divides the powers of citizen knowledge and information collection between the provincial and federal governments. The power and responsibility for citizenship[6] and census[7] taking rests with the federal government. The provinces have control over other primary registration systems (such as birth registrations), other vital statistics, as well as mandatory personal naming systems.[8]

2. The Constitution Act, 1867 (U.K.), 30 & 31 Victoria, c. 3, ss 91 & 92. Note that Canada also has three territories that constitutionally are under the jurisdiction of the federal government but in practice have powers akin to those of the provinces. The governance of specific areas of activity can be complicated and involve both levels of government. Legislation relating to the protection of privacy (with an indirect impact on the topic of anonymity) in the private sector is a good illustration of this.

3. *Ibid.*

4. The Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11, Part I, The Canadian Charter of Rights and Freedoms.

5. Library and Archives Canada, Canadian Genealogy Centre, "Civil Registration," http://www.collectionscanada.gc.ca/genealogy/022-906.006-e.html; and Statistics Canada, "History of the Census of Canada," http://www.statcan.ca/english/census96/history.htm.

6. Constitution Act s 91(25) (n. 2).

7. *Ibid.* s 8, s 51, s 91(6).

8. *Ibid.* s 92(13), (16).

Requirements for these registration systems dovetail as the provincial birth certificate is typically used to confirm identity and rights for "most government documents and services, including health cards, drivers' licences, passports and social benefits."[9]

B. Charter of Rights and Freedoms: Limited Anonymity Related to Constitutional Rights

The Charter guarantees specified rights and freedoms by preventing all levels of government from placing limits on the enumerated rights and freedoms unless such limits can be demonstrably justified in a free and democratic society.[10] Although the Charter does not address anonymity directly, a number of sections are indirectly concerned with protecting it in certain circumstances. With the exception of provisions related to the criminal law, addressed in section 3, these sections are canvassed below.

Section 2(b): The Protection of Freedom of Expression Including Freedom of the Press[11] Although freedom of expression has been recognized by the courts as an important democratic right,[12] the role of anonymity in facilitating the exercise of this right has not been established. Indeed, the lower court in *Harper v. Canada*,[13] the one case that expressly considered whether anonymity is a value protected by s.2 (b) of the Charter, limited its findings to attribution requirements for third party advertisers in election advertising finding that "while this argument should not be foreclosed upon . . . s. 2(b) does not guarantee anonymity for third party advertisers or contributors in the circumstances of this case. Elections in general, and specifically election financing, are highly regulated activities and third parties can have no expectations of anonymity."[14] The court noted that "the concerns for public information outweigh citizens' ability to participate."[15] In finding against a right to anonymous political advertising, the court notably confined the decision to the facts of this case and additionally implied that a right to Charter protection of anonymous speech might be found at a later date,[16] as anonymity may either curtail or enhance the right to freedom of expression depending on the nature

9. For example, in order to obtain a passport, see Passport Canada, "Proof of Canadian Citizenship," http://www.ppt.gc.ca/cdn/section4.aspx?lang=eng.

10. Charter s.1 (n. 4). See also *R. v Oakes* [1986] 1 S.C.R. 103.

11. *Ibid*. Charter s 2(b), which provides that everyone has the fundamental freedoms of thought, belief, opinion, and expression, including freedom of the press and other media of communication.

12. See, for example, *R. v Keegstra* [1990] 3 S.C.R. 697at 763–764; and *Edmonton Journal v Alberta (Attorney General)* [1989] 2 S.C.R. 1326 at 1336.

13. *Harper v Canada (Attorney General)* [2001] A.J. No. 808 (Q.B).

14. *Ibid*. para. 186.

15. *Ibid*. para. 109.

16. *Ibid*. para. 186, where Justice Cairns' intimates that s.2(b) of the Charter might protect some privacy or anonymity rights.

of the circumstances. On appeal of this decision, and despite not addressing the issue of anonymity, the Supreme Court of Canada finds that overriding considerations of trust in the integrity of the electoral system, election fairness, and transparency are sufficiently important to justify the infringement of freedom of expression in the case of third-party advertising.[17]

One circumstance in which the salutary effects of anonymity can be seen is the expression of otherwise unpopular or socially repressed ideas.[18] Although American jurisprudence has provided robust protections for this type of anonymous expression, Canadian courts have not followed suit. To date, our courts have not acknowledged that anonymous speech may, in some instances, be essential to the exercise of freedom of expression.

In relation to the freedom of the press, jurisprudence engaging the role of anonymity clearly tends to focus on its deleterious ability to stifle transparency in the judicial process. In both the civil and criminal contexts,[19] many such cases concern the need for openness of the courts. Often at the behest of the press, attempts to curtail this transparency by granting limited anonymity to parties or witnesses are interrogated. Anonymity in the judicial process has thus been limited to very specific circumstances, including protecting the vulnerable and promoting the prosecution of claims and crimes.

