

Winter 2007

Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach

Steven Penney

Follow this and additional works at: <https://scholarlycommons.law.northwestern.edu/jclc>

 Part of the [Criminal Law Commons](#), [Criminology Commons](#), and the [Criminology and Criminal Justice Commons](#)

Recommended Citation

Steven Penney, Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach, 97 J. Crim. L. & Criminology 477 (2006-2007)

This Symposium is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Journal of Criminal Law and Criminology by an authorized editor of Northwestern University School of Law Scholarly Commons.

REASONABLE EXPECTATIONS OF PRIVACY AND NOVEL SEARCH TECHNOLOGIES: AN ECONOMIC APPROACH

STEVEN PENNEY*

The “reasonable expectation of privacy” test, which defines the scope of constitutional protection from governmental privacy intrusions in both the United States and Canada, is notoriously indeterminate. This indeterminacy stems in large measure from the tendency of judges to think of privacy in non-instrumentalist terms. This “moral” approach to privacy is normatively questionable, and it does a poor job of identifying the circumstances in which privacy should prevail over countervailing interests, such as the deterrence of crime. In this Article, I develop an alternative, economically-informed approach to the reasonable expectation of privacy test. In contrast to the moral approach, which treats privacy as a fundamental right, the economic approach views it as an (normatively neutral) aspect of self-interest: the desire to conceal and control potentially damaging personal information. According to this view, privacy should not be protected when its primary effect is to impede the optimal deterrence of crime. In other cases, however, legal protections against governmental surveillance may enhance social welfare by encouraging productive transactions, diminishing the costs of non-legal privacy barriers, and limiting suboptimal policing practices such as discriminatory profiling and the enforcement of inefficient criminal prohibitions. Economics and public choice theory can also help to minimize decision-making error by predicting which legal actors—police, legislatures, or courts—are best placed to make optimal trade-offs between privacy and crime control.

* Associate Professor, Faculty of Law, University of Alberta, LL.M. (Harvard), LL.B. (Alberta), B.A. (Alberta). The author wishes to thank Norman Siebrasse for valuable feedback and Patrick Young for excellent research assistance.

I. INTRODUCTION

In both the United States and Canada, the reasonable expectation of privacy test defines the scope of constitutional protection from governmental privacy intrusions. When a court decides that a person has no reasonable expectation of privacy in relation to an investigative technique, there is no “search” or “seizure” within the meaning of the Fourth Amendment of the United States Constitution¹ or § 8 of the Canadian Charter of Rights and Freedoms.² In such cases, police are free (absent any statutory restriction) to use the technique without first obtaining a warrant or establishing individualized suspicion.³ When there is a reasonable expectation of privacy, in contrast, police must generally obtain a warrant based on probable cause before conducting the search.⁴

Unfortunately, the jurisprudence that American and Canadian courts have developed in applying the reasonable expectation of privacy test is notoriously circular, imprecise, and unpredictable.⁵ In this Article, I argue that this indeterminacy stems in large measure from the tendency of judges to think of privacy in non-instrumentalist terms. Courts typically view privacy as a fundamental right, rooted in notions of dignity, autonomy,

¹ “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.

² “Everyone has the right to be secure against unreasonable search or seizure.” Canadian Charter of Rights and Freedoms § 8, Part I of the Constitution Act, 1982, Canada Act, 1982, sched. B, ch. 11 (U.K.).

³ See generally *Katz v. United States*, 389 U.S. 347 (1967); *R. v. Wong*, [1990] 3 S.C.R. 36, 47 (Can.); *R. v. Duarte*, [1990] 1 S.C.R. 30, 42 (Can.).

⁴ In Canada, the equivalent terminology is “reasonable and probable grounds.” See *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 167-68 (Can.) (“The state’s interest in detecting and preventing crime begins to prevail over the individual’s interest in being left alone at the point where credibly-based probability replaces suspicion.”). Courts have not consistently articulated a precise or quantifiable definition of “probable.” Some courts have treated it as equivalent to “more likely than not,” but others have suggested that it signifies a lesser degree of probability. See WAYNE R. LAFAVE ET AL., *CRIMINAL PROCEDURE* 149-50 (3d ed. 2000); R.E. SALHANY, *CANADIAN CRIMINAL PROCEDURE* ¶ 3.1140 (6th ed. 2005). Courts in both nations have also recognized many circumstances in which, despite the existence of a reasonable expectation of privacy, the constitution does not require warrants, probable cause, or either. In some situations, police may obtain warrants or conduct warrantless searches on the basis of a lesser standard of suspicion (often called “reasonable suspicion”). See JAMES A. FONTANA, *THE LAW OF SEARCH AND SEIZURE IN CANADA* 458-59, 552-55, 595-97 (6th ed. 2005); LAFAVE ET AL., *supra*, at 148.

⁵ See, e.g., 1 WAYNE R. LAFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* 393-94 (3d ed. 1996); Richard Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188.

identity, personality, or liberty.⁶ And while they often acknowledge the existence of countervailing interests, they generally treat privacy as an unalloyed social good.⁷

There are several problems with this approach, which I refer to as the “moral” conception of privacy. First, casting privacy as a moral right is normatively questionable.⁸ It is not at all clear that privacy is as central to human flourishing as most deontologically-oriented jurists claim.⁹ Second, to the extent that it is important, the moral approach does a poor job of identifying the circumstances in which privacy should prevail over countervailing interests, such as the deterrence of crime. Third, neither the Fourth Amendment nor § 8 of the Charter protects privacy in a “fundamental” manner; they protect only the right to be free from “unreasonable” searches and seizures.¹⁰ Even gross privacy invasions may be justified when the State can show that they are likely to reveal evidence of serious crimes.¹¹ As courts in both countries have recognized, constitutional search and seizure decisions (including threshold reasonable expectation of privacy determinations) call for some kind of instrumentalist cost-benefit calculation.¹² Yet by conceptualizing privacy in moral terms,

⁶ See, e.g., Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1001-03 (1964); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

⁷ See *R v. Dyment*, [1988] 2 S.C.R. 417, 429 (Can.) (“[A]ll information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.” (quoting TASK FORCE ON PRIVACY AND COMPUTERS, *PRIVACY AND COMPUTERS: A REPORT OF A TASK FORCE ESTABLISHED JOINTLY BY DEPARTMENT OF COMMUNICATIONS/DEPARTMENT OF JUSTICE* 13 (1972))); Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 871 (2000) (“Liberals have generally assumed that privacy is something people want and that the main goal of public policy is to enhance their capacity to get what they want.”); see also ALAN F. WESTIN, *PRIVACY AND FREEDOM* 7 (1967).

⁸ The literature is replete with debates over the core meaning or meanings of privacy. See generally Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CAL. L. REV. 1447 (1976). The chief concern of this paper is informational privacy (i.e., privacy of personal information), which is the key privacy interest implicated by governmental use of advanced search and surveillance technologies. See generally *Dyment*, [1988] 2 S.C.R. at 429-30 (describing informational privacy).

⁹ See Richard Posner, *The Right To Privacy*, 12 GA. L. REV. 393, 406-09 (1978) [hereinafter Posner, *Right to Privacy*].

¹⁰ See Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 61-62 (1988).

¹¹ See, e.g., *R. v. Simmons*, [1988] 2 S.C.R. 495, 517 (Can.) (recognizing that invasive body cavity searches would require “greater” justification than routine pat-down and strip searches).

¹² See *Oliver v. United States*, 466 U.S. 170, 181 (1984) (stressing the need to find “a

courts have largely failed to perform this calculation with rigor, clarity, or transparency.

The intent of this Article, then, is to develop a fully instrumentalist approach to the reasonable expectation of privacy test. The obvious place to start is economic analysis. There is a flourishing literature on the law and economics of privacy. Drawing mostly from the economics of information,¹³ legal economists have taken on a wide variety of privacy issues.¹⁴ There have been few attempts, however, to apply economic insights to search and seizure law.¹⁵ This Article aims to help fill this gap. I provide an accounting of the costs and benefits of governmental privacy intrusions and propose a framework for making reasonable expectation of privacy decisions that maximize social welfare.

In contrast to the prevailing moral approach, which treats privacy as a fundamental right, the economic approach views it as a normatively neutral aspect of self-interest: the desire to conceal and control potentially damaging personal information. In this view, privacy should not be protected when its primary effect is to impede the optimal deterrence of crime. However, in other cases legal protections against governmental surveillance may enhance social welfare by encouraging productive

workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment"); *Delaware v. Prouse*, 440 U.S. 648, 654 (1979) ("[T]he permissibility of a particular law enforcement practice is judged by balancing its intrusion on . . . Fourth Amendment interests against its promotion of legitimate governmental interests."); *Camara v. Mun. Court*, 387 U.S. 523, 536-37 (1967) ("There can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."); *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 159-60 (Can.) (saying that the reasonable expectation of privacy test is an assessment "as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement"); see also Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 234-36 (1993).

¹³ See, e.g., JACK HIRSHLEIFER & JOHN G. REILY, *THE ANALYTICS OF UNCERTAINTY AND INFORMATION* (1992); INES MACHO-STADLER ET AL., *AN INTRODUCTION TO THE ECONOMICS OF INFORMATION: INCENTIVES AND CONTRACTS* (2d ed. 2001).

¹⁴ See, e.g., JACK HIRSHLEIFER, *ECONOMIC BEHAVIOUR IN ADVERSITY* 194-210 (1987); David Friedman, *Privacy and Technology*, 17 SOC. PHIL. & POL'Y 186 (2000); Posner, *Right to Privacy*, *supra* note 9; George Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623 (1980).

¹⁵ Exceptions include Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951 (2003); Hugo M. Mialon & Sue H. Mialon, *The Economics of the Fourth Amendment: Crime, Search, and Anti-Utopia* (Working Paper, 2004), available at <http://ssrn.com/abstract=591667>; Andrew Song, *Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches* (Berkman Center Research Publication No. 2003-04, Harvard Law School, Public Law Working Paper No. 73, 2003), available at <http://papers.ssrn.com/abstract=422220>.

transactions, diminishing the costs of non-legal privacy barriers, and limiting suboptimal policing practices such as discriminatory profiling and the enforcement of inefficient criminal prohibitions. Economics and public choice theory can also help to minimize decision-making error by predicting which legal actors—police, legislatures, or courts—are best placed to make optimal trade-offs between privacy and crime control.

The Article proceeds as follows. In Section II, I briefly describe the American and Canadian Supreme Courts' reasonable expectation of privacy doctrines and highlight their chief inadequacy: the indeterminacy of the "public exposure" and "intimacy" doctrines that the Courts have used to decide whether to regulate novel search technologies. Section III outlines the economic approach to the reasonable expectation of privacy test. Sections IV and V apply this approach to two novel search technologies: infrared imaging and location tracking. This analysis suggests that courts should recognize a reasonable expectation of privacy in the latter case, but not the former. Section VI concludes.

II. REASONABLE EXPECTATION OF PRIVACY DOCTRINE AND NOVEL SEARCH TECHNOLOGIES

The use of the reasonable expectation of privacy test dates from the United States Supreme Court's 1967 decision in *Katz v. United States*.¹⁶ *Katz* famously departed from the prevailing conception of Fourth Amendment searches as physical trespasses into "constitutionally-protected" areas.¹⁷ In deciding that the placement of an electronic listening and recording device outside a public telephone booth was a search, Justice Stewart declared for the majority that the Fourth Amendment protected "people, not places,"¹⁸ and the surreptitious interception of the petitioner's conversation "violated the privacy upon which he justifiably relied."¹⁹ The "reasonable expectation" phraseology, however, stems from Justice Harlan's concurring opinion. Harlan stated, in language later adopted by a majority of the Court, that to be considered a search, it must be shown both that a person "exhibited an actual (subjective) expectation of privacy and . . . that the expectation be one that society is prepared to recognize as

¹⁶ 389 U.S. 347 (1967).

