Protectiong the Social Value of Privacy in the Context of Police Investigations Using New Technologies

Arthur J. COCKFIELD*

I. Introduction

In pursuit of security, governments around the world are adopting powerful technologies to collect and share detailed personal information, potentially leading to an erosion of privacy. In order to investigate criminal or terrorist suspects, for example, many governments are: deploying close-circuit television (CCTV) to monitor public spaces; promoting the use of national identification cards embedded with biometric identifiers; and accessing personal information held in private sector databases. This Article discusses how legal analysis should respond to situations where technology developments challenge privacy interests in the context of state investigations. In particular, judges, lawyers and policy-makers need to take into more explicit account both the individual rights aspect of privacy as well as the social value of privacy, which is society's interest in preserving privacy apart from a particular individual's interest: both aspects of privacy are critical to the functioning of our democratic state.[1] This approach shows that legal analysis sometimes overstates the tension between privacy and security as both can be portrayed as social interests.

---

* Associate Dean and Associate Professor, Queen's University Faculty of Law. The research for this paper was supported by a Charles D. Gonthier Fellowship from the Canadian Institute for the Administration of Justice (CIAJ). An earlier draft of this article was presented at the CIAJ's conference on *Technology, Privacy and Justice,* held in Toronto in September 2005, and the author would like to acknowledge the helpful comments that he received from conference attendees. The author would like to thank Don Stuart for comments on an earlier version of this paper. This chapter has been modified from an article for the *University of British Columbia Law Review*.

1 See Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* 221 (Chapel Hill: The University of North Carolina Press, 1995).

Part II provides background by reviewing the general concept of privacy along with legal views on privacy in the context of state searches. The traditional understanding of privacy often focuses on the individual rights aspect of privacy by emphasizing privacy as an individual's claim against state interference. This understanding generally leads to legal analysis that sees privacy as a competing interest with security, sometimes resulting in calls for the need to dilute privacy to protect the public against criminal and/or terrorist activities.

Part III discusses an analytical framework to assist in striking a balance between protecting contemporary privacy norms while meeting security needs when state agents deploy new technologies to assist with their investigations. The approach requires an assessment of whether the new technologies are unduly destabilizing traditional privacy interests; if so, the analysis should become more forward-looking and less deferential to traditional doctrine to ensure that these interests are protected. Consistent with Supreme Court jurisprudence that scrutinizes state searches under section 8 of the Charter of Rights and Freedoms, the approach requires a more explicit exploration of the social value of privacy. Under this perspective, even if privacy becomes less important to certain individuals (as their subjective expectations of privacy are reduced in an era of enhanced state surveillance), it continues to serve other critical interests in a free and democratic state (e.g., the need to protect political dissent) beyond those that it performs for a particular person. As such, the preservation of the social value of privacy can be portrayed as consistent with the promotion of long-term security interests. Moreover, the approach requires scrutiny of the ways that technologies and/or technology policies can protect the social value of privacy by promoting privacy safeguards in the collection, use and disclosure of personal information by state investigators (e.g., policies that mandate the use of logs of database searches by state agents who are investigating crimes to create an audit trail to inhibit illegal and abusive searches).

Part IV considers how the Supreme Court implicitly recognized the importance of the social value of privacy in *Tessling*[2] by indicating that constitutional protections against state searches should not be diluted even if individual have reduced expectations of privacy under ubiquitous

---

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

government surveillance. In order to establish whether state searches intrude on reasonable expectations of privacy, *Tessling* requires a scrutiny of technology policies, if any, that govern the collection, use and distribution of personal information in the context of state investigations.

II. The Traditional Emphasis on the Individual Rights Aspect of Privacy in State Investigations

A. Non-legal and Legal Views on Privacy

Privacy can be a surprisingly difficult concept to define as there are many different definitions within the literature generated by different academic disciplines that examine privacy.[3] With respect to views on privacy within contemporary democracies, Alan Westin notes:[4]

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, whether in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and societal norms set by the society in which he lives.

---

[3] For discussion, see Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Ithaca: Cornell University Press, 1997) at 46-61 (providing narrow and expansive definitions for privacy interests).

[4] See Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 6-7.

Westin and other researchers recognize that privacy interests are shaped by complex social, economic and political processes.[5] These researchers sometimes try to measure privacy interests in a particular time and place (e.g., through polling or surveys), often by separating the interests into overlapping categories such as territorial, bodily, information, or communication privacy. As subsequently discussed, Canadian judicial views on state searches similarly attempt to define privacy interests by grouping them into related categories. By emphasizing privacy as an individual right—a claim against state interference with an individual's enjoyment of her privacy—these views tend to support an understanding of privacy as a competing interest with security.

Over time, many (generally Western) societies came to view privacy as an important value that gave rise to a privacy interest or right recognized by law or social convention.[6] But where did this notion that the law should somehow protect an individual's privacy interest come from? Views on privacy as a legal interest or right are sometimes traced to earlier political philosophical conceptions of private property that predated the modern conception of individual privacy.[7] For example, John Locke, one of the founders of liberalism, maintained that "every man has property in his own person. This no body has any right to but himself. The labour of his body, and the work of his hands, we may say, are

---

5 See, e.g., David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001), at 149 (discussing the ways that computerized surveillance shapes social processes and privacy interests); James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986); Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, NY: Cornell University Press, 1992).