Section 7: Right to Life, Liberty and Security of the Person[20] Section 7 of the Charter of Rights and Freedoms has been found to contain and protect a right to privacy.[21] This finding, however, has primarily been limited to the criminal law context (which is discussed below). Beyond this, there are some cases that recognize section 7 as protecting a right not to be identified or the right to limited anonymity as a component of the right to privacy.[22] *Cheskes*[23] exemplifies this protection. The case involved a recent challenge to new Ontario adoption legislation retroactively and nonconsensually disavowing birth parents and adoptees of their anonymity by opening the adoption record. The court found that the retroactive provisions infringed upon section 7 and were therefore of no force and effect, suggesting that section 7 protects anonymity, as incorporated in a right to privacy, beyond the criminal law context. As such *Cheskes* opens up section 7 anonymity protections and contextualizes the earlier limits placed on them in

17. *Harper v Canada (Attorney General)* [2004] 1 S.C.R. 827 at paras 136–139 and 142–146.

18. See, for example, C. Keen, "Anonymity and the Supreme Court's Model of Expression: How Should Anonymity be Analysed Under Section 2(b) of the Charter," *Canadian Journal of Law and Technology* 23, 2:3 (2003): 1671.

19. See sections III.A and IV.A.

20. S. 7 provides that "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof in accordance with the principles of fundamental justice."

21. *R. v O'Conner* [1995] 4 S.C.R. 41.

22. See *Cheskes v Ontario Attorney General* [2007] 87 O.R. (3d) 581 (S.C.)

23. *Ibid.*

Canadian AIDS Society v. Ontario.[24] In this case, public health legislation that required the reporting of blood donors' HIV seropositive status was challenged, specifically when blood samples taken before the HIV/AIDS test was available were retested. Here, the court found that the donors' section 7 right to security of the person was infringed. The legislative measures were upheld, however, because they accorded with the principles of fundamental justice due to the overriding public health considerations and public health officials' requirements to maintain reported information in confidence.

Section 3: Right to Vote[25] The Canada Elections Act[26] and provincial election acts, such as Ontario's Election Act,[27] recognize the role that anonymity plays in ensuring meaningful and free participation in the elections process. They have incorporated a number of provisions that deal with identification during the registration process, proof of elector identification when obtaining ballots at polling stations, anonymity in the actual voting process to ensure the secrecy of a person's vote, disclosure of campaign contributions, and disclosure of campaign advertising.[28]

Although voting eligibility requirements have always mandated that voters demonstrate their identity by providing their name and address in exchange for a ballot, for example, the new federal Canada Elections Act requires voters to provide physical identification at polling stations.[29] Voters are not, however, required to produce photo ID, and there are mechanisms to allow persons who are unwilling to show their faces to demonstrate their identities.[30]

Once elector identity has been confirmed, the Canada Elections Act ensures voting anonymity. The vote is to be secret[31] as a rule of absolute public policy that cannot be waived.[32] The identity of the elector can no longer be ascertained after the ballot has been provided to them.[33] Moreover, the Act obligates all in attendance at a polling station or at the counting of votes to maintain this secrecy.

---

24. (1995), 25 O.R. (3d) 388 (Gen. Div).); affirmed (1996), 31 O.R. (3d) 796 (C.A.).

25. Section 3 provides that "Every Citizen of Canada has the right to vote in an election of members of the House of Commons or of a legislative assembly and to be qualifies for membership therein."

26. Canada Elections Act SC 2007, c. 21.

27. Election Act RSA 2000 c. 9 s. 6.

28. Also see *Harper* (n. 17), which upholds the constitutionality of the latter two.

29. Canada Elections s 143(1) (n. 26) and clarified by The Chief Electoral Officer to include one piece of government issued photo ID containing name and address, two pieces of ID containing name and address, or to have another eligible voter vouch for a person's identity. Press Release, Elections Canada, http://www.elections.ca/content.asp?section=med&dir=spe&document=sep1007&lang=e&textonly_false.

30. *Ibid.*

31. *Ibid.* s 163.

32. *Walsh v Montage* [1888] 15 S.C.R. 495 (S.C.C.).

33. Canada Elections s 144.1 (n. 26).

Only an elector requiring assistance may reveal his or her vote to another.[34] This right to secrecy is also mirrored within provincial election legislation.[35]

III. CRIMINAL LAW

Anonymity is engaged throughout the criminal justice system. It concerns the concealment or disclosure of identity as well as methods and techniques of investigation, surveillance, and evidence gathering of such things as fingerprints or DNA.

A. Disclosing and Concealing Identity

General Requirement for Identification There is no general requirement that persons carry identification or identify themselves to law enforcement officers.[36] When law enforcement authorities have no reasonable grounds to detain or arrest an individual, that individual is provided a limited degree of anonymity by common-law principles and Charter guarantees of the right to be free from arbitrary detention[37] and the right to remain silent.[38] No law, however, prevents law enforcement officers from stopping people to ask questions. Courts have upheld the brief detention of people by officers as lawful for investigative purposes in a crime under investigation.[39] Reasonable grounds for the detention based on a reasonable suspicion of involvement must exist in such cases. Even though persons are not *required* to identify themselves when detained, there is nothing to prevent them from volunteering this information when questioned by law enforcement personnel.[40] Although refusing to answer such questions will not constitute a charge of obstructing justice, the provision of a false identity will.[41] If a person feels compelled to provide identifying information because of the circumstances of their physical or psychological detention, the use of obtained identifying information may be considered a Charter infringement of the right to be free from unreasonable search and seizure.[42] This is especially so if the identifying information is used to search law enforcement databases.