¹⁷ See, e.g., *Berger v. New York*, 388 U.S. 41, 57, 59 (1967); *Lopez v. United States*, 373 U.S. 427, 438-39 (1963); *Silverman v. United States*, 365 U.S. 505, 510, 512 (1960).

¹⁸ *Katz*, 389 U.S. at 351; see also *id.* at 353 ("Once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

¹⁹ *Id.*

‘reasonable.’”²⁰ In its first decision interpreting § 8 of the Charter, the Supreme Court of Canada adopted the same approach.²¹

How, then, have courts gone about deciding what constitutes a “reasonable expectation of privacy”? This is not the place to summarize the reams of doctrine on the question.²² It will be helpful, however, to provide some sense of how the American and Canadian Supreme Courts have applied the test to novel search technologies.

Not surprisingly (and contrary to Justice Harlan’s dictum in *Katz*), courts have not considered the existence of a subjective expectation of privacy to be a necessary condition of constitutional protection;²³ otherwise, police could simply advertise their intention to monitor everything capable of being monitored.²⁴ Moreover, people who were more suspicious or aware of governmental surveillance would receive less constitutional protection than those more trusting or ignorant.²⁵ The focus has instead been on the second component of Harlan’s formula: whether an expectation of privacy is “reasonable.”

Like other reasonableness standards, on its face, the reasonable expectation of privacy test is extremely vague. Insofar as it gauges “expectations” of privacy (both subjective and objective) in relation to prevailing social and technological conditions, it is also tautological. As Wasserstrom and Seidman have put it, “Reasonable expectations are

²⁰ *Id.* at 361 (Harlan J., concurring). For examples of later cases adopting Harlan’s language, see *Oliver v. United States*, 466 U.S. 170, 177 (1984); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *United States v. Chadwick*, 433 U.S. 1, 7 (1977); *United States v. Miller*, 425 U.S. 435, 442 (1976); *United States v. Dionisio*, 410 U.S. 1, 14 (1973); *Couch v. United States*, 409 U.S. 322, 335-36 (1973); *Terry v. Ohio*, 392 U.S. 1, 9 (1968).

²¹ *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 159 (Can.) (“The guarantee of security from *unreasonable* search and seizure only protects a *reasonable* expectation.”).

²² See generally SCOTT C. HUTCHISON & JAMES C. MORTON, *SEARCH AND SEIZURE LAW IN CANADA* (1990); LAFAVE ET AL., *supra* note 4.

²³ See *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979); *R. v. Tessling*, [2004] 3 S.C.R. 432, 451-52 (Can.).

²⁴ See Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 675-76 (1988).

²⁵ Surveillance-related paranoia could thus to some extent be a self-fulfilling prophecy. See *Tessling*, [2004] 3 S.C.R. at 452 (“It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a *subjective* expectation of privacy and thereby forfeits the protection of s. 8.”); Gutterman, *supra* note 24, at 675 (“A citizen’s unfounded belief that his private activities were not protected had a ‘self-determining’ quality: the fourth amendment’s protections as he perceived them were the maximum benefit that he could obtain.”).

defined by reference to a current reality that includes the very practices under attack, rather than by reference to the kinds of expectations people would have in a normatively attractive society.”²⁶ The test’s language implies that we can expect less and less constitutional protection for privacy as technology continues to enhance the power and lower the costs of surveillance.²⁷

To be sure, courts have attempted to suffuse the test with normative content.²⁸ They have pointed out many virtues of privacy and catalogued myriad factors influencing reasonable expectation of privacy decisions. But the key conceptual tools that the courts have developed to aid these decisions—the public exposure and intimacy doctrines—have produced little jurisprudential consistency, predictability, or consensus.

A. PUBLIC EXPOSURE

The public exposure doctrine exempts from constitutional protection information voluntarily disclosed to the public. As Justice Stewart explained in *Katz*, “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”²⁹ The doctrine is a natural outgrowth of liberal moral theory. If rational, autonomous agents freely choose to expose information to the public, then they cannot complain if others use that information against them.

It seems axiomatic that information voluntarily released into the public domain cannot attract a reasonable expectation of privacy. The problem, of course, is that the meanings of “voluntary” and “public” are sometimes contestable. People frequently divulge information, for example, assuming that it will be used only for certain limited purposes.³⁰ They may also

²⁶ Wasserstrom & Seidman, *supra* note 10, at 63-64.

²⁷ See *Kyllo v. United States*, 533 U.S. 27, 47 (2001) (Stevens, J., dissenting) (considering whether a sense-enhancing technology in general public use “is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available”); *Cloud*, *supra* note 12, at 262 (“If a majority of Justices ever were to conclude that satellite technology was generally available to the public, then its use for government surveillance would not constitute a search regulated by the amendment.”); *Guterman*, *supra* note 24, at 720 (“The fourth amendment may now be defined solely by the degree of sophistication used in the surveillance and the speed by which technological advances become generally disseminated and available to the public.”).

²⁸ See, e.g., *Tessling*, [2004] 3 S.C.R. at 452 (“Expectation of privacy is a normative rather than a descriptive standard.”).

²⁹ *Katz v. United States*, 389 U.S. 347, 351 (1967) (citation omitted).

³⁰ See *R. v. Buhay*, [2003] 1 S.C.R. 631, 642 (Can.); *R. v. Dyment*, [1988] 2 S.C.R. 417,

subject themselves to observation assuming that their identities will likely remain anonymous. But what happens when technological search tools upend these assumptions? Can we still say that there has been a voluntary exposure?

Judges have given divergent answers to these questions. For example, the American and Canadian Supreme Courts have differed on the question of whether the electronic interception of speech constitutes a “search” when one of the speakers is an undercover police informant. As discussed, the United States Supreme Court established in *Katz* that surreptitious interceptions of private communications are Fourth Amendment searches. Soon after, however, it decided that when one of the communicators is aware of the interception, *Katz* does not apply.³¹ In *United States v. White*, the Court held that if the law “gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State’s case.”³²

The Supreme Court of Canada has taken a different approach. Following *Katz*, it has unsurprisingly ruled that the surreptitious electronic interception of private communications invades a reasonable expectation of privacy.³³ But in *R. v. Duarte*, it rejected the “risk analysis” of *White* and held that participant surveillance also constitutes a § 8 search.³⁴ Writing for the Court, Justice La Forest asserted that while § 8 does not protect people from the risk that their confidants will turn out to be informers, it does prohibit the State from arbitrarily making a “permanent electronic record”

429-30 (Can.).

³¹ *United States v. White*, 401 U.S. 745 (1971) (plurality opinion) (holding that there was no expectation of privacy when a defendant communicates with an informant surreptitiously carrying a “wire” transmitting conversations to police). *White* therefore confirmed the vitality of the Court’s pre-*Katz* jurisprudence on participant intercepts. *See also Lopez v. United States*, 373 U.S. 427 (1963) (concluding that there was no Fourth Amendment search where a government agent records a conversation with the suspect with a concealed electronic device); *On Lee v. United States*, 343 U.S. 747 (1954) (ruling that there was no Fourth Amendment search where the suspect’s conversations with an undercover agent were transmitted to other agents via a concealed radio transmitter).

³² *Lopez*, 373 U.S. at 752.

³³ *See R. v. Thompson*, [1990] 2 S.C.R. 1111, 1136-37 (Can.); *R. v. Wiggins*, [1990] 1 S.C.R. 62 (Can.); *R. v. Duarte*, [1990] 1 S.C.R. 30, 42 (Can.) (“[S]urreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s. 8 of the Charter.”).

³⁴ *Duarte*, [1990] 1 S.C.R. at 42. In so doing, the Court struck down what was then § 178.11 of the Canada Criminal Code, R.S.C., ch. C 46 (1985), which exempted participant surveillance from the prohibition against warrantless electronic surveillance. *Duarte*, [1990] 1 S.C.R. at 42.

of their conversations.³⁵ The Court similarly held in *R. v. Wong* that surreptitious video surveillance (without audio interception) invades a reasonable expectation of privacy.³⁶

Similar differences have arisen over whether it invades a reasonable expectation of privacy to follow a suspect's vehicle over public roads using a surreptitiously-planted, radio-frequency tracking device. In *United States v. Knotts*, the United States Supreme Court held that it did not.³⁷ This type of surveillance, the Court reasoned, revealed no more information than could have been obtained through visual surveillance of the vehicle from public vantage points. "Nothing in the Fourth Amendment," then-Justice Rehnquist wrote, "prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them"³⁸ In *United States v. Karo*, however, the Court decided that the Fourth Amendment is engaged when beepers are used to track items within private residences.³⁹ Unlike in *Knotts*, the Court noted, the beeper in *Karo* was used "to obtain information that it could not have obtained by observation from outside the curtilage of the house."⁴⁰

Though it seemed reluctant to do so, the Supreme Court of Canada concluded in *R. v. Wise* that the use of a beeper to monitor a vehicle on public roads invaded a reasonable expectation of privacy.⁴¹ The Court declared, however, that the invasion of privacy was minimal.⁴² "This particular beeper," the majority stated, "was a very rudimentary extension of physical surveillance."⁴³

³⁵ *Duarte*, [1990] 1 S.C.R. at 48. Note however that § 8 of the Charter is not violated when someone privy to an illegally recorded communication (such as an undercover agent wearing a "wire") testifies at trial as to their recollection of the communication, even if the participant's memory has been refreshed by reference to the tainted recording. But § 8 is violated when portions of an illegally obtained recording or transcript that a witness does not recall are adduced in evidence. See *R. v. Fliss*, [2002] 1 S.C.R. 535 (Can.).

³⁶ *R. v. Wong*, [1990] 3 S.C.R. 36 (Can.) (holding that when police placed a hidden video camera in the wall of the suspects' hotel room, they violated a reasonable expectation of privacy).

³⁷ *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) (holding that when police attached a beeper to a chemical container that the suspect subsequently placed in his vehicle, the police violated a reasonable expectation of privacy).

³⁸ *Id.* at 283.

³⁹ *United States v. Karo*, 468 U.S. 705 (1984).

⁴⁰ *Id.* at 715.

⁴¹ *R. v. Wise*, [1992] 1 S.C.R. 527, 538 (Can.).

⁴² *Id.* at 534-36.

⁴³ *Id.* at 535. Notably, the Crown had conceded that the installation of the beeper violated § 8. *Id.* at 532, 538. Not surprisingly, the Canadian Supreme Court concluded that despite the violation, the trial judge should not have excluded evidence obtained from the beeper. *Id.* at 539-48. The Court also recommended the passage of legislation authorizing

There has also been disagreement on whether a reasonable expectation of privacy exists in relation to the non-content “envelope” information accompanying electronic communications.⁴⁴ In *Smith v. Maryland*, the United States Supreme Court ruled that the installation and use of a “pen register,” which records the numbers dialed from a telephone, did not invade a reasonable expectation of privacy.⁴⁵ The Court noted that the register did not record the content of conversations and suggested that people are aware that the numbers they dial may be recorded for commercial and law enforcement purposes.⁴⁶ In any event, it concluded, any expectation of privacy was not reasonable, as a person has “no legitimate expectation of privacy in information he voluntarily turns over to third parties.”⁴⁷ In Canada, in contrast, several lower courts have found that people have a reasonable expectation of privacy with respect to telephone envelope information, so warrants to seize it must be based on probable cause.⁴⁸

tracking warrants and hinted that a “lower standard” of suspicion would be sufficient to justify them. *Id.* at 548-49. As discussed *infra* note 143, Parliament subsequently enacted a provision authorizing the issuance of tracking warrants on the basis of reasonable suspicion.

⁴⁴ “Envelope” information refers to addressing and other information attached to a communication that is the functional equivalent of the information contained on the outside of a letter mail envelope. See Orin Kerr, *Internet Surveillance After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611-16 (2003) [hereinafter Kerr, *Internet Surveillance*].