6 Alan F. Westin, "Social and Political Dimensions of Privacy," [2003] Journal of Social Issues, vol. 59, no. 2.

7 See *Hunter v. Southam*, [1984] 2 S.C.R. 145, at 157-158; *Tessling*, supra note 2, at par. 16. See also Sonia K. Katyal, "The New Surveillance" [2004] 54 Case Western L. Rev. 297, 302-06. For a discussion on the liberal traditional, see Charles D. Gonthier, "Law and Morality," [2003] 29 Queen's L. J. 408 (arguing that Charter analysis should focus more on duties that accompany rights).

properly his."[8] Locke's conception of property, sometimes referred to as the labour theory of property, requires that the individual be able to exclude others from her privately held property. Under the classical liberal view, to secure these 'natural' rights to private property individuals require a certain amount of freedom from state interference.[9]

Private property rhetoric hence may have served as a proxy for then-undeveloped notions of privacy.[10] For example, the link between property and privacy is revealed by the famous passage by William Pitt, Earl of Chatham, in a speech on the *Excise Bill* in the English Parliament: "[t]he poorest man may in his cottage bid defiance to the Crown. It may be frail; its roof may shake; the wind may enter; the rain may enter—but the King of England cannot enter—all his forces dare not cross the threshold of the ruined tenement!"[11] Early common law protections similarly asserted that individuals have certain rights that flow from their ownership or residency of private homes in areas such as criminal law ("[t]he house of every one is his castle…") and tort law ("... our law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave.").[12]

---

8 See John Locke, *Two Treatises of Government* bk. 2, ¶ 123 (Mark Goldie ed., 1996)(1690) at 178.

9 For background, see Arthur J. Cockfield, "Income Taxes and Individual Liberty: A Lockean Perspective on Radical Consumption Tax Reform," [2001] 46 S. D. L. Rev. 8, 15-18.

10 See, e.g., William C. Heffernan, "Fourth Amendment Privacy Interests" [2002] Journal of Criminal Law and Criminology 1, 13.

11 See John Bartlett, *Familiar Quotations: A Collection of Passages, Phrases & proverbs Traced to their Sources in Ancient and Modern Literature*, 10th ed. (Boston: Little, Brown & Co., 1919) at 365.

12 The link between private property and privacy is revealed by the early common law recognition that individuals can defend their private properties without fear of state sanctions: "The house of every one is his castle, and if thieves come to a man's house to rob or murder, and the owner or his servants kill any of the thieves in defence of himself and his house, it is no felony and he shall lose nothing." Semayne v. Gresham (1604) 5 Co. Rep. 91a at 93a, 77 E.R. 194 at 198 (K.B.). Similarly, the common law recognized that an individual might be liable for damages for trespassing on private property even though the trespassor may have only stepped onto the property for a moment. See *Entick v. Carrington and Three Other King's*

As noted by Warren and Brandeis who, in 1890, first argued that privacy was a separate legal interest, "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society… Gradually the scope of legal rights broadened, and now the right to life has come to [include] … the right to be left alone."[13] More recently, in 1948, the United Nations' Universal Declaration of Human Rights asserted that people have the right to be free from "arbitrary interference with … privacy, family, home, or correspondence."[14]

B. Privacy and State Searches

In Canada, common law and legislative protections against state searches ultimately evolved to constitutional protections where section 8 of our Charter of Rights and Freedoms now provides, "Everyone has the right to be secure against unreasonable search or seizure." With respect to this Charter provision, courts have struggled to set out the scope and ambit of privacy in the context of state scrutiny of alleged criminal behavior.

Section 8 case law likely provides the most developed and detailed judicial analysis of privacy interests within the Canadian justice system.[15] In its first section 8 case that referenced privacy, the Supreme Court noted that the rights guaranteed under section 8 can be expressed "negatively as

---

Messengers (1765), 19 How. St. Tr. 1029 ("No man can set foot upon my ground without my license, but he is liable to an action, though the damage be nothing.").

13 See Louis D. Brandies and Samuel Warren, [1890] "The Right to Privacy" 4 Harv. L. Rev. 193. According to Warren and Brandeis, rights to protect personal writings from publication did not emerge from principles of private property, but should be seen as forming part of, they argue, a distinctive common law right to privacy. Other commentators subsequently argued that privacy is not a separate right in and of itself.

14 See art. 12 of the United Nations, Universal Declaration of Human Rights (1948).

15 In addition to state searches for criminal investigation purposes, section 8 has also been used to restrict the ability of government officials to seize and disclose tax returns for purposes of assessing a taxpayer's tax return. See *Gernhart v. R.,* [1999] 181 D.L.R. (4th) 506 (Fed. C.A.). Section 7 appears to be becoming increasingly important in Charter privacy analysis. See *Ruby v. Canada (Solicitor-General*) [2002] 4 S.C.R. 3, at par. 32 ("[T]here is an emerging view that the liberty interest in s. 7 of the Charter protects an individual's right to privacy.").

freedom from 'unreasonable' search or seizure, or positively as an entitlement to a 'reasonable' expectation of privacy."[16] The reasonable expectation of privacy contains both a subjective and an objective element.[17] An early decision focused on the need for a contextual approach that "allows for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement."[18]

The more recent *Tessling* case provides an example of this ongoing struggle. The Court began its overview of the state of privacy laws in the context of state searches by reiterating the words of La Forest J., "[t]he restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state."[19] As a result of this policy concern, section 8 has been interpreted to create certain areas of personal autonomy where state agents cannot enter.[20] According to the Court, these areas "have now been gathered up under the general heading of privacy" and that "privacy became the dominant organizing principle" for section 8 analysis.[21] Like the definitions of privacy found within non-legal academic disciplines, the Court accepts that privacy can be divided into discrete, but related categories that include personal privacy, territorial privacy and information privacy.[22] The Court indicates that personal privacy has the "strongest claim" to constitutional protection because it "protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal."[23]

---

16 See *Hunter v. Southam*, [1984] 2 S.C.R. 145, at 159.

17 See *R. v. Edwards*, [1996] 1 S.C.R. 128, at par. 45.

18 See *R. v. Plant*, [1993] 3 S.C.R. 281, at 293 (Sopinka J.).

19 *Tessling*, supra note 2, at par. 13, citing R. v. Dyment, [1988] 2 S.C.R. 417, at pp. 427-428.