---

34. *Ibid.* S. 164(1)–(2).
35. For example, *Elections Act*, R.S.A., 2000, c. E-1, s. 93.
36. *R. v Mann* [2004] 3 S.C.R. 59, see also, *R. v Legault* [1998] 54 C.R.R. (2d) 155 and *R. v Greaves*, [2004] 189 C.C.C (3d) 305 (BCCA).
37. Charter s 9 (n. 4).
38. *Ibid.* S 7 has been held by the courts to contain the right to remain silent. See, for example, *R. v Hebert* [1990] 2 S.C.R. 151 (SCC).
39. *Mann* at para 17 (n. 36).
40. *Greaves* at 47–48 (n. 36).
41. *Ibid.* at 49–51.
42. *R. v Harris* [2007] 87 O.R. (3d) 214 (On CA).

Nonetheless, this sphere of limited anonymity is very restricted. It does not apply once a person has been charged with an offence[43] or arrested,[44] or when there is a legal duty to identify oneself—for example, as exists in the Highway Traffic Acts.[45] Proposals to introduce a National Identification Card threaten to further restrict, if not obliterate, the limited anonymity currently enjoyed in Canada.[46]

Concealing Identity: Informants, the Accused, and Witnesses In the judicial process, the concealment of identity generally arises during criminal trials. It may relate to disclosing all information to the accused for the purposes of making a full defense or the placement of publication bans on the names of the accused, victims, or witnesses. Generally, when bans are issued, the person is known under a pseudonym in publications and in reported legal decisions of the case.

Informants There is a long-standing common-law rule preventing the disclosure of police informants' identities on the grounds that it is important for people to assist the police without fear of retaliation.[47] Informer privilege has been extended to more recent programs such as "Crime Stoppers." This program encourages people to report potential crimes to the police on the understanding that their identities will be concealed.[48] Informer privilege is not absolute, and identity may be revealed in certain limited circumstances relating to trial fairness and the rights of the accused.[49] Even here, there is a preference for providing nonidentifying information to the accused.[50]

The Accused Generally, the identity of the accused is not concealed or subject to publication restrictions. This adheres to the general policy of court openness prevalent in the Canadian criminal justice system. Young offenders represent an exception to this general rule. In most cases, the Youth Criminal Justice Act[51] prohibits the publication of the identity of a child[52] or young person[53]

---

43. *R. v Beare* [1988] 2 S.C.R. 387.

44. *Moore v The Queen* [1978] 43 CCC (2d) 83 (SCC). See also Criminal Code, R.S.C. 1985, c. C-46 s 495(2)(d)(i).

45. For example, Highway Traffic Act RSO 1990, c H.8, s 33, s 104.1(4)) and s 218.

46. See, Privacy Commissioner of Canada, "Appendix A: The National Identity Card Debate" in *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues* (Ottawa: Privacy Commissioner of Canada, September 2007), http://www.privcom.gc.ca/information/pub/ID_Paper_e.asp.

47. *R. v Leipert* [1997] 1 S.C.R. 281.

48. *Ibid.*

49. *R. v Scott* [1990] 3 S.C.R. 979, see also, *R. v Rodney Appleby* (2006), [2007] 263 Nfld. & P.E.I.R. 262.

50. *Scott* (n. 52) per Cory, J.

51. S.C. 2002, c 1.

52. A person who is or appears to be less than 12. *Ibid.* s 2(1).

53. A person who is or appears to be older than 12 but younger than 18. *Ibid.* s 2(1).

accused of a crime.[54] Exceptions to this general prohibition concern treating the accused as an adult for the purposes of the Act,[55] disclosure of identity for the purposes of the administration of justice,[56] disclosure of identity when required to apprehend the young person or if the young person is a danger to others,[57] and at the request of the person to whom the disclosure prohibition applies.[58]

A more limited exception exists to protect the reputation of the accused when there is some doubt about the laying of charges and the accused's reputation in a small community may be severely damaged as a result of the charges.[59]

Witnesses The strong presumption of open courts, supported by the Charter protection of freedom of the press, generally requires the identity of witnesses to be known and subject to publication. However, their identities may be concealed for a variety of policy reasons.[60] Crimes such as extortion or sexual offences may go unprosecuted or become underreported if victims are not permitted to conceal their identity.[61] The identity of child and youth victims and witnesses are concealed under both the Criminal Code[62] and the Youth Criminal Justice Act.[63] Police informants, undercover operatives, and persons subject to witness protection schemes[64] may be harmed if their identities become known. Consequently, publication bans will often be granted in these cases.[65]

---

54. *Ibid.* s 110.

55. *Ibid.* s 110(2)(a) and (b).

56. *Ibid.* s 110(2(c).

57. *Ibid.* s 110(4).

58. *Ibid.* s 110 (3) and (6).

59. *In the matter of an application by an unnamed person for an Order banning the publication of his name* [2005] 249 Nfld. & P.E.I.R. 233 citing as authority for permitting the ban *Dagenais v Canadian Broadcasting Corporation* [1994] 3 S.C.R. 835 at paras 87–88, which recognized the privacy of the accused and his or her family as a factor to consider in granting a publication ban.