⁴⁵ *Smith v. Maryland*, 442 U.S. 735 (1979). It is implicit in the Court’s decision that “trap and trace” devices, which record the numbers associated with incoming telephone calls, do not invade a reasonable expectation of privacy. See *S. Bell Tel. & Tel. Co. v. Hamm*, 409 S.E.2d 775, 780 (S.C. 1991) (“In light of the holding in *Smith*, we cannot hold that the telephone number of the equipment from which a call has been placed is entitled to more privacy than the telephone numbers called by someone.”).

⁴⁶ *Smith*, 442 U.S. at 742.

⁴⁷ *Id.* at 743-44. The Supreme Court of Canada has not considered communications envelope data. Before 1993, most lower Canadian courts had followed the United States Supreme Court in holding that the seizure of such data did not invade a reasonable expectation of privacy. See *R. v. Sampson*, [1983] 45 Nfld. & P.E.I.R. 32 (Nfld. C.A.) (Can.); *R. v. Fegan*, [1993] 13 O.R.3d 88 (Ont. C.A.) (Can.). In 1993, Parliament enacted a warrant provision authorizing such seizures on the basis of reasonable suspicion. See *infra* note 142-145 and accompanying text.

⁴⁸ See *R. v. Nguyen*, [2004] B.C.J. No. 248 ¶ 51 (B.C. S.C.) (Can.) (use of reasonable suspicion warrant to obtain a record of outgoing and incoming telephone numbers from the defendant’s mobile phone violated § 8); *R. v. Hackert*, [1997] O.J. No. 6384 (Ont. Gen. Div.) (Can.) (holding that the Criminal Code provision authorizing reasonable suspicion warrants for telephone envelope information violates § 8).

B. INTIMACY

As its name suggests, the intimacy doctrine holds that searches revealing sensitive personal information are more likely to trigger a reasonable expectation of privacy than those uncovering only mundane information. Like the public exposure doctrine, the intimacy doctrine is intuitively appealing.⁴⁹ People are less concerned about disclosing routine details of their daily lives than potentially stigmatizing information, such as views or activities relating to sexuality, politics, or religion. And like the public exposure doctrine, the intimacy doctrine derives from liberal moral philosophy. For liberal privacy theorists, intimate information is more central to autonomy, identity, and personality than non-intimate information.⁵⁰

But as legal economists have pointed out, intimate information is not self-evidently deserving of legal protection.⁵¹ Under competitive conditions, there is no reason to protect one party's ability to conceal private information. In voluntary transactions (whether economic or social), the parties' preferences for knowledge and privacy should generate the disclosure of the efficient amount of information.⁵² Granting legal protection for the concealment of discreditable (but truthful) information is inefficient because it increases the cost of productive transactions. If it is inefficient to protect sellers' ability to misrepresent the quality of their goods, then it is equally inefficient to protect people's ability to misrepresent their character to others.⁵³ By limiting our ability to discern others' characters, trustworthiness, and other attributes, privacy either increases the cost of or deters productive economic and social interactions.

It is inappropriate, some might argue, to analogize the state's attempt to obtain personal information to the sale of goods between private parties. But the case for protecting intimate, private information from governmental scrutiny rests on the same ground as in private transactions. While the capacity of government to cause harm by collecting personal information is great, so is the people's capacity to cause harm by concealing it. More

⁴⁹ See generally *R. v. Mills*, [1999] 3 S.C.R. 668, 722 (Can.) (“[P]rivacy concerns are at their strongest where aspects of one’s individual identity are at stake, such as in the context of information ‘about one’s lifestyle, intimate relations or political or religious opinions.’”).

⁵⁰ See, e.g., Bloustein, *supra* note 6; Gavison, *supra* note 6, at 444-45; Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 SETON HALL L. REV. 371 (2003); Jeffrey Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26 (1977); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

⁵¹ See Stigler, *supra* note 14, at 627.

⁵² Posner, *Right to Privacy*, *supra* note 9, at 399-400; Stigler, *supra* note 14, at 627.

⁵³ See Posner, *Right to Privacy*, *supra* note 9, at 399-400.

crime is the inevitable consequence of inhibiting the government's ability to uncover discreditable, private information. However, as discussed in detail below, allowing police to obtain personal information by certain *means* may sometimes generate suboptimal outcomes; for example, unrestricted wiretapping might inhibit communication or induce wasteful spending on measures to protect privacy. In such cases, it may be efficient to regulate investigative methods that invade privacy. This suggests that in determining the constitutionality of a novel search technique, courts should focus on the methods used by police rather than the nature of the information those methods reveal. In most cases, this is precisely what the law does. When police can demonstrate sufficient grounds for suspicion, they are permitted to collect highly intimate information.⁵⁴

Of course, courts use the reasonable expectation of privacy test to determine whether police can search in the absence of such a demonstration. In such cases, it could be argued that gauging the intimacy of the information revealed by a search technique helps predict whether regulating the technique would prevent inefficient behavioral responses.

In practice, however, measuring the inherent intimacy of information has proven to be exceedingly difficult. Courts have come to varying conclusions, for example, on the question of whether a reasonable expectation of privacy is invaded when information normally contained in constitutionally protected areas (such as residences, vehicles, or luggage) is extracted by "sense-enhancing" technologies. Before and after *Katz*, the United States Supreme Court ruled that the use of flashlights and telescopic lenses does not constitute a Fourth Amendment search.⁵⁵ In *California v. Ciraolo*, the Court came to the same conclusion with respect to the visual observation of property from the air (with either the untrained eye or cameras), so long as the airspace is "public[ly] navigable," and the search is "in a physically nonintrusive manner."⁵⁶ The *Ciraolo* Court reasoned that

⁵⁴ See *infra* notes 82-91 and accompanying text.

⁵⁵ See *United States v. Dunn*, 480 U.S. 294, 303 (1987) (upholding the police use of a flashlight from an "open field" vantage point to illuminate a barn's interior); *Texas v. Brown*, 460 U.S. 730, 739-40 (1983) (ruling that the police use of a flashlight to illuminate a portion of an automobile interior open to plain sight is not a search); *United States v. Lee*, 274 U.S. 559, 563 (1927) ("[U]se of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution.").

⁵⁶ *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (approving the police's unaided visual surveillance from 1000 feet of a backyard enclosed by high double fences); see also *Florida v. Riley*, 488 U.S. 445 (1989) (upholding the police's unaided visual surveillance of a partially-covered greenhouse from 400 feet); *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986) (allowing the police's use of high-resolution mapping camera at 12,000, 3,000, and 1,200 feet to photograph industrial facilities shielded from ground-level observation). As the *United States v. Kyllo* majority noted, the only one of these cases in which police used a

activities that are “clearly visible” from a “public vantage point” are not protected by the Fourth Amendment.⁵⁷ It warned, however, that it might decide differently where observations are made with “modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens”⁵⁸ or “highly sophisticated surveillance equipment not generally available to the public, such as satellite technology.”⁵⁹

The Court heeded this warning in *Kyllo v. United States*, where a narrow majority ruled that the police violated the Fourth Amendment by using an infrared camera to detect heat radiating from a residential marijuana growing operation, despite the fact that the device was not physically penetrating and showed only crude images of relatively warmer and cooler areas.⁶⁰ “[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’” Justice Scalia wrote, “constitutes a search—at least where (as here) the technology in question is not in general public use.”⁶¹ The Court came to a different conclusion in two cases where police used drug sniffing dogs to detect narcotics concealed in airport luggage⁶² and the trunk of a vehicle.⁶³ Such searches are relatively non-intrusive, the Court concluded, and reveal no information other than the presence of contraband.⁶⁴

The Supreme Court of Canada has not yet dealt with either visual aerial surveillance or drug sniffing dogs. Lower courts, however, have typically rejected the American approach and found a reasonable expectation of privacy.⁶⁵ But in *R. v. Tessling*,⁶⁶ the Supreme Court

technological aid to the naked eye, *Dow*, involved surveillance of commercial buildings—not a private residence. *United States v. Kyllo*, 533 U.S. 27, 33 (2001).

⁵⁷ *Ciraolo*, 476 U.S. at 213.

⁵⁸ *Id.* at 215 n.3 (quoting Brief of Petitioner at 14-15, *Ciraolo*, 476 U.S. 207 (No. 84-1513)).

⁵⁹ *Dow*, 476 U.S. at 238.

⁶⁰ *Kyllo*, 533 U.S. at 30. I discuss *Kyllo* in detail *infra* notes 151-165 and accompanying text.

⁶¹ *Id.* at 34 (citations omitted).

⁶² *United States v. Place*, 462 U.S. 696, 707 (1983).

⁶³ *Illinois v. Caballes*, 543 U.S. 405, 409-10 (2005).

⁶⁴ *See id.*; *Place*, 462 U.S. at 707.

⁶⁵ *See R. v. Lam*, [2003] 178 C.C.C.3d 59, 69-72 (Alta. C.A.) (Can.) (concluding that a sniff of luggage and luggage locker at bus terminal by a trained dog invades a reasonable expectation of privacy); *R. v. Cook*, [1999] A.B.Q.B. 351 ¶¶ 55-62 (Alta. Q.B.) (Can.) (ruling that the unaided visual surveillance of a residential lot from 50-100 (but not 1,000) feet invades a reasonable expectation of privacy); *R. v. Kelly*, [1999] 169 D.L.R. (4th) 720, 735-37 (N.B. C.A.) (Can.) (holding that the unaided aerial surveillance of residential garden

unanimously held (on the same facts as *Kyllo*) that warrantless infrared camera searches did not violate § 8 of the Charter. “[H]eat distribution,” Justice Binnie stated, “offers no insight into [the suspect’s] private life, and reveals nothing of his ‘biographical core of personal information.’”⁶⁷

The limitations of the intimacy doctrine have also been exposed in a line of cases dealing with searches of third party information databases. In *United States v. Miller*, the United States Supreme Court held that prosecutors invaded no reasonable expectation of privacy when they subpoenaed a suspect’s banking records.⁶⁸ The records contained only “information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”⁶⁹ “The depositor takes the risk, in revealing his affairs to another,” the Court reasoned, “that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”⁷⁰

The Supreme Court of Canada has not dealt definitively with banking records, though some of its members have suggested that they do attract a reasonable expectation of privacy.⁷¹ Lower courts have come to varying conclusions.⁷² The Supreme Court has decided, however, that no reasonable expectation of privacy was invaded when police obtained a

from any altitude invades a reasonable expectation of privacy).

⁶⁶ [2004] 3 S.C.R. 432 (Can.). I discuss *Tessling* in detail *infra* notes 151-165 and accompanying text.

⁶⁷ *Id.* ¶ 63 (citing *R. v. Plant*, [1993] 3 S.C.R. 281, 293 (Can.)).

⁶⁸ *United States v. Miller*, 425 U.S. 435 (1976).

⁶⁹ *Id.* at 442.

⁷⁰ *Id.* at 443 (citing *United States v. White*, 401 U.S. 765, 751-52 (1971)).

⁷¹ In *Schreiber v. Canada (Attorney General)*, the Supreme Court of Canada considered whether the seizure of a suspect’s foreign banking records violated § 8 of the Charter. [1998] 1 S.C.R. 841 (Can.). The majority concluded that the Canadian government’s request for foreign assistance did not engage § 8; it declined to consider whether a warrantless search of a suspect’s domestic banking records would have attracted a reasonable expectation of privacy. *Id.* In his concurrence, Chief Justice Lamer indicated that he would have answered “yes” to this question. *Id.* ¶ 22 (Lamer, C.J., concurring). In his dissent, Justice Iacobucci concluded that the suspect did have a reasonable expectation of privacy in his foreign banking records. *Id.* ¶ 55 (Iacobucci, J., dissenting).