20 *Id.* at par. 15.

21 *Id.* at par. 15 and 19. The Court is careful to point out that s. 8 could cover "interests beyond the right of privacy," quoting Dickson J., in *Hunter v. Southam Inc.,* [1984] 2S.C.R. 145.

22 *Id.* at par. 20.

23 *Id.* at par. 21

With respect to territorial privacy, Canadian courts have developed a nuanced hierarchy that offers greatest constitutional protection to privacy in the home, and lesser protection to activities that take place in the perimeter space around the home, in commercial spaces, in private cars, in a school and even in a prison. While section 8 extends protection to "people not places", this hierarchy of places is used to help evaluate whether an individual has a reasonable expectation to privacy as this expectation is tied to a certain extent to the place where an individual's activities take place.[24]

With respect to informational privacy, the Court adopts Westin's definition that this type of privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[25] Moreover, drawing from an earlier decision by the Supreme Court, the Court reiterates that this information includes information that "tends to reveal intimate details of the lifestyle and personal choices of the individual."[26]

The Court notes that the discrete categories of privacy interests may overlap depending on the facts of a given case.[27] For example, as subsequently explored in Part IV, a search by RCMP planes that involved the use of technology to see whether a residence's exterior revealed heat patterns implicates informational privacy (because it is concerned with the activities of the accused), but also involves territorial privacy concerns because the activities under investigation took place in a private residence.

Finally, the Court appears sensitive to the ways that technology can subvert privacy interests, repeating La Forest J.'s assertion that "we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."

---

24 *Id.* at par. 22.

25 *Id.* at par. 23, citing A.F. Westin, *Privacy and Freedom* (1970), at 7.

26 *Id.* at par. 25, citing *R. v. Plant*, supra, at p. 293.

27 *Id.* at par. 24.

Indeed, in earlier decision the Court recognized that, "Electronic surveillance is the greatest leveler of human privacy ever known."[28]

In summary, legal views on privacy interests have been influenced by researchers such as Westin as well as classical liberal views of the relationship between the state and the individual: "In much of the philosophical writing about privacy, the components of society are not identified; only the individual and society are recognized. What elements make up "society" and whether the interests of these elements are indeed "social" are not critically explored."[29] The emphasis on the individual rights aspect of privacy has influenced the view on the need to 'balance' privacy against security, which, as explored in the next Part, is increasingly viewed as unhelpful for legal analytical purposes.

III. Exploring the Social Value of Privacy in State Investigations Using New Technologies

A. Deploying a Law and Technology Analytical Framework

In an earlier work, I outlined an analytical framework to assist judges and policy makers with developing optimal public policy in an environment where technological change can subvert interests that the law seeks to protect.[30] This Part draws from this framework and elaborates on ways that can assist in striking the right balance between the sometimes competing – and sometimes consistent – objectives of protecting privacy and enhancing security. Under this analytical framework, the legal decision-maker should first determine whether the technological change is undermining traditional privacy interests (including both the individual and social aspects of privacy). If this step determines that technology change is disrupting traditional interests, the next step is to deploy more

---

28 See *R. v. Duarte*, [1990] 1 S.C.R. 30 at 43, quoting Douglas J. in *U.S. v. White* 401 U.S. 745 (1971).

29 See Regan, supra note 1, at 218.

30 See Arthur J. Cockfield, "Towards a Law and Technology Theory," [2004] 30 MAN. L. J. 383.

forward-looking analysis (i.e., less deferential to traditional doctrinal analysis) that seeks to find legal solutions to protect these interests.[31]

This analytical framework is consistent with the views of Chief Justice McMurtry in Chapter 2 where he suggests that judges should use a more creative approach if they determine that traditional common law analysis is less helpful to preserve interests in the context of globalization and online defamation. Moreover, the analytical approach is informed by theories of technology that have been developed by scholars outside of the legal academy.[32] In particular, the second step of the analysis corresponds with the views under substantive theories of technology where technological developments are seen as embedded within social, political and economic processes.[33] Under one view, "[t]he issue is not that machines have 'taken over,' but that in choosing to use them we make many unwitting cultural choices. Technology is not simply a means but has become an environment and a way of life: this is its 'substantive' impact." [34] While there exists an extensive diversity of views on this topic, the substantive theories share a suspicion that technology change can overcome human agency and lead to unanticipated and adverse policy outcomes. As subsequently discussed, a consideration of the social value of privacy in additional to the traditional individual rights aspect of privacy may better protect against adverse social outcomes such as a dilution of values necessary to promote a free and democratic society.

---

[31] To a certain extent, the first step of the framework could be compared to the doctrinal method of constitutional interpretation while the second part more closely resembles the contextual balancing act of different interests under prudential interpretation although it is recognized there are other potential interpretive approaches (and it is recognized that contextual analysis is also needed to determine what interests have been affected by the technology change). For discussion on different interpretative techniques and forms of legal reasoning, see, e.g., Philip Bobbitt, *Constitutional Interpretation* 11-22 (1991).

[32] For discussion, see Arthur J. Cockfield and Jason Pridmore, "A Synthetic Theory of Law and Technology," 8 *Minn. J. L. Science and Tech.* (forthcoming, 2007).

[33] For discussion, see Andrew Feenberg, *Critical Theory of Technology* (New York: Oxford University Press, 1991), at 5. See also Donald MacKenzie & Judy Wajcman, eds., *The Social Shaping of Technology*, 2nd ed. (Buckingham: Open University Press, 1999).

[34] See Feenberg, supra note 32, at 8.