60. *Ibid. Dagenais*, which articulates the factors to be taken into consideration when considering whether to grant a publication ban; *A.G. (Nova Scotia) v MacIntyre* [1982] 1 S.C.R. 175 (protecting the innocent), *R. v O.N.E*, 2001 SCC 77 and *R. v Mentuck*, 2001 SCC 76 (proper administration of justice and protection from harm). S 486.5(1) of the Criminal Code (n. 44) encapsulates much of the common law with respect to whether to grant a publication ban in the interests of the proper administration of justice.

61. Criminal Code s. 486.4(1) (n. 44) lists a number of offences where a nonpublication order may be issued. Generally, the issuing of an order is discretionary; however, s 486.4(2) provides that a complainant must be informed of this section and non-publication order *must* be issued if an application is made. See also *Canadian Newspapers Co. v Canada (Attorney General)* [1988] 2 S.C.R. 122 and *R. v Seaboyer* [1991] 2 S.C.R. 577.

62. *Ibid.* Criminal Code s. 486.4(2).

63. Youth Criminal Justice s 111.(1) (n. 51).

64. Witness Protection Program Act, S.C. 1996 c.15.

65. *O.N.E.* and *Mentuck* (n. 60).

B. Investigation, Surveillance, and Evidence Gathering

Reasonable Expectation of Privacy Section 8 of the Charter[66] guarantees the right to be free from unreasonable search or seizure and has thus been used to determine the constitutionality of law enforcement methods of investigation and evidence gathering. The Supreme Court of Canada, in *R. v. Dyment*, [67] articulated what is of concern and why, as follows: "The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state."[68] Anonymity is here engaged more in the sense of being left alone by the state and not having information collected and known, rather than identity being revealed per se.

The threshold question for engaging the protections accorded by section 8 is whether, in the circumstances, a person has a reasonable expectation of privacy. If not, then a search is considered to have not occurred for constitutional purposes; section 8 remains unengaged.[69] Many of the cases consequently center around whether there was a reasonable expectation of privacy in the context of specific state activity. If a search is found to have taken place, thereby engaging section 8, the specific activity is scrutinized by asking: was the activity authorized by law and is that law reasonable? For the most part, courts expect to see judicial authorization (generally a warrant) for the activity.

Some authorization requirements are found in legislation. The Criminal Code, for example, contains a general provision concerning the need for a warrant in certain circumstances[70] as well as specific reference to such things as the interception of private communications[71] and the use of video surveillance.[72] General provisions for the warrant state that it is necessary when the activity would constitute an unreasonable search and seizure if not authorized.[73] This implies the necessity of a warrant when there is a reasonable expectation of privacy.

As noted, a key question in the jurisprudence is whether, in the circumstances, there is a reasonable expectation of privacy. The 2004 *Tessling*[74] case summarizes the law in this regard as well as the impact of the use of newer methods of surveillance on the reasonable expectation of privacy. In synthesizing the law, the court notes three realms of privacy subject to a reasonable expectation: personal, territorial, and informational.[75] Personal privacy is accorded the greatest protection.[76]

66. Charter (n. 4).
67. [1988] 2 S.C.R. 417.
68. *Ibid.* Para 17.
69. *R. v Tessling*, [2004] 3 S.C.R. 432 at para 18.
70. Criminal Code s.487.01 (n. 44).
71. *Ibid.* s.184.
72. *Ibid.* s.487.01(4).
73. *Ibid.* s. 487.01(1).
74. *Tessling* (n. 69).
75. *Ibid.* Para 20.
76. *Ibid.* Para 21.

Territorial privacy, especially as it relates to the home or dwelling place, is also given a high degree of protection.[77] Informational privacy is accorded the lowest degree of protection, and authorization for its collection is only required with respect to a "biographical core of personal information."[78] This core includes "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[79]

In many instances, a reasonable expectation of privacy may not be found as a consequence of the privacy hierarchy and judicial authorization will not be required, especially if the context is characterized as concerning informational privacy. These contexts include information that is in public view, information that has been abandoned, and information that is not subject to customer confidentiality (for example, electricity records).[80] In *Tessling*, it included images of heat emanating from a building captured by a forward-looking infrared camera installed in a plane that flew over the building. To determine whether a reasonable expectation of privacy existed, the *Tessling* court looked at the "totality of the circumstances" taking into account subjective expectations of privacy and whether these are objectively reasonable.[81] The Supreme Court stated that technology should be considered in light of its current capabilities and noted that advances in surveillance capabilities and the diminished subjective expectation of privacy that might ensue should not lower the constitutional protection given. Simply put, Binnie J. wrote "expectation of privacy is a normative rather than a descriptive standard."[82]

Somewhat contentious are the spaces that may entail some, albeit a diminished, expectation of privacy. For example, schools,[83] lockers in bus stations,[84] hotel rooms,[85] airports, and motor vehicles.[86] The law continues to develop as to the standards of search which they require. Two recent cases concerning the permitted uses of sniffer dogs to detect illegal drugs have destabilized the law to some degree because the Supreme Court was divided on a number of points, in

77. *Ibid.* Para 22, which recognizes privacy interests in a number of places beyond the home including places of work, private cars, and prisons.

78. *Ibid.* Para 25 citing *R. v Plant* [1993] 3 S.C.R. 281. A recent Supreme Court decision has clarified that if information fails to meet the 'core biographical' test it will not necessarily be without protection, citing wire tapping as an example. See *R. v A.M.*, 2008 SCC 19 at para 68.