⁷² See *R. v. Eddy*, [1994] 119 Nfld. & P.E.I.R. 91 ¶¶ 183-84 (Nfld. S.C.) (Can.) (holding that a police inquiry as to the owner of a bank account and whether any transactions had occurred on a particular date invaded a reasonable expectation of privacy); *R. v. Lillico*, [1994] 92 C.C.C.3d 90 (Ont. Gen. Div.) (Can.) (holding that a police request for information with respect to a single check and subsequent account activity did not invade reasonable expectation of privacy).

suspect's electrical consumption records from the local utility.⁷³ "Such records," Justice Sopinka wrote, do not invade that "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."⁷⁴ The records, he reasoned, "cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence."⁷⁵

III. THE ECONOMIC APPROACH

Can economics point the way to a more determinate and normatively satisfying approach to the reasonable expectation of privacy test? As mentioned, economists typically view privacy as an aspect of rational self-interest.⁷⁶ They posit that privacy permits people to conceal (discreditable) personal information that might be used to their disadvantage.⁷⁷ It is in people's interest to maximize this ability, selectively disclosing (and thereafter controlling) their personal information to achieve desired ends.⁷⁸ This, however, is not always in society's interests.⁷⁹ If privacy in a particular realm is used chiefly to conceal socially harmful conduct (such as crime), then legal protection for privacy in that realm should be weak and police should be given broad search powers. If, on the other hand, privacy encourages efficient behaviors, then legal protections should be strong and police powers should be limited. Courts applying the reasonable expectation of privacy test to an investigative technique should thus identify

⁷³ R. v. Plant, [1993] 3 S.C.R. 281 (Can.).

⁷⁴ *Id.* at 293.

⁷⁵ *Id.*

⁷⁶ See Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SECURITY & PRIVACY 26, 26 (2005).

⁷⁷ See Richard Epstein, *Deconstructing Privacy: And Putting it Back Together Again*, 17 SOC. PHIL. & POL'Y 1, 12-14 (2000); Posner, *Right to Privacy*, *supra* note 9, at 399; Charles M. Kahn et al., *A Theory of Transactions Privacy 2* (Fed. Reserve Bank of Atlanta, Working Paper No. 2000-22, 2000), available at <http://fic.wharton.upenn.edu/fic/papers/01/0112.pdf>; see also Allen, *supra* note 7, at 872. Empirical evidence has indicated that group members' concern for privacy increases in relation to the degree to which they perceive that their characteristics (such as age and weight) deviate from the group's norm. See Bernardo Huberman et al., *Valuating Privacy*, 3 IEEE SECURITY & PRIVACY 22 (2005), available at <http://www.hpl.hp.com/research/idl/papers/deviance/deviance.pdf>.

⁷⁸ See James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 U. TORONTO L.J. 183, 188 (2004).

⁷⁹ See Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 251 (2004).

and weigh the costs and benefits of limiting the state's ability to obtain information about criminal suspects.

A. PRIVACY COSTS

The costs of privacy are the easiest to discern. By thwarting the detection and punishment of criminals, legal privacy protections generate two types of social costs. First, most crimes are inefficient,⁸⁰ so privacy laws detract from social welfare by diminishing the deterrence of crime. For example, if police cannot use electronic surveillance to acquire evidence that would support an application to obtain a warrant to physically search a suspected drug dealer's home, and there is no other equally effective investigative technique available, fewer physical searches will occur, diminishing the probability of punishment and thus the expected cost of dealing drugs. Drug dealing will thus become a more attractive endeavor. Second, by restricting the use of particular search techniques, privacy laws may force authorities to use more costly substitutes.⁸¹ For example, if police replace electronic surveillance with undercover informants, law enforcement costs may rise, as undercover operations are very likely more expensive and dangerous than electronic surveillance.

B. PRIVACY BENEFITS

Though privacy's social benefits are somewhat more obscure, they are by no means insignificant. While privacy makes it easier for people to engage in antisocial conduct (including crime), it may also provide an incentive for productive activity.⁸² Privacy may thus reduce "avoidance costs"; that is, the opportunity cost of forgoing socially beneficial transactions due to the fear of disclosure of information that could be used against those that disclose. There are two types of avoidance costs that privacy laws can mitigate. First, privacy enhances the quantity and quality of interpersonal communications. For example, legal restrictions on eavesdropping (by police or nosy neighbors) free people to communicate more candidly.⁸³ Privacy diminishes the risk that the information that we

⁸⁰ See generally ROBERT COOTER & THOMAS ULEN, *LAW AND ECONOMICS* 443 (3d ed. 2000).

⁸¹ See Stigler, *supra* note 14, at 628-29.

⁸² See Song, *supra* note 15, at 3.

⁸³ See Epstein, *supra* note 77, at 9; Charles J. Hartmann & Stephen M. Renas, *Anglo-American Privacy Law: An Economic Analysis*, 5 *INT'L REV. L. & ECON.* 133, 145 (1985); Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 *BUFF. L. REV.* 1, 17 (1979) [hereinafter Posner, *Privacy, Secrecy, and Reputation*]; Posner, *Right to Privacy*, *supra* note 9, at 401-03. For a similar argument articulated in non-economic terms, see Amsterdam,

rationally disclose to intended recipients will be obtained (and used to our detriment) by unintended recipients.⁸⁴ Conversely, widespread eavesdropping causes people to be more formal and guarded in their communications—not only in relation to criminal conversations, but also those revealing discreditable (but non-criminal) information.⁸⁵ As Richard Posner states, the “principal effect of allowing eavesdropping would not be to make the rest of society more informed about the individual but to make conversations more cumbersome and less effective.”⁸⁶ This helps to explain why legal protections against invasions of communicative privacy are so robust.⁸⁷

Second, privacy (in the form of anonymity) may encourage people to participate in beneficial activities that they would not engage in otherwise.⁸⁸

supra note 24, at 388.

⁸⁴ The benefits of privacy in promoting productive activity are magnified when the activity produces external benefits. Communication is especially likely to generate positive externalities. Information revealed under the cloak of privacy in pursuit of self-interest may also be highly valuable to the intended recipients of that information. But if the absence of privacy means that the marginal private cost of revealing the information is greater than the private benefit, the information will not be disclosed, and the external benefits will not materialize. See Peter H. Huang, *The Law and Economics of Consumer Privacy Versus Data Mining* (Working Paper, 1998), available at <http://ssrn.com/abstract=94041>; Song, *supra* note 15, at 11-12.

Another benefit of privacy (more relevant in the case of private transactions than governmental surveillance) is that it can increase the amount of socially productive information. In the absence of privacy, there would be little incentive for people to invest in obtaining valuable information, since this information would be easily obtainable. This is the economic justification for the law of confidentiality, which provides contractual and tort remedies for disclosures of information imparted in confidence. See, e.g., Ejan Mackaay, *Economic Incentives in Markets for Information and Innovation*, 13 HARV. J.L. & PUB. POL'Y 867 (1990). I am indebted to Norman Siebrasse for this insight.

⁸⁵ See *R. v. Fliss*, [2002] 1 S.C.R. 535, 555 (Can.) (“In a free country, social discourse should not be inhibited by a concern that conversations are being secretly recorded and transcribed without lawful independent prior authorization.”); *R. v. Duarte*, [1990] 1 S.C.R. 30, 50 (Can.) (“Few of us would ever speak freely if we knew that all our words were being captured by machines for later release before an unknown and potentially hostile audience. No one talks to a recorder as he talks to a person.”).

⁸⁶ Posner, *Privacy, Secrecy, and Reputation*, *supra* note 83, at 18; see also Posner, *Right to Privacy*, *supra* note 9, at 403.

⁸⁷ See *R. v. Wong*, [1990] 3 S.C.R. 36, 47 (Can.); *R. v. Thompson*, [1990] 2 S.C.R. 1111 (Can.); *R. v. Wiggins*, [1990] 1 S.C.R. 62 (Can.); *Duarte*, [1990] 1 S.C.R. 30; see also Canada Criminal Code, R.S.C., ch. C 46 § 184(1) (1985) (criminalizing the willful interception of private electronic communications).

⁸⁸ This goal might also be furthered by restricting law enforcement’s ability to disclose information that it has collected for reasons unrelated to the furtherance of criminal investigations and prosecutions. See William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2183-85 (2002) [hereinafter Stuntz, *Local Policing*].

This is a social benefit that must be measured against privacy's impact in facilitating crime. If teenagers were required to provide proof of identity before purchasing condoms, for example, sexually transmitted diseases and unwanted pregnancies would become more prevalent. Similarly, the placement of video surveillance cameras in a high-crime neighborhood could dissuade people from using nearby needle exchanges or AIDS clinics.

Privacy laws may also reduce the costs associated with protecting privacy by non-legal means: defensive costs.⁸⁹ Instead of avoiding communications or activities that could reveal personal information, people may wastefully expend resources to protect their privacy.⁹⁰ Without wiretapping laws, for example, people would be more likely to use public payphones instead of their own phones.

In the absence of legal privacy protections, the likelihood that people will employ non-legal substitutes depends on both the price of those substitutes and the elasticity of the demand for privacy. This insight may help us decide when it is cost-justified to regulate governmental surveillance. Suppose that there were no law limiting police's ability to intercept or search e-mail communications. People using e-mail for non-criminal purposes could rationally conclude that the marginal private benefit of encrypting e-mail is lower than its cost.⁹¹ Such persons would suffer the costs incurred by either exposing sensitive information or using more costly methods of communication. The marginal private benefit of using encryption for criminal purposes, in contrast, would in most cases be higher than for non-criminal purposes. Criminals are consequently more likely to use encryption to thwart governmental surveillance than non-criminals. In these circumstances, regulating the state's ability to obtain e-mail communications is likely to reduce non-criminals' avoidance costs without substantially diminishing the deterrence of crime.

So far I have been discussing the value of privacy in fostering socially productive *non-criminal* discourse and activity. I have assumed that there is no value in protecting people against governmental intrusions revealing *criminal* behavior. This assumption can be questioned. Where there is a

⁸⁹ Friedman, *supra* note 14, at 192-93; Song, *supra* note 15, at 15-16.

⁹⁰ See United States v. Dunn, 480 U.S. 294, 319 (Brennan, J., dissenting); Amsterdam, *supra* note 24, at 403 ("The question is not whether you or I must draw the blinds before we commit a crime. It is whether you and I must discipline ourselves to draw the blinds every time we enter a room, under pain of surveillance if we do not.").

⁹¹ These include material costs, such as adoption and usage costs, as well as immaterial costs, such as learning and switching costs as well as any social stigma associated with using privacy-protecting technologies. See Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, in THE ECONOMICS OF INFORMATION SECURITY 165 (L. Jean Camp & Stephen Lewis eds., 2004).

strong consensus that the harms caused by a type of crime are severe, we should be willing to tolerate the use of fairly intrusive investigative methods as a means of deterrence,⁹² provided that productive non-criminal behavior is not unduly chilled. Privacy invasions are less acceptable, however, when this consensus is not as strong, as is arguably the case for many “consensual” crimes like drug trafficking, prostitution, and gambling.⁹³ In economic terms, enforcing these prohibitions (or enforcing them through privacy-invasive techniques) may be inefficient, as enforcement costs may outweigh the harms generated by the prohibited activities.⁹⁴ In some cases, therefore, legal privacy protections may help to limit the enforcement of bad laws.

Privacy laws may also help to prevent governments from discriminating against disfavored minorities.⁹⁵ Broad, discretionary investigative powers are more likely to be used against those disadvantaged by poverty, race, or ethnicity than powers constrained by the requirements of prior authorization and probable cause.⁹⁶ These requirements increase the likelihood that searches will be based on concrete, individualized suspicion—not discriminatory stereotypes.

But what exactly is discriminatory stereotyping? Economists distinguish between “biased” profiling (based on animus towards members of a minority group) and “statistical” profiling (arising from the disproportionate targeting of group members based on an accurate assessment of that group’s offending rate).⁹⁷ If group members are more likely to commit a particular offense than people in the general population, then many economists would say that it is legitimate to consider group membership in deciding whom to investigate.⁹⁸ If, on the other hand,

⁹² See Friedman, *supra* note 14, at 200; Posner, *Privacy, Secrecy, and Reputation*, *supra* note 83, at 52-53.