B. The Social Value of Privacy and Section 8 Charter Jurisprudence

Intrusive surveillance practices are normally rationalized under the view that reduced privacy is necessary to promote public security. In fact the traditional privacy/security dialectic in public policy circles is increasing challenged by observers as unhelpful.[35] By drawing from substantive theories of technology, a more accurate assessment of the risks associated with reducing legal protections in an era of enhanced surveillance technologies could be derived.[36] Under the substantive view, legal analysis should recognize the 'social' aspect of privacy that acknowledges how a reduced level of privacy may in fact make us less secure. Priscilla Regan, for instance, claims that privacy serves purposes beyond those that it performs for a particular individual: she notes that one aspect of the social value of privacy is that it sets boundaries that the state's exercise of power should not transgress to preserve, for example, freedom of speech and association within a democratic political system.[37] In her view, even if particular individual privacy interests become less compelling, social interests in privacy may remain.

Consistent with this view, research by sociologists, political scientists and others discusses how surveillance technological advances

---

[35] For criticisms of the over-emphasis of individual control over privacy as a way to understand privacy interests, see Paul M. Schwartz, "Internet Privacy and the State" [2000] 32 Conn. L. Rev. 815, 821-22 (noting that governments play a critical role in shaping privacy norms through state policies, including an absence of government action); Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (London: Ashgate Press, 2003); Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, (1989) 77 Calif. L. Rev. 957.

[36] See also Lisa Austin, "Privacy and the Question of Technology" [2003] 22 Law and Philosophy 119, 142 (arguing that technology forces us to clarify our understanding of privacy interests and that an "independent justification approach" better protects these interests).

[37] See Regan, supra note 1, at 221-230. She divides privacy into three social values: (1) a common value where all persons have a common interest in a right to privacy although they may differ on views on the specific content of privacy; (2) a public value where privacy is instrumentally valuable to a democratic political system; and (3) a collective value where privacy is seen as a collective good that, from an economist's perspective, cannot be efficiently provided by the marketplace.

could dilute the social value of privacy and heighten the risk of unanticipated adverse social consequences.[38] More specifically, increased scrutiny by state agents can:[39] (a) stifle political dissent as individuals fear reprisal by government actors; (b) inhibit freedom of expression as individuals fear public scrutiny of their views or behavior; (c) lead to racial or religious profiling (i.e., discrimination) that targets identifiable groups despite no evidence of individual wrong-doing, which could lead to social alienation for members of the targeted group who increasing take on an 'us' versus 'them' mentality (d) have a disproportionately adverse impact on lower income Canadians who tend to make greater use of public spaces, which are increasingly subjected to state scrutiny; (e) results in political complacency to the extent that ubiquitous surveillance eliminates any subjective expectation of privacy and discourages citizens from questioning more and more state scrutiny; and (f) make it harder to hold state agents accountable for their potentially abusive behavior in part because of the surreptitious nature of the new technologies. A concern shared by these researchers is that an erosion of the social value of privacy dilutes important shared values within a free and democratic state that, at least in the long run, will make the Canadian public less secure. For example, religious or racial profiling without any evidence of individual wrong-doing may make members of the targeted group less willing to assist authorities with terrorist investigations.

---

38 See *e.g.* David Lyon & Elia Zureik, Surveillance, Privacy, and the New Technology, in David Lyon & Elia Zureik eds., *Computers, Surveillance & Privacy* (Minneapolis: University of Minnesota Press, 1996); James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986); Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, NY: Cornell University Press, 1992).

39 For discussion, see Gary T. Trotter, "The Anti-terrorism Bill and Preventative Restraints on Liberty", in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom : Essays on Canada's Anti-terrorism Bill 246* (Toronto : University of Toronto Press) (arguing that the cumulative effect of anti-terrorism laws may significantly dilute liberty interests); Arthur J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Growing Government and Private Sector Surveillance", (2003) 29 *Queen's L.J.* 364, 391-398; Kevin D. Haggerty and Amber Gazso, "Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats," (2005) 30 *Can. J. Soc*. 169, 180-185.

While Canadian courts may not have explicitly analyzed privacy as a concept involving both individual and collective components, the importance of the social value of privacy has at least been implicitly recognized by the Supreme Court in certain cases. Consider two early section 8 cases that interpreted constitutional protections against government searches and the use of electronic forms of surveillance by the police. In *Duarte*,[40] the Supreme Court was confronted with its first post-Charter case involving so-called participant surveillance. To investigate alleged drug trafficking, the police rented an apartment for a police informer and equipped the apartment with audio-visual recording equipment installed in a wall. The main issue was whether a warrant was necessary to conduct this electronic search because the *Criminal Code* provisions at the time excepted the need for a warrant when one of the parties consents to the surveillance. The Ontario Court of Appeal employed traditional analysis that focused on the fact that the accused had assumed the risk that he would be subjected to surveillance by his "tattletale" informer.

Consistent with the law and technology analytical framework noted previously, the Supreme Court rejected this view in favor of a broader and more contextual understanding of the potential harm to privacy interests. According to the Court, warrantless participant surveillance would give the police unfettered discretion to record and transmit our words which "might be superbly equipped to fight crime, but would be one in which privacy no longer have any meaning."[41] Rather, the real question is "not whether criminals must bear the risk of warrantless surveillance, but whether it should be imposed on all members of society."[42] These views acknowledge the importance of the social value of privacy because if warrantless participant surveillance was

---

40 See *R. v. Duarte*, [1990] 1 S.C.R. 30.

41 *Id.*

42 Quoting *Commonwealth v. Thorpe*, 424 N.E.2d 250 (1981), at 258 (Mass. Supreme Court).

permitted it would undermine the privacy interests of all Canadians, which is "the very hallmark of a free society."[43]

In *Wong*[44], the police installed without prior judicial authorization a video camera in a hotel room to investigate an alleged illegal gambling house. Based on the surveillance, the police conducted a raid and arrested the accused. The Ontario Court of Appeal held that the accused, who had openly engaged in a criminal activity, did not have a reasonable expectation of privacy that the police would not monitor him through video surveillance.