79. *Tessling* para 25 (n. 69).

80. *Plant* (n. 78).

81. *Tessling* paras 34–62 (n. 69).

82. *Ibid.* para 42.

83. *R. v M. (M.R.)* [1998] 3 S.C.R. 393 and *R. v. A.M* (n. 78).

84. *R. v Buhay* [2003] 1 S.C.R. 631.

85. *Ibid.*, at para 22.

86. *R. v Wise* [1992] 1 S.C.R. 527.

particular, whether or not there was a reasonable expectation of privacy in the circumstances and the standard to be used to allow sniffer dogs to investigate.[87]

Biometric Banks The collection and use of fingerprints and DNA foreclose anonymity in cases in which this information has been added to databases that are made available for law enforcement purposes. Indeed, courts have accepted that persons convicted of designated, serious offences lose their expectation of privacy and anonymity. The Supreme Court in *Rogers* wrote "can persons convicted of designated offences . . . reasonably expect to retain any degree of anonymity *vis-à-vis* law enforcement authorities after their conviction?"[88] The court concluded that "a person convicted of a designated offence would reasonably expect the authorities to gather and retain identifying information, such as fingerprints, distinctive body markings, or eye color. The bodily sample here is simply another form of identification." Mr. Rodgers consequently lost

> any reasonable expectation of privacy in the *identifying information* derived from DNA sampling in the same way as he . . . lost any expectation of privacy in his fingerprints, photograph or any other identifying measure taken under the authority of the Identification of Criminals Act.[89]

The collection and use of fingerprint information for identification purposes has long been accepted in common law and more recently held to be constitutional[90] along with the collection and use of DNA for similar purposes.[91] Legislation, such as the Identification of Criminals Act[92] (dealing with fingerprints and photographs) and the DNA Identification Act,[93] provides for the collection of information and its use. Generally, collection is only permitted in connection with serious offenses, and use is restricted to the purpose of identification. The constitutionality of the DNA Identification Act and provisions in the Criminal Code relating to the collection of DNA has been upheld, in part, on the basis that the use of DNA information is restricted to identification and that the collection of DNA information generally occurs under judicial authorization.[94]

Addressing Newer Technologies Anonymity may be enhanced by the use of new technologies, particularly in an electronic or online environment. This is of particular concern to law enforcement and national security agencies seeking to ensure that a link is maintained between individuals and their activities.

---

87. *R. v Kang-Brown*, 2008 SCC 18 and *R. v. A.M* (n. 78).

88. *R. v Rodgers* [2006] 1 S.C.R. 554 at para 43. See also, *R. v. S.A.B.*, [2003] 2 S.C.R. 678, 2003 SCC 60.

89. *Ibid. Rogers.*

90. *Beare* (n. 43). See also The Identification of Criminal Act, RSC 1985, c. I–1.

91. *Rogers* (n. 88).

92. R.S.C. 1985, c. I–1.

93. S.C. 1998, c. 37. See also Criminal Code ss 487.04–487.092 (n. 44).

94. *Rogers* (n. 88).

For a number of years, the federal government has attempted to introduce legislation that would require telecommunications service providers, such as cell phone and Internet service companies, to provide identifying information under certain terms and conditions.[95] These legislative initiatives are ongoing[96] and may result in legislative change. Questions remain regarding the necessity of the change,[97] the sufficiency of existing law enforcement access to identifying information, and if change is required, the nature of the judicial oversight and grounds for authorizing the provision of identity information.

Encryption technologies, although helpful in enabling secure online interactions, communications, and anonymity, also pose a challenge to law enforcement and security agencies. At present, there are few legal controls concerning the use of encryption technologies.[98] This may change, however, due to growing opposition mounted by government agencies to their unregulated employment and development. The main concern raised involves the ability of encryption to frustrate counterterrorism and law enforcement initiatives by impeding law enforcement access to information.

In October 1998, Industry Minister John Manley confirmed that Canada's Cryptography Policy established Canadians' freedom "to develop, import and use whatever cryptography products they wish."[99] Concurrently, he also committed the government to "[giving] law enforcement agencies and national security agencies the legal framework they need to ensure public safety." [100] This included "making it an offence to wrongfully disclose private encryption key information and to use cryptography to commit or hide evidence of a crime."[101] He continued,

95. Proposed legislation has been hotly contended by privacy and civil liberties groups. See Canadian Internet and Public Policy Clinic, *Lawful Access* (updated June 2, 2007), http://www.cippic.ca/projects-cases-lawful-access/ for a discussion of the history and links to relevant information.

96. In the fall of 2007 a consultation paper was released by Public Safety Canada and Industry Canada; see Public Safety Canada, *Customer Name and Address Information Consultation*, http://securitepublique.gc.ca/prg/ns/cna-en.asp.

97. For example, Criminal Code s. 430(1.1) (n. 44) creates the offence of mischief for willfully obstructing, interfering, or denying access to data to any person who is entitled to it.