⁹³ See Gavison, *supra* note 6, at 452-53; Posner, *Privacy, Secrecy, and Reputation*, *supra* note 83, at 53. In earlier times, criminal laws prohibiting alcohol trafficking, abortion, homosexual intercourse, contraception, and miscegenation could have been added to this list.

⁹⁴ See Darryl K. Brown, *Cost-Benefit Analysis in Criminal Law*, 92 CAL. L. REV. 323, 352 (2004) (writing that a cost-benefit analysis “is likely to suggest that for many crime problems, criminal law is a suboptimal or poor choice”).

⁹⁵ See Amsterdam, *supra* note 24, at 415.

⁹⁶ See Wasserstrom & Seidman, *supra* note 10, at 94.

⁹⁷ See Vani K. Borooah, *Economic Analysis of Police Stops and Searches: A Reply*, 18 EUR. J. POL. ECON. 607 (2002); Shanti P. Chakravarty, *Economic Analysis of Police Stops and Searches: A Critique*, 18 EUR. J. POL. ECON. 597 (2002). Statistical discrimination is sometimes referred to as “rational” discrimination. See Jeff Dominitz, *How Do the Laws of Probability Constrain Legislative and Judicial Efforts to Stop Racial Profiling?*, 5 AM. L. & ECON. REV. 412, 413 (2003).

⁹⁸ See John Donohue, *The Law and Economics of Antidiscrimination Law*, in HANDBOOK

offense rates for a particular crime are equal as between groups, then it is likely that any inter-group disparity in arrest rates reflects bias against the group with the higher arrest rate.⁹⁹

Which of these scenarios is closer to reality? Numerous studies have shown that in many places in the United States, police are more likely to stop and search African American and Hispanic drivers than white drivers.¹⁰⁰ Explanations for this disparity vary. Some researchers argue that for offenses typically associated with “racial profiling,”¹⁰¹ minority and majority offending rates are generally similar; they conclude therefore that any disproportionate targeting of minorities indicates bias.¹⁰² However, many of the studies showing disproportionate stop rates have also found that majority and minority “hit” rates (the ratio of successful to unsuccessful searches) are very similar. Some have argued that this is

OF LAW AND ECONOMICS (A. M. Polinsky & Steven Shavell eds., 2005), available at <http://ssrn.com/abstract=763486>.

⁹⁹ We might say that police who engage in biased profiling have a “taste” for discrimination; that is, the private cost to them of searching minority suspects is lower than for searching white suspects. See generally GARY S. BECKER, ACCOUNTING FOR TASTES (1996); GARY S. BECKER, THE ECONOMICS OF DISCRIMINATION (1957).

¹⁰⁰ In the United States, many law enforcement agencies record the race of targeted suspects. See Brandon Garrett, *Remedying Racial Profiling*, 33 COLUM. HUM. RTS. L. REV. 41, 81-83 (2001); Katheryn K. Russell, *Racial Profiling: A Status Report of the Legal, Legislative, and Empirical Literature*, 3 RUTGERS RACE & L. REV. 6, 68-71 (2001). For the most recent data, see Northeastern University, Data Collection Resource Center, <http://www.racialprofilinganalysis.neu.edu> (last visited Apr. 21, 2007). Most studies of racial profiling have focused on highway traffic stops. See DAVID A. HARRIS, PROFILES IN INJUSTICE: WHY RACIAL PROFILING CANNOT WORK 62-64 (2002); Samuel R. Gross & Katherine Y. Barnes, *Road Work: Racial Profiling and Drug Interdiction on the Highway*, 101 MICH. L. REV. 651 (2002); David Rudovsky, *Law Enforcement by Stereotypes and Serendipity: Racial Profiling and Stops and Searches Without Cause*, 3 U. PA. J. CONST. L. 296 (2001). On a particular stretch of I-95 in Maryland, for example, African Americans are nearly ten times more likely to be stopped than whites. See Dominitz, *supra* note 97, at 417. There is also evidence that minorities are disproportionately targeted by police in many other types of investigations. See generally BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING 173-75 (2001).

Canadian police forces do not typically keep statistics on the basis of race or ethnicity; thus, there has been little in the way of rigorous empirical analysis of profiling in Canada. There is evidence, however, that at least some Canadian police forces disproportionately target certain racial groups, especially African Canadians. See COMM’N ON SYSTEMIC RACISM IN THE ONT. CRIMINAL JUSTICE SYS., REPORT 358 (1995).

¹⁰¹ I use the phrase “racial” or “ethnic” profiling to mean the taking of individuals’ race or ethnicity into account in deciding whether to investigate them, leading to the disproportionate targeting of members of that group in relation to their numbers in the relevant population. Profiling may thus be a result of either biased or statistical discrimination.

¹⁰² See HARRIS, *supra* note 100.

consistent with legitimate statistical discrimination based on higher minority offending rates.¹⁰³

Despite the ambiguity of the American data and the dearth of Canadian evidence, there are good reasons to think that biased profiling is widespread in both countries, and that it likely generates significant social costs that in most cases outweigh any concomitant benefits. There is strong evidence, for example, that police in several U.S. states search Hispanic motorists much more frequently than can be explained by statistical discrimination.¹⁰⁴ And rigorously designed psychological experimentation has shown that racial, ethnic, and gender stereotyping are pervasive and insidious.¹⁰⁵ This

¹⁰³ This assumes drivers who face a higher probability of being searched will be less likely to carry contraband. It assumes, in other words, that the relationship between policing and offending is elastic. It follows that when faced with higher hit rates for minority suspects, unbiased police will disproportionately target minorities until hit rates equalize. Data from Maryland, for example, reveal that while African American drivers are many times more likely to be searched than whites, African American and white hit rates are very similar. See John Knowles et al., *Racial Bias in Motor Vehicle Searches: Theory and Evidence*, 109 J. POL. ECON. 203, 219-22 (2001) (analysis of Maryland statistics that shows similar hit rates for searches of African American and white drivers but lower hit rates for Hispanics); see also Vani K. Borooah, *Racial Bias in Police Stops and Searches: An Economic Analysis*, 17 EUR. J. POL. ECON. 17, 35 (2001) (English study finding little disparity in success rates for searches of different racial groups); Rubén Hernández-Murillo & John Knowles, *Racial Profiling or Racist Policing?: Bounds Tests in Aggregate Data*, 45 INT'L ECON. REV. 959 (2004) (analysis of hit rates in Missouri for discretionary and non-discretionary searches that shows strong evidence of bias against Hispanics and weaker evidence of bias against African Americans); Jeff Dominitz & John Knowles, *Crime Minimization and Racial Bias: What Can We Learn From Police Search Data?* (Penn Institute for Economic Research, Working Paper No. 05-019, 2005), available at <http://ssrn.com/abstract=719981> (summarizing other recent hit rate analyses).

Dominitz demonstrates that if the hit rate theory is correct, then it would be impossible to simultaneously equalize rates (as between racial groups) of apprehending the guilty and detaining the innocent. See Dominitz, *supra* note 97, at 423-24. Policymakers, in other words, would have to choose between ending the disproportionate searching of innocent minority drivers and ensuring that guilty minority drivers are as likely to be caught as whites. See *id.* at 423-24.

¹⁰⁴ See Hernández-Murillo & Knowles, *supra* note 103; Knowles et al., *supra* note 103, at 219-22.

¹⁰⁵ The psychological dynamics of racial and other forms of stereotyping, which are often deployed subconsciously and reflexively, are described by Jerry Kang in *Trojan Horses of Race*, 118 HARV. L. REV. 1489, 1499-1520 (2004). Kang summarizes recent social cognition research as follows:

There is now persuasive evidence that implicit bias against a social category . . . predicts disparate behavior toward individuals mapped to that category. This occurs notwithstanding contrary explicit commitments in favor of racial equality. In other words, even if our sincere self-reports of bias score zero, we would still engage in disparate treatment of individuals on the basis of race, consistent with our racial schemas. Controlled, deliberative, rational processes are not the only forces guiding our behavior. That we are not even aware of, much less intending,

research supports the growing recognition among jurists, especially in Canada, that racial bias (including biased investigative profiling) is an endemic feature of the criminal justice system.¹⁰⁶

Moreover, even unbiased statistical profiling may generate undesirable distributive outcomes.¹⁰⁷ Even if we restrict our assessment of the social costs of profiling to conventional economic concerns, it is not clear that statistical profiling is efficient. As Bernard Harcourt has argued, law enforcement efficiency is not achieved by equalizing hit rates, but rather by minimizing both crime and enforcement costs.¹⁰⁸ Profiling is efficient, therefore, only when it: (1) reduces the amount of profiled crime;¹⁰⁹ (2) does not diminish the efficient allocation of police resources; and (3) does not produce a “ratchet effect”¹¹⁰ on the profiled population.¹¹¹

such race-contingent behavior does not magically erase the harm.

Id. at 1514; see also Robert E. Suggs, *Poisoning the Well: Law and Economics and Racial Inequality*, 57 HASTINGS L.J. 255, 288-89 (2005). Audit studies have revealed similar results. See, e.g., IAN AYRES, PERVERSIVE PREJUDICE: UNCONVENTIONAL EVIDENCE OF RACE AND GENDER DISCRIMINATION (2001); Ian Ayres et al., *To Insure Prejudice: Racial Disparities in Taxicab Tipping*, 114 YALE L.J. 1613 (2005); Marianne Bertrand & Sendhil Mullainathan, *Are Emily and Greg More Employable Than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination*, 94 AM. ECON. REV. 991 (2004).

¹⁰⁶ See, e.g., *R. v. Williams*, [1998] 1 S.C.R. 1128 (Can.); *R. v. S.(R.D.)*, [1997] 3 S.C.R. 484, 505 (Can.) (L’Heureux-Dubé, McLachlin, JJ., concurring); *R. v. C.R.H.*, [2003] 174 C.C.C.3d 67, 81-82 (Man. C.A.) (Can.); *R. v. Brown*, [2003] 64 O.R.3d 161, 165 (Ont. C.A.) (Can.); *R. v. Parks*, [1993] 84 C.C.C.3d 353 (Ont. C.A.) (Can.); COMM’N ON SYSTEMIC RACISM IN THE ONT. CRIMINAL JUSTICE SYSTEM, *supra* note 100; RICHARD V. ERICSON, *REPRODUCING ORDER: A STUDY OF POLICE PATROL WORK 200-01* (1982); Julian V. Roberts & Anthony N. Doob, *Race, Ethnicity and Criminal Justice in Canada*, in *ETHNICITY, CRIME AND IMMIGRATION: COMPARATIVE AND CROSS-NATIONAL PERSPECTIVES* 469, 519 (Michael Tonry ed., 1997).

¹⁰⁷ See Donohue, *supra* note 98, at 23-25 (discussing how statistical discrimination can lead to the reinforcement of stereotypes that worsen the disadvantage of historically subordinated groups); CASS R. SUNSTEIN, *FREE MARKETS AND SOCIAL JUSTICE* 157-58 (1997) (noting that discrimination, in whatever form, can reduce minorities’ incentive to invest in human capital).

¹⁰⁸ See Bernard Harcourt, *Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally*, 71 U. CHI. L. REV. 1275, 1281-82, 1307-15 (2004).

¹⁰⁹ This condition may not be satisfied, for example, if the profiling of minority drivers gives white drivers a sense of impunity and thus increases their criminal activity. More generally, if law enforcement resources are fixed, profiling will reduce total crime “only if the ratio of the minority to white motorist population is greater than the differential of the change in offending by race.” This will depend on the groups’ elasticity of offending to policing and their natural offending rates. *Id.* at 1279, 1281-82, 1296, 1306.