The Supreme Court disagreed and held that section 8 requires judges to ask from a neutral perspective whether an innocent person—not a criminal—would have a reasonable expectation of privacy. The Court reviewed the potential for abuse surrounding new electronic search methods, and concluded that the neutral question would better protect against technological change that could harm privacy interests: "[T]he technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being."[45] As such, the searches must be scrutinized in light of "the standards of privacy that persons can expect to enjoy in a free and democratic society."[46] Otherwise, the Court feared that anti-democratic outcomes could result to the extent that citizens fear ubiquitous government surveillance, again apparently recognizing the critical importance of the social value of privacy. As discussed in Part IV, the Supreme Court's most recent pronouncement on these issues in *Tessling* also supports a recognition of the importance of the social value of privacy in section 8 analysis.

---

43 The Court nevertheless held that the evidence collected by the surveillance was admissible in part on the grounds that it would not bring the administration of justice into disrepute.

44 See *R. v. Wong*, [1990] 3 S.C.R. 36.

45 *Id.*

46 *Id.*

C. Explore Whether Technology or Technology Policies Can Protect the Social Value of Privacy

Canada and other governments are responding to their constituents' concerns about security by promoting the use of new technologies by police and/or intelligence officials to locate, track and arrest suspected criminals and/or terrorists. These efforts have been accompanied by legislative changes that dilute traditional safeguards against state searches.[47] To promote optimal policy outcomes with respect to the individual rights aspects as well as more collective aspects of privacy, governments need to focus on the ways that technologies or policies that govern usage of these technologies can protect privacy.[48]

This view follows the so-called "code is law" perspective (where 'code' is the software and hardware technologies that constitute the Internet) that maintains that governments should, at times, regulate the development of technology so that they can indirectly regulate an individual's behavior.[49] In other words, the regulation of technology itself can often assist governments in promoting their policy goals.

---

47 The Canadian government responded to perceived security threats by, among things, passing omnibus anti-terrorism legislation (Bill C- 36, *Anti-Terrorism Act*, S.C. 2001, c. 41) to assist state agents in investigating suspected terrorist activities. These legal changes included: making it easier to obtain warrants to use electronic surveillance against terrorist suspects; abolishing the need to obtain warrants in cases of perceived national security; reducing legal thresholds to obtain electronic records; enhancing the government's ability to share personal information among different government agencies or with foreign governments; and increasing the powers to deport residents for violations of immigration laws. Most controversially, the legislation permits warrantless searches of terrorist suspects and judicial investigative hearings in certain circumstances, eliminating traditional common law safeguards against unauthorized arrests and searches. For discussion, see, e.g., Ronald J. Daniels, Patrick Macklem and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001).

48 For discussion, see Arthur J. Cockfield, "The State of Privacy laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government" (2004) 1 *Univ. Ottawa L. and Tech. J.* 325, 338-344.

49 See generally Lawrence Lessig, *Code and other laws of cyberspace* (New York: Basic Book, 1999) at 6.

In this 'fight fire with fire' approach, policy-makers regulate technology developments to address problems promoted by other technologies.[50] For instance, under the draft *Modernization of Investigative Techniques Act*, the former federal Liberal government proposed a law to compel Internet Service Providers (ISPs) to adopt technologies that permit investigators to intercept Internet communications.[51] In another example, the U.S. Federal Communications Commission voted in August 2005 to require providers of Internet phone calls (who employ VoIP technology, touched on previously) to ensure their equipment can allow police wiretaps.

In addition to attempts to regulate the development of technologies for security purposes, there are increasing government efforts to develop laws, policies and practices to govern how state agents may use technologies to collect, store and share personal information. For example, under the Advance Passenger Information/Passenger Name Record (API/PNR) program, the Canada Borders Services Agency (CBSA) is authorized to collect and retain information on travelers for customs purposes for up to six years.[52] In order to enhance privacy protections, the CBSA adopted guidelines and safeguards, including: permitting access to the information by customs officials for the first seventy-two hours, then restricting access after this date and making names available only after the obtainment by state agents of a warrant; restricting access to a limited number of intelligence officials; and purging information such as what travelers ordered to eat.[53] In another example, the federal Office of the Privacy Commissioner of Canada, provincial privacy commissioners as well as European governments have issued guidelines with respect to the use of close-circuit television cameras in public spaces.[54]

---

[50] For a discussion on the ways that technology can enhance government accountability over surveillance measures, see [deleted for review purposes].

[51] Bill C-74, First Session, Thirty-eighth Parliament 53-54 Elizabeth II, 2004-2005 (First Reading, Nov. 15, 2005).

[52] *Customs Act*, R.S. 1985, c. 1 (2nd Supp.), s. 107.1

[53] See "Canada Border Services Agency, Advance Passenger Information/Passenger Name Record Fact Sheet" (Jan. 2004).

[54] See, e.g., Office of the Privacy Commissioner of Canada, OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement

The common thread behind these policies is an attempt to promote policies and practices to protect privacy interests in an era when governments are deploying new technologies to collect personal information. A potentially helpful approach would look to recent privacy law reform efforts such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into full effect in January 2004, to assist with the development of guidelines and practices.[55] In fact, PIPEDA offers stronger privacy protections for personal information collected by the private sector than is often the case with respect to similar information collected by the state investigators (although it is recognized that PIPEDA itself has been criticized for having inadequate enforcement mechanisms and other problems). This occurs in part because the *Privacy Act*, the legislation that governs the information collection practices of federal agencies, took effect in 1983 and may not reflect more recent views.[56] Moreover, law enforcement activities are typically exempt from the *Privacy Act*'s obligations with respect to the collection and management of personal information.