98. For example, the Export and Import Permits Act, R.S.C. 1985, c-E–19, and the United Nations Act, R.S.C. 1985, c.U–2 limit the export of technologies such as methods of encryption to a limited number of countries and groups and were implemented to minimize the threat that such technologies would be used against Canada in conflict. The Security of Information Act, R.S.C. 1985, c. O–5, s.1; 2001, c.41, s.25; (updated by the Anti-terrorism Act, R.S.C. 1985, c.O–5, s.1; 2001, c.41, s.25) makes the possession of any "device, apparatus or software useful for concealing the content of information or for surreptitiously communicating, obtaining or retaining information," enumerated in the act, an offence ss.22(1)(e).

99. Industry Canada, Canada's Cryptography Policy (October 1, 1998), http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00119e.html.

100. *Ibid*., policy, 6th point.

101. *Ibid.*

"we also need to make it clear that warrants and assistance orders also apply to situations where encryption is encountered—to obtain the decrypted material or decryption keys."[102]

IV. PRIVATE LAW

A. Legal Proceedings

Parties and Witnesses As with criminal law, legal proceedings in court are generally open, parties and witnesses are known, and their identities are subject to publication. Children and youth involved in child protection or adoption proceedings,[103] the innocent in need of protection,[104] and those who may be subject to harm[105] present the main exceptions to this general rule. A gray area concerns when the likelihood of suffering embarrassment, shame, or humiliation will suffice to tip the scales in favor of permitting the concealing of identity. By and large, courts are reluctant to allow these as grounds for shielding identity; yet, exceptions have been made for some plaintiffs, letting them proceed under a pseudonym.[106]

Traditionally, courts have shown a reluctance to permit the shielding of identity on a simple claim of privacy. This may be changing, however, especially in circumstances in which the plaintiffs wish to uphold a previously established pseudonym. A recent case suggests that pseudonyms will be upheld in cases in which identity was already shielded behind a pseudonym prior to the civil action; at issue (in part) was the revelation of the identities of individuals using pseudonyms during peer-to-peer music file sharing.[107]

Although courts clearly favor openness and disclosure of identity, this is not the case for all decision-making bodies. For example, the federal private sector

---

102. *Ibid.*

103. These provisions are generally specified in legislation. See, for example, The Child and Family Services Act, RSO, 1990 c. C11 s 45.

104. *A.G. (Nova Scotia) v MacIntyre* [1982] 1 S.C.R. 175 at pp. 186–187. This exception usually applies to children; however, in *T.H. v C.D.G (*Man QB 1997), 7 W.W.R. 318, 120 Man. R. (2d) 11, a case of alleged sexual abuse by clergy, the alleged perpetrator, and institution were permitted to proceed under a pseudonym.

105. Concealing identity because harm may ensue is more common in criminal cases; however, discrimination may be considered a sufficiently compelling ground to permit pseudonym use. For example in cases concerning HIV/AIDs, see *A.(J.) v Canada Life Assurance Co.* (Ont HCJ 1989), 66 O.R. (2d) 736.

106. See, *T. (S.) v Stubbs* (Ont Gen Div 1998), 38 O.R. (3d) 788 and *B. (A.) v Stubbs* (Ont Gen Div 1999), 44 O.R. (3d) 391, where, based on similar facts (a penis enlargement operation that did not go well) different decisions were rendered concerning permitting the use of a pseudonym.

107. *BMG Canada Inc. v John Doe* [2004] 3 F.C.R. 241, affirmed in result but, in some instances, on different grounds [2005] 4 F.C.R. 81 (CA).

privacy legislation contemplates an ombudsperson approach to dispute resolution, which includes the publishing of case summaries without the names of parties.[108]

Revealing the Identity of Potential Defendants The identity of potential defendants may be known by third parties but not by the party seeking to pursue a claim. Before the widespread use of pseudonyms in the online environment, legal tests had been developed to determine when such third parties would be required to divulge identity. With the expanded use of pseudonyms, and the relative anonymity they provide, there have been a number of cases that have addressed the conditions under which third parties such as Internet service providers (ISPs) will be compelled to reveal identity. Outlining the legal test for this purpose, the case of *BMG*[109] requires first that a bona fide claim be made out and, second, that factors mitigating in favor of and against disclosure be considered. The ability to pursue the claim is the chief factor in favor of disclosure. Factors mitigating against disclosure are less clear but center on a number of interests including privacy, competing public-interest considerations (such as freedom of speech), and the nature of the relationship between the party whose identity has been concealed and the identity of the revealing party. In refusing to permit disclosure, the court in *BMG* took into consideration the lack of reliability of the information linking identity to pseudonym, the implied desire for privacy as a result of pseudonym use, and the contractual agreement of privacy between the user and the ISP.

B. Anonymous Transactions

In theory, many transactions, including contracts, can be executed anonymously, especially if these are simple transactions requiring a single instance of mutual exchange, such as the purchase of a product or service for cash. The scope for anonymity is limited in practice. Contracts contemplating an ongoing relationship that are reduced to writing require identity information of the parties.[110] Simple exchanges often use cash substitutes such as credit or debit cards, which could be used to track the identity of a person. Vendors of various goods and services collect identity information for a variety of purposes including advertising and customer service. The return or exchange of a product may require the provision of identity information if a refund is to be provided. The provision of specific services may entail the provision of identity information. Provided that the collection of identity information is considered reasonable in the circumstances, it will not be in contravention of private sector privacy legislation restricting the collection of personal information.[111]

---

108. Personal Information Protection and Electronic Documents Act, S.C. 2000 c 5 (PIPEDA).

109. *BMG* (n. 107). See also *Irwin Toy v Doe* (Ont SCJ 2000), 12 C.P.C. (5th) 103).