¹¹⁰ A “ratchet effect” occurs when profiling “produces a supervised population that is disproportionate to the distribution of offending by racial group.” *Id.* at 1329. By unjustifiably targeting group members, profiling may increase the group’s crime rate, as

Unfortunately, the data does not allow us to determine directly whether highway profiling meets these conditions. However, drawing from other data sources, Harcourt argues that it probably does not. Minority drivers likely have slightly lower elasticities of offending to policing than white drivers,¹¹² as well as slightly higher natural offending rates.¹¹³ As a consequence, racial profiling is likely to both increase the crime rate (due to diminished deterrence of white drivers) and cause a ratchet effect in minority populations (resulting in disproportionate arrests and convictions over and above any natural higher offending rate).¹¹⁴ As Harcourt notes, this increase in negative contacts with police “will aggravate the disproportional representation of minorities in the correctional population, more unevenly distribute criminal records, supervision, and post-punitive collateral consequences, and significantly boost the public perception that minorities are drug users, traffickers, and couriers.”¹¹⁵

Search and seizure law is neither the only nor the most direct means of combating discriminatory profiling.¹¹⁶ However, it is very difficult to

measured by arrest or conviction rates rather than actual offending. This is because the former is always a fraction of latter. This increase in the group’s crime rate will provide justification, albeit false, for further wasteful profiling.

¹¹¹ *Id.* at 1279-80.

¹¹² This may result from minorities having fewer non-criminal employment opportunities, as well as cultural factors. *Id.* at 1282, 1299, 1356-57; *see also* Nicola Persico, *Racial Profiling, Fairness, and Effectiveness of Policing*, 92 AM. ECON. REV. 1472, 1474 (2002).

¹¹³ This is largely a product of greater minority participation in drug trafficking. Harcourt, *supra* note 108, at 1282, 1371.

¹¹⁴ *Id.* at 1282, 1297-99, 1330-35, 1371-73.

¹¹⁵ *Id.* at 1282; *see id.* at 1329-31; *see also* Dominitz, *supra* note 97, at 425 (“[W]hen police officers use race-ethnicity in stop and search decisions, the rate of apprehension of the guilty will be higher for those groups that are searched at a higher rate . . .”). Note that Harcourt’s approach does not require making a distinction between biased and statistical profiling. In his estimation, the evidence shows that profiling, whatever the police’s motivation, is likely inefficient and counterproductive. As he states, “If targeting minority motorists increases long-term offending on the highways or the overall costs to society, then it is in effect racially prejudiced. It may be inadvertent and mistaken, but it is effectively racist because it uses a racial category without any benefit to society.” Harcourt, *supra* note 108, at 1306-07 (emphasis omitted).

It has also been argued that racial profiling, whether biased or statistical, may also lead to higher rates of false arrests among minorities. Tomic and Hakes report that dismissal rates for African Americans charged with offenses typically associated with racial profiling are higher than those for whites, as well as for African Americans charged with other offenses. This disparity is lower in counties with a greater proportion of African American police officers, as well as in those with locally-elected judges and high proportions of African Americans. *See* Aleksandar Tomic & Jahn K. Hakes, *Case Dismissed: New Evidence in Racial Profiling* (Working Paper, 2004), available at <http://ssrn.com/abstract=618122>.

¹¹⁶ *See* Sujit Choudhy, *Protecting Equality in the Face of Terror: Ethnic and Racial*

mitigate profiling directly.¹¹⁷ Proving bias in any individual case is challenging, to say the least, and evidence of statistical disproportion cannot in itself prove that any particular search is illegitimate.¹¹⁸

One of the most effective ways to diminish discriminatory profiling may therefore be to limit the ability of police to conduct discretionary searches. As discussed, if a court finds that an investigative technique does not invade a reasonable expectation of privacy, then the technique is not a “search” and police may use it without restriction. In applying the reasonable expectation of privacy test to a novel search technique, courts should therefore consider the extent to which the technique is likely to be used in a discriminatory manner.

C. DECISION-MAKING ERROR

Constitutional provisions in Canada and the United States command courts to protect people against unreasonable governmental searches and seizures. These provisions, of course, are not the only sources of such protection. In both countries, legislatures regulate search powers exercised by executive authorities, and those authorities regulate themselves with various non-legal mechanisms, including official policies and informal norms. Microeconomic analysis and its public law offshoot, public choice theory, can help determine which branch of government is best placed to undertake such regulation. Cost-benefit calculations are made by self-interested decision-makers with imperfect information.¹¹⁹ Judges share these imperfections, but they have some capacity to develop rules that take their own and others’ weaknesses into account.¹²⁰ Identifying the biases

Profiling and s. 15 of the Charter, in THE SECURITY OF FREEDOM: ESSAYS ON CANADA’S ANTI-TERRORISM BILL 367 (Ronald J. Daniels et al. eds., 2001); RANDALL KENNEDY, RACE, CRIME, AND THE LAW 138-63 (1997); Tim Quigley, *Brief Investigatory Detentions: A Critique of R. v. Simpson*, 41 ALTA. L. REV. 935 (2004); Kent Roach, *Making Progress on Understanding and Remediating Racial Profiling*, 41 ALTA. L. REV. 895 (2004); David M. Tanovich, *Using the Charter to Stop Racial Profiling: The Development of an Equality Based Conception of Arbitrary Detention*, 40 OSGOODE HALL L.J. 145 (2002).

¹¹⁷ See Stuntz, *Local Policing*, *supra* note 88, at 2162-63, 2177-79.

¹¹⁸ *Id.* But see *R. v. Brown*, [2003] 64 O.R.3d 161, 174 (Ont. C.A.) (Can.) (“[W]here the evidence shows that the circumstances relating to a detention correspond to the phenomenon of racial profiling and provide a basis for the court to infer that the police officer is lying about why he or she singled out the accused person for attention, the record is then capable of supporting a finding that the stop was based on racial profiling.”).

¹¹⁹ See JAMES M. BUCHANAN & GORDON TULLOCK, *THE CALCULUS OF CONSENT: LOGICAL FOUNDATIONS OF CONSTITUTIONAL DEMOCRACY* (1962); Daniel A. Farber & Philip P. Frickey, *The Jurisprudence of Public Choice*, 65 TEX. L. REV. 873 (1987).

¹²⁰ See Cass R. Sunstein & Edna Ullmann-Margalit, *Second Order Decisions, in BEHAVIORAL LAW AND ECONOMICS* 187 (Cass R. Sunstein ed., 2000).

and information-gathering deficits of courts, legislatures, and police should reduce the frequency and magnitude of the errors that the reasonable expectation of privacy test inevitably generates.

The deficits of the police are obvious. While they may face pressure to avoid egregious privacy intrusions, the incentives bearing on them tilt heavily against investigative restraint. As individuals and institutions, police are rewarded primarily for minimizing crime, and the benefits of intrusive search techniques in achieving this objective are clear. In contrast, apart from budgetary constraints, the social costs of surveillance, such as those detailed above, are abstract, diffuse, and largely externalized; accordingly, police have little incentive to either discover or take them into account in exercising discretionary investigative powers.¹²¹ Police also lack the institutional means to perform the kind of comprehensive cost-benefit analysis that the reasonable expectation of privacy test entails. Consequently, while crime control interests must obviously be considered in applying the reasonable expectation of privacy test, courts should not show any significant degree of deference to police assessments of the need for a search technique.

Therefore, the legislatures and courts are primarily responsible for attaining an optimal balance between privacy and crime control. The key question for judges in applying the reasonable expectation of privacy test, then, is to what extent they should defer to legislative decisions to regulate or decline to regulate a particular investigative technique.

Legislatures generally have better access than courts to information important to accurate decision-making in this area. This information comes in two varieties. First, unlike judges, legislators are politically accountable, and are thus in a better position to gauge citizens' preferences for privacy and crime control. Second, legislatures have better access to information on the nature and effects of investigative methods. This advantage is especially apparent in the context of novel, technologically sophisticated search tools. In dealing with such matters, legislatures typically seek input from a variety of sources, including not only law enforcement agencies, but also industry organizations, advocacy groups, academics, technical experts, and the general public.¹²² By contrast, the ability of courts to obtain expert assistance and canvass the views of diverse stakeholders is much more limited.¹²³

¹²¹ See Brown, *supra* note 94, at 361; Stuntz, *Local Policing*, *supra* note 88, at 2179.

¹²² See, e.g., SUMMARY OF SUBMISSIONS TO THE LAWFUL ACCESS CONSULTATION (Nevis Consulting Group ed., 2003).

¹²³ See Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245, 261-63 (2002); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths*

Legislatures are also typically able to deal with new technologies more quickly than courts. Most judicial rule-making is performed by appellate courts, which usually encounter novel search technologies many years after they are put into use, and even then only if relevant cases are tried and appealed.¹²⁴ By this time, the factual record undergirding the rule-making process may be outdated.¹²⁵ Legislation is also often overtaken by technological developments, but here as well legislatures are better equipped to respond flexibly to changing circumstances. Unlike courts, legislatures can adopt measures to ensure that statutory provisions are periodically reviewed. Courts, in contrast, are constrained by *stare decisis*,¹²⁶ and, in the realm of constitutional interpretation, courts also impose constraints on legislative action.¹²⁷

All of this suggests that courts should be reluctant to usurp the legislature's capacity to regulate the use of novel search technologies as it sees fit. Public choice scholarship teaches us, however, that the legislative process may be skewed in favor of motivated and powerful interest groups.¹²⁸ Consequently, the interests of groups disproportionately harmed by legislation may be systematically discounted.¹²⁹ It is often asserted, for example, that the legislative process operates as a one-way ratchet in the

and the Case for Caution, 102 MICH. L. REV. 801, 875-76 [hereinafter Kerr, *Fourth Amendment*]; see also Cass R. Sunstein & Adrian Vermeule, *Interpretations and Institutions*, 101 MICH. L. REV. 885 (2003); William J. Stuntz, *Accountable Policing* (Harvard Public Law Working Paper No. 130, 2006), available at <http://ssrn.com/abstract=886170> [hereinafter Stuntz, *Accountable Policing*].

¹²⁴ See Kerr, *Fourth Amendment*, *supra* note 123, at 868-69.

¹²⁵ See Stuart Minor Benjamin, *Stepping Into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269, 272 (1999).

¹²⁶ See Kerr, *Fourth Amendment*, *supra* note 123, at 871-73. Many of the enhanced investigative powers enacted by Congress and Parliament in the immediate aftermath of the September 11, 2001 terrorist attacks were made subject to "sunset" clauses mandating expiry after a certain period absent legislative renewal. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272, §§ 202, 206, 209, 212, 214, 215, 217, 218, 220; *Canada Criminal Code*, R.S.C., ch. C 46 § 83.32 (1985).

¹²⁷ See Stuntz, *Accountable Policing*, *supra* note 123, at 34-41.

¹²⁸ See DANIEL A. FARBER & PHILIP P. FRICKEY, *LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION* (1991); MANCUR OLSON, *THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS* (1965); *PUBLIC CHOICE AND PUBLIC LAW: READINGS AND COMMENTARY* (Maxwell L. Stearns ed., 1997).