When the determination is made to employ new technologies as investigatory tools, the starting point for the development of a government privacy/technology policy could be the ten fair information practice principles (FIPPs) found in Schedule One of PIPEDA: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance. These FIPPs were drawn from widely-accepted

---

Authorities (March 2006); Ann Cavoukian, Guidelines for Using Video Camera Surveillance in Public Spaces (Information and Privacy Commissioner (Ontario), 2001). Privacy commissioners from British Columbia and Alberta have proposed similar guidelines. See also Robert W. Hubbard, Susan Magotiaux, and Matthew Sullivan, [2004] 49 Crim. L. Quart. 222, 248-249 (discussing operational guidelines to defining and limiting the usage of close-circuit television cameras in public spaces in Europe and elsewhere).

55 S.C. 2000, c. 5.

56 For example, the Privacy Commissioner recommended over one hundred changes to the *Privacy Act* to make it more responsive to current concerns. See Privacy Commissioner of Canada, "Annual Report (1998-1999)" See also *Re Privacy Act*, [2000] F.C.J. 179 (F.C.A.), leave to appeal denied [2001] S.C.J. 86 (holding that information collected by government departments can be freely shared with other departments without consent or notice under the *Privacy Act*).

views on fair information collection practices for the private sector.[57] The PIPEDA principles would serve two purposes. One, it would ensure that information collection practices for justice system matters are subjected to at least the same rigour as the private sector (when appropriate). Two, it would promote a certain amount of consistency and coherence among the practices developed by different aspects of the justice system.

The principles can be used to provide a check-list to see whether government collection practices are addressing important privacy concerns. The principles could then be modified to take into consideration the particular security needs of the particular aspect of the justice system under scrutiny, as well as the relevant legal regime that governs the collection of information. In many cases, the use of certain principles will be inappropriate if they unduly constrain state investigations (e.g., national security would be compromised if individuals are provided access to personal information held by investigators). Nevertheless, the FIPPs could serve as a useful starting point. The approach is similar to the use of privacy impact assessments, which promote compliance with all relevant laws while meeting the "privacy expectations of the public with respect to moral and ethical considerations."[58]

In summary, by using PIPEDA as a guide or through some other approach, technology policies can be developed to: (a) enhance accountability by providing rules to govern how state agents can use technologies to collect, store and exchange personal information; (b) ensure that only personal information that is relevant to security purposes is retained; and (c) provide information to the public on existing forms of state scrutiny. These sorts of approaches could serve to defend against the dilution of the social value of privacy and, at least in the run, promote

---

[57] The principles were drawn from the Canadian Standards Association model code of information collection practices, which in turn were based on earlier documents from the OECD. See OECD, Department of Science, Technology & Industry, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980).

[58] See David Flaherty, Privacy Impact Assessments: An Essential Tool for Data Protection (2000), available at http://aspe.hhs.gov/datacncl/flaherty.htm. See also Treasury Board of Canada, Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks (2002), at 5.3.2. (applying the PIPEDA principles via a questionnaire for government programs with cross-border information flows).

security interests by preserving important democratic values. As subsequently discussed, the fact that the RCMP may not have put in place any policy to govern the collection, usage or disclosure of information obtained by FLIR searches may, in and of itself, threaten the social value of privacy in such a way to render the searches constitutionally impermissible.

IV. Case Study: FLIR Searches

This Part elaborates on the analysis in the previous Parts by discussing how the Supreme Court continues to recognize the importance of the social value of privacy in the context of state surveillance employing new technologies.

A. The Facts of *Tessling*

In *Tessling*, the RCMP used an airplane equipped with a Forward Looking Infra-Red (FLIR) camera to take a "heat" picture of Mr. Tessling's home without first seeking judicial authorization through a warrant.[59] FLIR technology records the relative distribution of heat over the surface of a building: it cannot peer through the external surfaces of a building. As a result of the FLIR recording and information supplied by two informants, the RCMP was able to obtain a warrant and discovered a large quantity of marijuana and several guns at Mr. Tessling's premises. At trial, Mr. Tessling unsuccessfully argued that the FLIR recording constituted a violation of his right to be free from unreasonable search and seizure under section 8 of the Charter. The Ontario Court of Appeal, however, agreed that Mr. Tessling's constitutional rights were violated and set aside the convictions. In a unanimous decision, the Supreme Court of Canada allowed a Crown appeal, agreeing with the trial court that the use of FLIR aerial camera to detect heat rays emanating from a private home did not constitute a search within the meaning of section 8.

---

[59] See *Tessling*, supra note 2.

B. Assessing the Analysis

i. Scrutinizing the Specific Privacy Interests at Stake under a FLIR Scan

Consistent with step one of the law and technology analytical framework, the Court's analysis initially focused on the nature of the information that is revealed after a FLIR overflight. Binnie J., on behalf of the Court, noted that: "This device … is essentially a camera that takes photographs of heat instead of light … The rooms of marijuana growing operations with halide lights are warmer than the average room in a residence. The walls of these rooms emanate this heat to the outside, and are therefore detectable by the FLIR. Heat in a residence is usually evenly distributed throughout the building's exterior. By comparing the pattern of heat emanating from the structure, it is possible to detect patterns of heat showing rooms or sections of a structure that may be housing the marijuana growing operation."[60]

In other words, FLIR is used to draw possible broad inferences about an individual's activities although given "the relative crudity of the present technology does not, in itself, permit any inferences about the precise activity giving rise to the heat."[61] The Court focused its attention on the technology and its impact on the informational privacy interest as the FLIR technology could potentially reveal details about the activities of the residents.

According to the Court, the territorial privacy interest also comes into play because the FLIR scrutinized the exterior of the home to draw inferences about activities within the home. But, given the state of the current technology, the distribution of heat on the building's surfaces could be consistent with different possible activities, only one of which is the operation of a marijuana grow-op. The Court noted that the usefulness of the FLIR-revealed information depends on what other information has been collected by the police.[62] As a result, no warrant should be granted

---

60 *Id.* at par. 34.

61 *Id.* at par. 36.