110. For example, the Statute of Frauds, R.S.O. 1990, c S19 requires that certain types of contracts be reduced to writing and signed by the parties.

111. For example, Privacy Commissioner of Canada, PIPEDA case summaries # 361 (refund or exchange of goods), #288 (provision of cell phone services), and #280 (preventing signal theft).

In addition to the collection of identity information being considered reasonable and therefore permissible under private sector privacy legislation and the requirements of the heavily regulated financial and securities sectors, other legislation, such as the Pawn Brokers Act[112] and the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations,[113] may expressly require the collection of identity information before transactions are permitted.

Identity is also connected to signature in the electronic environment, where legislation enabling the use of electronic signatures also contemplates a link to identity information.[114] In such environments, where there is an increased opportunity for the collection and use of identity information and therefore fewer opportunities for anonymity, the Privacy Commissioner of Canada has called for making the right to anonymity the norm.[115]

C. Surveillance

The Personal Information Protection and Electronic Documents Act[116] and companion provincial private sector privacy legislation[117] govern the collection and use of personal information in the private sector, including the collection of information using surveillance technologies. The use of technologies such as video surveillance is generally not prohibited. However, guidelines produced by the Office of the Privacy Commissioner of Canada[118] as well as findings related to surveillance[119] indicate, among other things, that the use of such technology will be reasonable (and hence lawful) if:

1. There is a compelling reason engage in surveillance[120]
2. It is deployed only if less privacy-invasive measures are inadequate
3. Surveillance is not used in highly private areas such as washrooms
4. Notice of the deployment of surveillance cameras is given

---

112. For example, Pawnbrokers Act RSO 1990 c P.6 s 9.

113. Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, S.C. 2000, c 17, s 6.1, S.O.R. 202–184 s 53.

114. PIPEDA (n. 108).

115. Privacy Commissioner, Identity, Privacy at 16–17 (n. 46).

116. PIPEDA (n. 108).

117. Alberta, British Columbia, and Quebec have private-sector privacy legislation that has been found to be substantially similar to PIPEDA. See Privacy Commissioner of Canada, "Substantially Similar Provincial Legislation," http://www.privcom.gc.ca/legislation/ss_index_e.asp.

118. Office of the Privacy Commissioner of Canada, *Guidelines for Overt Video Surveillance* (Office of the Privacy Commissioner of Canada: Ottawa, 2008), http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_e.asp.

119. *Eastmond v Canadian Pacific Railway*, (2004), 16 Admin. L.R. (4th) 275 (FC) at para 127; Privacy Commissioner of Canada, PIPEDA Case Summaries #114, #268, #269, #273, #279, #290, #379.

120. Examples given include bank machines and high-crime areas.

Other legislation will also have an impact on what techniques of surveillance are permitted. For example, the Criminal Code makes it an offence to intercept telecommunications,[121] and consequently this type of surveillance activity is curtailed.

In the employment context, video surveillance of employees for performance purposes is generally frowned upon and disallowed.[122] Provided that surveillance is being conducted for legitimate purposes such as theft prevention or detection, the inadvertent capture of employee information might not be problematic so long as its subsequent use is in compliance with PIPEDA.[123] When used for legitimate purposes, other technologies that have a surveillance component, such as global positioning devices and voice print biometrics, have also been found to be consistent with PIPEDA.[124]

D. Data Mining

Privacy legislation protects personal information that is connected to an identifiable individual. Consequently, information with identifiers removed is not protected under privacy law. As such, the commercial and health care setting displays a great deal of latitude for the unimpeded use of de-identified information. Apart from the questions surrounding the efficacy of techniques used to de-identify personal information—is the information truly anonymous?—thorny questions concerning whether consent is needed *prior to* anonymization have yet to be discussed or answered by courts or policy makers.

E. Special Areas Permitting or Requiring Anonymity

Copyright Law Copyright legislation provides authors and creators of works with the right to remain anonymous with respect to attribution, including the right to use a pseudonym.[125]

Adoption and Reproductive Technologies Rules surrounding adoption and the use of donor gametes hold that the anonymity of all concerned is the general rule.[126] Nonidentifying and useful information such as health information is generally available to children who have been adopted or were conceived through the

121. Criminal Code s. 184 (n. 44).

122. This is a very complex topic and only very briefly touched on here. See Eastman (n. 119) at paras 126–173.

123. *Ibid*. See, for example, Privacy Commissioner of Canada, Case Summary #290. Case Summary #279 strongly suggests that the use of video surveillance solely for performance monitoring would be contrary to PIPEDA. Note that even covert surveillance has been found to be acceptable provided that it meets the strict standards of the legislation; see Case Summary #379.