¹²⁹ See generally JOHN HART ELY, *DEMOCRACY AND DISTRUST* (1980). As William Stuntz has said, "Anytime the government does something that has concentrated costs but diffused benefits, there is a danger that it will do too much—harming one voter to please ten is generally thought to be a good deal from the point of view of politically accountable decisionmakers." Stuntz, *Local Policing*, *supra* note 88, at 2165.

criminal sphere.¹³⁰ According to this view, legislatures respond robustly to demands for greater investigative powers and harsher sanctions from police, prosecutors, victims, and the crime-fearing public, while ignoring calls from defense lawyers, civil libertarians, and academics for greater police regulation and punitive restraint.¹³¹

Some commentators have argued that this may often be true of search and seizure laws, which as we have seen sometimes impose disproportionate costs on politically marginal groups (such as certain racial and ethnic minorities).¹³² It would be a mistake to assume, however, that legislatures are always incapable of tempering demands for intrusive search and surveillance powers.¹³³ When a surveillance technique threatens to impose substantial costs on a broad or politically powerful segment of the population, the legislature will often be pressured to regulate it.¹³⁴ Indeed, in most cases Congress has regulated new search technologies long before the courts have encountered them.¹³⁵ And in cases where the Supreme Court has found that a technology does not invade a reasonable expectation of privacy, Congress has often intervened to regulate it. For example, after the Court held that pen registers were not Fourth Amendment searches,¹³⁶ Congress responded with legislation prohibiting their use without a court

¹³⁰ See Stephen B. Bright, *Counsel for the Poor: The Death Sentence Not for the Worst Crime but for the Worst Lawyer*, 103 YALE L.J. 1835, 1870 (1994); Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079 (1993); Charles Ogletree, Jr., *An Essay on the New Public Defender for the 21st Century*, 58 LAW & CONTEMP. PROBS. 81, 83-85 (1995). But see Stuntz, *Accountable Policing*, *supra* note 123, at 19 ("Contrary to the conventional wisdom, criminal suspects are a powerful interest group.").

¹³¹ See KENT ROACH, *DUE PROCESS AND VICTIMS' RIGHTS: THE NEW LAW AND POLITICS OF CRIMINAL JUSTICE* (1999); William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 553-56 (2001).

¹³² See Wasserstrom & Seidman, *supra* note 10, at 93-104; see also MICHAEL H. TONRY, *MALIGN NEGLECT: RACE, CRIME, AND PUNISHMENT IN AMERICA* (1995).

¹³³ See generally Kerr, *Fourth Amendment*, *supra* note 123, at 839-58 (noting that Congress, and not the courts, has taken the lead in providing privacy in the face of novel search technologies); Ronald F. Wright, *Parity of Resources for Defense Counsel and the Reach of Public Choice Theory*, 90 IOWA L. REV. 219, 254-60 (2004) (arguing that legislators can sometimes be motivated to enact criminal defendant-friendly legislation).

¹³⁴ See Stuntz, *Accountable Policing*, *supra* note 123, at 19, 53. Stuntz also points out that there is a considerable body of legislation designed to redress the kinds of police abuses (such as racial profiling) that are disproportionately visited on minorities. *Id.* at 22-24; see also Stuntz, *Local Policing*, *supra* note 88, at 2165-66.

¹³⁵ See Kerr, *Fourth Amendment*, *supra* note 123, at 870-82; Stuntz, *Accountable Policing*, *supra* note 123, at 21-22.

¹³⁶ *Smith v. Maryland*, 442 U.S. 735 (1979).

order.¹³⁷ Similarly, after lower courts found no reasonable expectation of privacy in cordless telephone conversations,¹³⁸ Congress enacted provisions protecting them.¹³⁹ And after the Supreme Court concluded that bank records attract no reasonable expectation of privacy,¹⁴⁰ Congress prohibited authorities from obtaining them without a subpoena, warrant, or formal written request providing grounds for the search.¹⁴¹

In the pre-Charter era, the Canadian Parliament was similarly proactive in protecting privacy against intrusive surveillance technologies.¹⁴² This effort lagged somewhat in the first two decades after the passage of the Charter, when Parliament was forced to respond to a series of assertive § 8 decisions by the Supreme Court.¹⁴³ Yet even during this period, Parliament

¹³⁷ Electronic Communications Privacy Act, 18 U.S.C. § 3121-27 (2000). Law enforcement agencies may obtain such an order, however, merely by showing that the “information likely to be obtained . . . is relevant to an ongoing criminal investigation.” *Id.* §§ 3122(b)(2), 3123(a). This standard is likely lower than reasonable suspicion. See JAMES A. ADAMS & DANIEL D. BLINKA, *ELECTRONIC SURVEILLANCE: COMMENTARIES AND STATUTES* 121 (2003/2004 ed.). Courts may not exclude evidence, moreover, on the basis that it was obtained in violation of this legislation. See *United States v. Thompson*, 936 F.2d 1249 (11th Cir. 1991) (courts should not imply a suppression remedy unless a statute specifically refers to the exclusionary rule); Kerr, *Internet Surveillance*, *supra* note 44, at 632.

¹³⁸ See *United States v. McNulty*, 47 F.3d 100, 104-06 (4th Cir. 1995); *United States v. Smith*, 978 F.2d 171, 177-81 (5th Cir. 1995); *Tyler v. Behrodt*, 877 F.2d 705, 706 (8th Cir. 1989).

¹³⁹ See Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202(a), 108 Stat. 4279 (1994).

¹⁴⁰ *United States v. Miller*, 425 U.S. 435 (1976).

¹⁴¹ Right to Financial Privacy Act (RFPA) of 1978, 12 U.S.C. §§ 3402-3422; see U.S. Sec. & Exch. Comm’n v. *Jerry T. O’Brien, Inc.*, 467 U.S. 735, 745-46 (1984). To obtain banking records, the government must have “reason to believe that the records sought are relevant to a legitimate law enforcement inquiry.” See 12 U.S.C. §§ 3405, 3407, 3408. This standard is lower than probable cause. See *Hunt v. U.S. Sec. & Exch. Comm’n*, 520 F. Supp. 580 (N.D. Tex. 1981). Again, evidence obtained in violation of these provisions is not subject to suppression at trial. See 12 U.S.C. § 3417(d) (“The remedies and sanctions described in this chapter shall be the only authorized judicial remedies and sanctions for violations of this chapter.”); *United States v. Daccarett*, 6 F.3d 37, 52 (2d Cir. 1993) (holding that the only remedy under the RFPA is provided in the statute); *United States v. Frazin*, 780 F.2d 1461, 1466 (9th Cir. 1986) (same).

¹⁴² See Canada Protection of Privacy Act, R.S.C., ch. 50 (1973-74) (prohibiting the interception of private communications, providing procedure for obtaining wiretap warrants, and prohibiting admission of evidence obtained in contravention of warrant requirements).

¹⁴³ As discussed, in *R. v. Duarte*, the Court struck down what was then § 178.11 of the Criminal Code, which exempted participant surveillance from the prohibition of warrantless electronic surveillance. [1990] 1 S.C.R. 30 (Can.). The Criminal Code was subsequently amended to permit warrantless participant surveillance in two circumstances: (1) as protection for undercover agents (in which case any evidence obtained is inadmissible); and (2) when police obtain a warrant based on reasonable and probable grounds. Canada

took the lead over the courts in protecting privacy in a number of areas. After two courts found that pen registers did not invade a reasonable expectation of privacy,¹⁴⁴ Parliament authorized the issuance of “number recorder” warrants on the basis of reasonable suspicion.¹⁴⁵ And after one court determined that wireless telephone communications might not be subject to the same statutory protections as land line calls,¹⁴⁶ Parliament passed legislation clarifying that most wireless calls are protected.¹⁴⁷

Courts should generally be reluctant, then, to preempt the legislature’s decision to regulate (or decline to regulate) novel surveillance techniques. They should be especially deferential when dealing with sophisticated and rapidly changing search technologies whose social costs are likely to be distributed across a broad segment of society.¹⁴⁸ Less deference may be

Criminal Code, R.S.C., ch. C 46 §§ 184.1, 184.2 (1985). Recall as well that in *R. v. Wong*, the Court held that surreptitious, video-only surveillance (which the Criminal Code has never prohibited) of a hotel room invaded a reasonable expectation of privacy. [1990] 3 S.C.R. 36 (Can.). Parliament responded by enacting a provision allowing police to obtain warrants to conduct video surveillance on reasonable and probable cause. Canada Criminal Code, R.S.C., ch. C 46 § 487.01. And in *R. v. Wise*, the Court concluded that the installation and monitoring of a tracking device invaded a reasonable expectation of privacy. [1992] 1 S.C.R. 527 (Can.). Parliament soon thereafter authorized the granting of tracking warrants on the basis of reasonable suspicion. See Canada Criminal Code, R.S.C., ch. C 46 § 492.1.

¹⁴⁴ See *R. v. Sampson*, [1983] 45 Nfld. & P.E.I.R. 32 (Nfld. C.A.) (Can.); *R. v. Fegan*, [1993] 13 O.R.3d 88 (Ont. C.A.) (Can.).

¹⁴⁵ Canada Criminal Code, R.S.C., ch. C 46 § 492.2. The provision defines a “number recorder” as “any device that can be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received.” As mentioned *supra* note 48, at least two courts have since held that the use of the reasonable suspicion standard in place of reasonable and probable grounds violates § 8 of the Charter. See *R. v. Nguyen*, [2004] B.C.J. No. 249 (B.C. S.C.) (Can.); *R. v. Hackert*, [1997] O.J. No. 6384 (Ont. Gen. Div.) (Can.).

¹⁴⁶ See *R. v. Solomon*, [1992] 77 C.C.C.3d 264 (Que. Mun. Ct.) (Can.) (holding that an intercepted wireless telephone communication was not a “private communication” within the meaning of Part VI of the Criminal Code, as the accused could not reasonably have expected that his conversations would not be intercepted).

¹⁴⁷ Section 183 of the Criminal Code now specifies that any radio-based telephone communication that “is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it” is a “private communication” subject to the same protections as land-line telephone communications. Canada Criminal Code, R.S.C., ch. C 46 § 183. Section 184.5 also makes it an offense to intercept radio-based telephone communications “maliciously or for gain.” *Id.* § 184.5

¹⁴⁸ See Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 555-56 (2005); Stuntz, *Local Policing*, *supra* note 88, at 2166. This is not to say that where the social costs of a privacy-invasive search technique are broadly distributed, legislatures will ineluctably choose the optimal level of privacy protection. Like other decision-makers (including judges), the rationality of legislators (and the constituents who elect them) is limited by a

warranted when the costs of a technique are likely to be borne disproportionately by “discrete and insular minorities” with little political power.¹⁴⁹ Concluding that a technique invades a reasonable expectation of privacy (and is hence subject to privacy-protecting regulations) improves the odds that its costs will be internalized by society as a whole.¹⁵⁰

IV. INFRARED CAMERA SEARCHES

To illustrate how economically-informed cost-benefit analysis can improve the conventional reasonable expectation of privacy test, consider the use of infrared cameras to detect indoor marijuana cultivation operations. Recall that in *Kyllo*, the United States Supreme Court held that residential infrared camera searches invade a reasonable expectation of privacy, and that in *Tessling*, the Canadian Supreme Court came to the

number of factors, including incomplete and asymmetric information, bounded rationality, and systemic psychological distortions. See Christine Jolls et al., *A Behavioral Approach to Law and Economics*, in BEHAVIORAL LAW AND ECONOMICS, *supra* note 120, at 13, 48; Roger G. Noll & James E. Krier, *Some Implications of Cognitive Psychology for Risk Regulation*, in BEHAVIORAL LAW AND ECONOMICS, *supra* note 120, at 325, 342-47. There is evidence that cognitive, decisional, and informational limitations may lead people to prefer suboptimal levels of privacy protection. While the risks of being a victim of crime are typically straightforward, immediate, and highly salient, the risks of privacy invasions may often be complex, cumulative, context dependent, and realized far into the future. See Allesandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, 1 PROC. 6TH ANN. ACM CONF. ON ELECTRONIC COM. 21, 23-24 (2004), available at <http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf>; Acquisti & Grossklags, *supra* note 76, at 26-27; Brown, *supra* note 94, at 343. Judges are just as likely, however, to suffer from these limitations as legislators.

¹⁴⁹ *United States v. Carolene Prods. Co.*, 304 U.S. 144, 153 n.4 (1938) (“Nor need we enquire whether similar considerations enter into the review of statutes directed at particular religious, or racial minorities, whether prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry.” (citations omitted)); see also Wasserstrom & Seidman, *supra* note 10, at 95 (“[W]hen the privacy costs of law enforcement are spread more widely, and there is a reduced risk that the politically less powerful are being forced to bear disproportionate privacy losses, the courts often have allowed searches and seizures without prior judicial supervision or particularized suspicion.”).