62 *Id.* at par. 53.

based solely on a FLIR image, given the current state of the technology.[63] A FLIR image, however, that is combined with other information such as that provided by informants (as occurred in *Tessling*) may be sufficient to give police reasonable and probable grounds to persuade a judge or justice of the peace to issue a search warrant for a private home.

The Court maintained that the nature and quality of the information revealed by the search do not attract constitutional protections because the search only showed that some of the activities in the house generate heat, and hence did not reveal intimate details of Tessling's lifestyle.[64] The argument that that FLIR can detect different sources of heat, including a wood burning stove, a fireplace, a sauna, which involve private and lawful activities within the home, was rejected.[65] The Court also noted that section 8 is designed only to provide security from unreasonable search and seizure to protect reasonable expectations of privacy.[66] In the Court's view, Tessling did not enjoy a reasonable expectation of privacy in the heat distribution information, in part because the heat emanations are revealed to the public by, for example, snow melting at different rates on a poorly insulated roof.[67]

Assuming that one accepts the debatable point that FLIR searches did not intrude on Tessling's reasonable sphere of privacy, the Court properly used traditional analysis to reject Tessling's assertion that his rights to be free from an unreasonable search were violated.[68] As

---

63 *Id.* at par. 55.

64 *Id.* at par. 62.

65 See Canadian Civil Liberties Association, *Factum of the Intervenor* (2004), at par. 17.

66 *Tessling* at par. 19.

67 The Court nevertheless recognized that FLIR extends the senses to see more than members of the public. *Id.* at ¶ 47.

68 See, e.g., *R. v. Ly*, 2005 ABPC 32, at par. 45-47 (following *Tessling* to hold that the installation of an energy reading meter, which offered more definitive evidence of marijuana grow operation, resulted in a breach of the accused s. 8 Charter rights). But see Lisa Austin, "One Step Forward or Two Steps Back? R. v. Tessling and the Privacy Consequences for Information Held by Third Parties" [2004] 49 *Crim. L. Quart.* 22, 32 (asserting that the Ontario Court of Appeal came to the right decision that a FLIR search violated s. 8 although its analysis was problematic); Don Stuart, "Annotation: R. v. Tessling" 23 C.R. (6th) 209 [2005] (arguing that the ruling in

explored below, the potential absence of any policy to govern FLIR usage by the RCMP should have been taken into account at the trial level to determine the reasonableness of Tessling's expectation of privacy.

ii. Taking into Consideration the Social Value of Privacy

The Court also examined whether FLIR searches could lead to less obvious and more socially ambivalent results. The Court recognized that an age of enhanced surveillance technologies may lead to diminished subjective expectations of privacy as individuals come to expect that their communications or activities are being monitored.[69] Nevertheless, the Court indicates that constitutional protections against unreasonable searches should not be lowered, even if an individual's actually believes she has less privacy in an emerging surveillance society: "Expectation of privacy is a normative rather than a descriptive standard."[70]

This view is consistent with the research by Regan and others who emphasize that privacy has a social value apart from an individual's or group of individuals' interests. Accordingly, even if certain individuals embrace enhanced government surveillance to protect their security, section 8 calls for a benchmark to protect reasonable privacy expectations. Under the Court's view, a requisite amount of protection against state intrusion into the private life of its citizens is needed to promote important democratic values such as the ability to express political dissent without fear of state reprisal.[71] The view acknowledges that the preservation of

---

Tessling "appears to tilt section 8 principles markedly in favour of the interests of law enforcement rather than protecting privacy").

69 *Id.* at par. 45.

70 *Tessling* has led certain observers to suggest that the Court, when evaluating reasonable expectations, may have returned to its earlier view of privacy as a "normative core" aspect of a free and democratic society. See James A. Q. Stringham, *Reasonable Expectations Reconsidered: A Return to the Search to the Search for a Normative Core for Section 8*?, 23 C.R. (6th) 245 (2005).

71 See *Tessling* at par. 42; Austin, supra note 35, at 143. Without a consistent theory to assist in understanding the role of privacy within a free and democratic society, the Supreme Court's jurisprudence on privacy has been criticized as arbitrary and circular because "the present regime resembles more of a guessing game where privacy is defined and proclaimed on a case-by-case basis." See Renee M. Pomerance, "Shedding Light on the Nature of Heat: Defining Privacy in the wake of R. v. Tessling" [2004] 23 C.R. (6th) 229.

social value of privacy is closely linked with the maintenance of a vibrant democracy and hence, at least in the long run, promotes security interests.

As discussed, the Court indicated that existing FLIR technologies are somewhat crude and do not reveal intimate aspects of an individual's lifestyle. But what happens if FLIR technologies changes so that it can collect more detailed personal information about suspects? Under substantive theories of technology, a concern exists that technologies may initially appear to be innocuous in nature, but as they develop they exert more and more control over individuals within society by shaping or 'determining' the way we live: one view suggests that more embedded technologies tend to be increasingly deterministic and resistant to change.[72]

The Court noted that courts must make decisions based on the existing technologies and not seek to, as the Ontario Court of Appeal attempted to, forecast the "theoretical capacity" of technology.[73] If, as expected, FLIR technologies improve and collect more accurate information on the probable activities taking place within the home, then the privacy implications will need to be re-evaluated in light of this technological change: "Whatever evolution occurs in future will have to be dealt with by the courts step by step."[74] The Court hence provides a built-in protection that requires continual reassessment if technologies become more privacy intrusive. This would seem to work against the potential problem of technological determinism because the constant re-examination permits judicial intervention when technology change leads to overly intrusive infringements into privacy interests.

iii. Section 8 and the Need to Examine Technology Policy

The Court's decision permits the police to use FLIR as part of their investigation to collect sufficient evidence to get judicial authorization to conduct a search of suspects' homes. In *Tessling*, the RCMP's FLIR fly-

---

[72] For discussion, see Towards a Law and Technology Theory, supra note 30, at 385-386.