124. See, for example, Privacy Commissioner of Canada, Case Summaries #351 and #281.

125. Copyright Act, R.S.C. 1985, c. C–42, s. 14.1(1).

126. For example, Child and Family Services Act, R.S.O. 1990, c. C.11.

use of donor gametes. In the case of adoption, there are also significant provisions to allow parties to connect when the child reaches maturity. Additionally, some Canadian jurisdictions show a move toward more open adoptions, allowing parties to contact each other more easily and with fewer constraints.[127] Over time, the social policies favoring the support of anonymity in this context have given way to a greater emphasis on the provision of at least nonidentifying information as well as promoting the provision of identity information to facilitate contact.

V. ANONYMITY IN PUBLIC

The cumulative effect of government and industry deployment of technology, particularly systems of surveillance, has resulted in a loss of the de facto anonymity once enjoyed in public spaces.[128] The increased deployment of surveillance by government[129] has a clear impact on individuals seeking anonymity in public places.

There is no clear answer as to how the law will limit the use of generalized surveillance, that is, surveillance that is not time-limited and targeted to a particular person, circumstance, or event. However, there are a number of reasons to believe that there are some legal limits placed on government before generalized public surveillance systems are deployed.

An influential 2002 legal opinion[130] suggests that the use of generalized video surveillance for law enforcement purposes violates the public sector Privacy Act[131] and section 8 of the Charter.[132] Although this opinion makes a strong case, it is not definitive, and a number of other developments suggest that although deployment may be controlled, it will nonetheless be permitted.

A number of jurisdictions have put forth guidelines concerning the deployment of video camera surveillance by the government that restrict deployment on the basis of provisions of the public sector privacy legislation regulating the collection and use of personal information by government. This includes law enforcement agencies. These guidelines express concern about the increased deployment of generalized surveillance and seek to limit it to situations in which deployment is a last resort measure.

---

127. See note 23 and accompanying text.

128. Ian Kerr, *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (New York: Oxford University Press, 2009), Chapter 5.

129. Office of the Privacy Commissioner of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (Office of the Privacy Commissioner of Canada: Ottawa, 2006).

130. Opinion by Justice Gérard La Forest, April 5, 2002, Privacy Commissioner of Canada, http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp.

131. R.S.C. 1985, c. P–21.

132. Charter (n. 4).

Regrettably, the promulgation of guidelines and their content indicates that there is no anticipated bar on this form of government activity. Moreover, a number of formal findings concerning the deployment of generalized surveillance for law enforcement or security purposes suggest that private sector privacy legislation will not be violated if properly justified with sufficient safeguards in place.[133] An example that bodes poorly with respect to establishing limits is the special report of the Information and Privacy Commissioner of Ontario. The report focused on the use of generalized surveillance in Toronto's mass transit system.[134] The commissioner found that the deployment of video surveillance and its ability to provide information to law enforcement authorities was in compliance with public sector privacy legislation.

The criminal law section above noted that surveillance for law enforcement purposes is somewhat constrained and curtailed. In order to determine whether the deployment of generalized video surveillance[135] is constitutionally sound and free from section 8 Charter infringements, one must determine the "status" of public space with respect to the reasonable expectation of privacy.

The jurisprudence in this area is far from clear. Although there are strong statements to the effect that unrestricted video surveillance on the part of the state could annihilate privacy,[136] other statements recognize that some spaces and circumstances are not likely to be found to have a reasonable expectation of privacy.[137] Until this matter is squarely before the courts, it is not possible to state definitively that the deployment of generalized video surveillance by the government for law enforcement purposes would be found to be constitutionally sound.

---

133. See section IVC.

134. Office of the Information and Privacy Commissioner of Ontario, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report* (March 2008).

135. Particularized surveillance of a specific individual or event would be subject to the normal legal tests.

136. For example, *R. v Wong* [1990] 3 S.C.R. 36 "The notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society. There are [. . .] situations and places which invite special sensitivity to the need for human privacy. Moreover . . . we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."

137. For example, *Tessling* (n. 69) found that there was no reasonable expectation of privacy in images of heat emanating from a building that were captured by a plane using FLIR camera and, in discussing the lesser protection afforded informational privacy, suggests that if generalized surveillance in public places is characterized as "informational" and is not seen to contain core biographical then it may well be consistent with section 8 of the Charter (n. 4).

Although technically within the "private realm," shopping malls, stores, and buildings with general public access may well be considered by those using them to be quasi-public and similar to public spaces such as streets and parks. Although the deployment of surveillance in these spaces was discussed above, here it is important to take stock of the cumulative impact that surveillance in these and public spaces has on the overall ability to remain anonymous outside the home. Apart from the "feeling" of being surveilled and the impact that this may have on behavior, there is also the fact of significant data collection concerning activities in these spaces, which, if recorded, may be used in combination for a variety of purposes, including law enforcement purposes.

VI. CONCLUSION

Anonymity is a complex topic and one that the law has dealt with in a piecemeal rather than coherent fashion. As a result, the impact on the de facto anonymity once enjoyed in Canada of information collection practices, information consolidation, and general surveillance has not been fully appreciated or addressed. The existing social climate is one that is marked more by concerns related to security than concerns related to lessening opportunities for anonymity. The current legal structure has not proved sufficiently able to preserve and protect what might be considered a somewhat fragile "right" of anonymity. Although it is extraordinarily difficult to hold back the juggernaut of surveillance, information collection, and consolidation on the part of government and industry, it is the authors' view that more robust protections for anonymity should be explicitly considered and adopted in order to preserve fundamental elements of what it is to be human.