[73] *Tessling* at ¶ 29.

[74] *Id.* at ¶ 55.

over was conducted after informants provided information to suggest that criminal activities were taking place in the suspect's home. It is less clear whether FLIR scans used by police to trigger an investigation would constitute an unreasonable search that would attract the need for prior judicial authorization. For example, the RCMP could fly over and scan vast rural areas to attempt to discern unusual heat emanations coming from farms or homes then focus their investigation on suspected grow-ops. By taking into account the social value of privacy, if FLIR technology can reveal sufficient inferences about activities within a home to trigger an investigation then this sort of search should attract constitutional protections to avoid anti-democratic outcomes.[75]

To provide more certain guidance to citizens as well as the police, it would have been helpful for the Court if it had been presented with trial evidence to assess in greater detail the RCMP's policies with respect to FLIR usage. In fact, the Court offered, as part of the test to determine reasonableness, the question: "Was the use of the surveillance technology itself objectively unreasonable?",[76] which would seem to require this sort of enquiry. While there was not apparently any evidence on RMCP policies concerning FLIR usage before the trial court, the over-extension of FLIR technology (even in its current developmental state) could potentially lead to anti-democratic results such as an increasingly complacent citizenry who fail to try to hold state agents accountable for abusive practices.

Consistent with the views in Part III.C., a better approach would have been, at the trial level, to scrutinize RCMP practices and policies to see: (a) whether the technology is widely-deployed; (b) whether the technology is used to trigger investigations; and (c) whether the RCMP has developed internal practices and policies to ensure that any

---

[75] The fact that the Supreme Court indicates FLIR technology only provides "meaningless" information, yet this so-called meaningless information can be used as grounds, along with other information, for issuing a search warrant has been criticized as contradictory. A proposed solution could involve creating a lower threshold test under the Criminal Code for FLIR searches, such as "reasonable suspicion." See Steve Coughlan & Marc S. Gorbet, "Nothing Plus Nothing Equals … Something? A Proposal for FLIR Warrants on Reasonable Suspicion", [2005] 23 C.R. (6th) 239.

[76] See *Tessling*, supra note 2, at par 56.

information collected is properly managed according to fair information practices. An absence of any police policy could be an indicator that the use of FLIR technology will lead to unacceptable intrusions into reasonable expectations of privacy. For example, extensive use of FLIR fly-overs, given the current crude state of this technology, could enhance the risk of generating false positives that would trigger investigations on innocent individuals. Moreover, to the extent that FLIR fly-overs can trigger investigations, individuals may reasonably expect that the RCMP has put in place a policy to guide the usage, collection and retention of information collected through FLIR or any other searches.

By recognizing the critical importance of the social value of privacy, the reasoning in *Tessling* and earlier section 8 jurisprudence (see Part III.B.) compels the development of such policies by state agencies to ensure that reasonable expectations of privacy are not unduly diluted by the use of new technologies. Under this view, the absence of such a policy heightens the risk that real or feared state scrutiny will reduce security, at least in the long run, by undermining democratic values such as the right for individuals to go about their lives unmolested by state agents as long as there is no evidence of individual wrong-doing.[77] *Tessling* may be a signal by the Court that, in future section 8 cases to establish that a search is constitutionally permissible, the Crown should be required to prove that the relevant police agency has adopted a policy to promote adequate privacy safeguards.

---

[77] But see *R. v. Kang-Brown*, 2005 ABQB 608, at par. 73 (holding that, under the test developed in *Tessling*, an accused does not have a reasonable expectation that their luggage will not be subjected to a dog sniff search in an era of "random terrorist attacks."). In my view, this decision is inconsistent with the reasoning in *Tessling* because the Supreme Court asserted that privacy plays a critical role in enabling democratic values that enhance security, and hence the court will not lower constitutional protections, despite the fact that individuals may have lower expectations of privacy in an era of enhanced surveillance. The Court of Queen's Bench of Alberta, on the other hand, appears to suggest that terrorism threats may permit a circumvention of Charter protections against unreasonable searches even though the search in question was for illegal narcotics, and had nothing to do with terrorism.

V. Conclusion

Legal analysts have traditionally emphasized the individual rights aspect of privacy in the context of police investigations. This view has sometimes led to the notion that privacy is a competing interest with security hence privacy must be diluted to protect the public against criminals and/or terrorists. In an era where the state is deploying new information, communication and genetic technologies that greatly enhance its ability to collect, use and share personal information as part of their investigations, a broader consideration of the privacy interests at stake is required. Accordingly, privacy researchers are increasingly emphasizing the need to protect the social value of privacy, which can be understood as a broader societal interest in privacy beyond the interests of particular individuals. An understanding of the social value of privacy promotes a view of privacy as an enabler of democratic values that are critical to the promotion of long term security. As such, the social value of privacy can be portrayed as consistent—and not competing—with security interests.

Taking into consideration these views, the Supreme Court's analysis in *Tessling* struck the struck the appropriate balance in protecting the accused's right to be free from an unreasonable state search. The Court's decision properly respected security concerns while at the same time ensuring that privacy rights will not be unduly inhibited by, in part, requiring courts to re-examine evolving FLIR technologies to see whether they can reveal more detailed private activities that take place in the home or elsewhere. Moreover, the Court was clear that section 8 requires recognition of the social value of privacy as both a fundamentally important aspect and an enabler of a free and democratic society, signaling that dilutions of constitutional protections for privacy should not be tolerated in an environment of enhanced usage of new surveillance technologies. A closer examination of the RCMP's policies surrounding FLIR usage at the trial level, however, should have been made to ascertain whether the search violated Mr. Tessling's reasonable expectation of privacy. To establish that a state search is constitutionally permissible, *Tessling* compels the Crown to prove that a state agency has developed and initiated technology policies to govern the usage of privacy-encroaching surveillance technologies.