¹⁵⁰ This assumes that economically privileged, unelected judges are better attuned to the problem of law enforcement discrimination than legislators. This assumption has been questioned. See Wasserstrom & Seidman, *supra* note 10, at 100. However, on account of their extensive experience with police-citizen encounters and relative insulation from majoritarian pressures, judges may be able to discern differential impacts on privacy that are likely to be ignored or discounted by legislators. See William M. Landes & Richard A. Posner, *The Independent Judiciary in an Interest Group Perspective*, 18 J.L. & ECON. 875 (1975).

opposite conclusion.¹⁵¹ The *Tessling* Court described the capabilities of infrared cameras as follows:

FLIR¹⁵² technology records images of thermal energy or heat radiating from a building. Once a baseline is calibrated, cooler areas show up as dark, and warmer areas are lighter. FLIR imaging cannot, at this stage of its development, determine the nature of the source of heat within the building. It cannot distinguish between heat diffused over an external wall that came originally from a sauna or a pottery kiln, or between heat that originated in an overheated toaster or heat from a halide lamp. In short, the FLIR camera cannot “see” through the external surfaces of a building. However, the substantial amounts of heat generated by marijuana growing operations must eventually escape from the building. The FLIR camera creates an image of the distribution of escaping heat at a level of detail not discernible by the naked eye. A FLIR image, put together with other information, can help the police get reasonable and probable grounds to believe that a marijuana growing operation is in residence.¹⁵³

Though both courts invoked the public exposure and intimacy doctrines, neither doctrine proved particularly helpful. Justice Scalia began his majority decision in *Kyllo* by noting that the visual inspection of a dwelling (from any publicly accessible vantage point) is not a search.¹⁵⁴ He quickly concluded, however, that infrared searches differ from “naked eye surveillance” because they allow police to obtain “information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area.’”¹⁵⁵ Scalia found, in other words, that *Kyllo* did not voluntarily expose the heat radiating from his home to public observation.

Justice Stevens, writing for the *Kyllo* dissenters, took a different approach. In his view, infrared cameras do not give police direct access to private information; rather, they merely help them to infer what is going on

¹⁵¹ *United States v. Kyllo*, 533 U.S. 27 (2001); *R. v. Tessling*, [2004] 3 S.C.R. 432 (Can.). Note that these results do not fit the general pattern of the respective Courts’ recent search and seizure decisions. The United States Supreme Court has generally been more accommodating of law enforcement interests than its Canadian counterpart. *See supra* notes 31-75 and accompanying text. It is also worth noting that each of the two camps in *Kyllo* consisted of a curious amalgam of conservatives and liberals. The Justices in the majority were Justices Scalia, Souter, Thomas, Ginsburg, and Breyer. *Kyllo*, 533 U.S. at 28. Chief Justice Rehnquist, along with Justices O’Connor, Stevens, and Kennedy dissented. *Id.*

¹⁵² “FLIR” stands for “Forward Looking Infra-Red.” *See Tessling*, [2004] 3 S.C.R. ¶ 2.

¹⁵³ *Id.* ¶ 5 (citation omitted). The device used in *Kyllo* was described as a

“non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house”; it “did not show any people or activity within the walls of the structure”; “the device used cannot penetrate walls or windows to reveal conversations or human activities”; and “no intimate details of the home were observed.”

Kyllo, 533 U.S. at 30 (quoting from the evidentiary findings of the district court).

¹⁵⁴ *Kyllo*, 533 U.S. at 31-33.

¹⁵⁵ *Id.* at 33-34 (internal citation omitted).

inside residences from “information in the public domain.”¹⁵⁶ Expressly applying the public exposure doctrine, he concluded that infrared camera searches could not be constitutionally distinguished from naked eye observations of heat emanations, as when someone notices that “one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces.”¹⁵⁷

In *Tessling*, the Supreme Court of Canada treated the public exposure doctrine with more ambivalence. In assessing whether Tessling had a subjective expectation of privacy in his home’s thermal profile, Justice Binnie asserted that “allowing” heat to escape does not count as a knowing or voluntary exposure.¹⁵⁸ In determining the objective reasonableness of any expectation of privacy, however, he noted that heat loss from external walls is “obvious to even the most casual observer,”¹⁵⁹ and while an infrared camera reveals more detail than is apparent to the naked eye, it nonetheless “records only information exposed to the public.”¹⁶⁰

There is no way to determine which of the forgoing approaches is correct. The dissipation of thermal energy is inevitable,¹⁶¹ and in many circumstances, differential heat production will be visually discernable. It is also true that infrared imaging produces a more detailed picture of heat distribution than is apparent in the visible part of the electromagnetic spectrum. Attempting to categorize the information revealed by infrared searches as “public” or “private” or emanating from a home’s “exterior” or “interior” is a fruitless endeavor.

It is perhaps for this reason that the *Tessling* majority and the *Kyllo* dissent focused on the nature of the information obtained by infrared searches, concluding that they revealed only non-intimate information.¹⁶² This argument has some merit. The images in *Kyllo* and *Tessling* allowed police to make only general inferences about the nature of the activities taking place inside the home. Justice Scalia had a point, however, when he stated that “in the home . . . all details are intimate details.”¹⁶³ He questioned whether it would be possible to articulate a standard “specifying

¹⁵⁶ *Id.* at 41 (Stevens, J., dissenting).

¹⁵⁷ *Id.* at 43 (Stevens, J., dissenting).

¹⁵⁸ *Tessling*, [2004] 3 S.C.R. ¶¶ 39-41.

¹⁵⁹ *Id.* ¶ 46.

¹⁶⁰ *Id.* ¶ 47.

¹⁶¹ See *Pennsylvania v. Gindlesperger*, 743 A.2d 898, 904-05 (Pa. 1999) (“The laws of thermodynamics dictate that no matter how much one insulates, heat will still escape.”).

¹⁶² See *Kyllo*, 533 U.S. at 42-46, 50-51 (Stevens, J., dissenting); *Tessling*, [2004] 3 S.C.R. ¶¶ 59-62.

¹⁶³ *Kyllo*, 533 U.S. at 37.

which home activities are ‘intimate’ and which are not.”¹⁶⁴ Assessments of intimacy vary widely depending on subjective preferences, context, and the extent to which information from disparate sources is compiled and aggregated. The infrared images produced in *Kyllo* and *Tessling* were crude, but combined with other information, they could nonetheless generate probabilistic inferences about a number of non-criminal activities that some people would prefer to keep private.¹⁶⁵ While it can be argued that the information uncovered by infrared cameras is not especially sensitive, ultimately the intimacy doctrine is only marginally more helpful than the public exposure doctrine in deciding whether the technology invades a reasonable expectation of privacy.

A. PRIVACY COSTS

Economic cost-benefit analysis promises to be more helpful in making this determination. Consider first the social costs that would ensue if infrared searches were held to invade a reasonable expectation of privacy. When a court finds such an expectation, it subjects the search technique to constitutional regulation, usually by requiring police to obtain a probable cause warrant. Even if we assume that police could obtain infrared warrants on a lesser standard (such as reasonable suspicion), the costs would be substantial. Police would be forced to rely on more expensive and riskier investigative methods (such as undercover operations) either as substitutes for infrared searches or to provide evidentiary foundations for warrant applications.¹⁶⁶ Higher costs mean less enforcement and less deterrence.

¹⁶⁴ *Id.* at 38-39.

¹⁶⁵ Justice Scalia asserted, for example, that the infrared technology used in *Kyllo* may have permitted police to determine “at what hour each night the lady of the house takes her daily sauna and bath.” *Id.* at 38; see also *United States v. Cusumano*, 67 F.3d 1497, 1501 (10th Cir. 1995) (“While the heat lost by a building is data of some limited value, the true worth of the device—the very reason that the government turned the imager on the home of the Defendants—is predicated upon the translation of these thermal records into intelligible (albeit speculative) information about the activities that generate the observed heat.”), *vacated and decided on other grounds*, 83 F.3d 1247 (10th Cir. 1996) (en banc).

¹⁶⁶ This remains true even if it is assumed that infrared images must usually be supplemented by corroborating evidence to establish probable cause to conduct physical searches. See *Tessling*, [2004] 3 S.C.R. at 456 (“[A]t present no warrant could ever properly be granted solely on the basis of a FLIR image.”). Thus, prohibiting infrared searches in the absence of reasonable suspicion would increase the need for corroborating evidence.

B. PRIVACY BENEFITS

Our willingness to bear these costs depends on the magnitude of the benefits that a warrant requirement would produce. In the absence of legal privacy protections, people may either avoid productive activities or defend their privacy by other means. Unrestricted infrared searches are unlikely to produce either avoidance or defensive costs. As discussed, even crude infrared images may permit probabilistic inferences about non-criminal residential activity, and some may not want police to have unrestricted access to this information. But for people who are not growing marijuana, knowing that police might be monitoring heat escaping from their homes is unlikely to prompt any behavioral changes, let alone chill participation in socially valuable discourse or activity. The fact that electricity consumption records have been freely available to police for years does not appear to have prompted people to modify their residential activities.¹⁶⁷ Similarly, the widespread use of infrared cameras is not likely to cause law-abiding individuals to install better insulation or find other means of limiting the escape of heat from their homes.

The next question is whether regulating infrared searches is likely to prevent suboptimal enforcement expenditures. At first blush, the marijuana prohibition might appear to be the kind of inefficient law that privacy rights should aim to thwart.¹⁶⁸ The economic case for legalizing marijuana (and perhaps other illicit drugs) is strong.¹⁶⁹ There is considerable evidence that the costs of enforcement vastly outweigh the harms of consumption.¹⁷⁰ But even if this is correct, it does not follow that privacy law should be used to hamper the ability of police to detect producers. As long as marijuana trafficking remains illegal, a substantial portion of its profits will flow to people involved in broader criminal enterprises.¹⁷¹ Restricting infrared searches would diminish the risk of detection, thereby lowering the costs of

¹⁶⁷ See *R. v. Plant*, [1993] 3 S.C.R. 281 (Can.).

¹⁶⁸ There is a hint of this reasoning in the appeals court's decision in *Tessling*. See *R. v. Tessling*, [2003] 171 C.C.C.3d 361, 382-83 (Ont. C.A.) (Can.) (“[T]here has been public, judicial, and political recognition that marijuana is at the lower end of the hierarchy of harmful drugs.”), *rev'd*, [2004] 3 S.C.R. 432 (Can.).

¹⁶⁹ See Gary S. Becker et al., *The Market for Illegal Goods: The Case of Drugs*, 114 J. POL. ECON. 38 (2006); Cooter & Ulen, *supra* note 80, at 479-84 (reviewing theoretical and empirical evidence demonstrating the inefficiency of the “war on drugs”).

¹⁷⁰ See, e.g., COMM'N OF INQUIRY INTO THE NON-MEDICAL USE OF DRUGS, CANNABIS, A REPORT OF THE COMMISSION OF INQUIRY INTO THE NON-MEDICAL USE OF DRUGS (1972); see also *R. v. Malmo-Levine*, [2003] 3 S.C.R. 571 (Can.); *R. v. Parker*, [2000] 146 C.C.C.3d 193 (Ont. C.A.) (Can.).

¹⁷¹ See Paul J. Goldstein et al., *Drug-Related Homicide in New York: 1984 and 1988*, 38 CRIME & DELINQ. 459 (1992).

entry into the trade and increasing revenues available to finance crimes that do cause substantial social harm. It would also lead to an increase in violence and other criminal activity associated with competition between producers.¹⁷² If the marijuana prohibition is a bad law, then we should press for its reform or abolition—not use privacy law to promote the growth of an illicit market.¹⁷³

The discretionary use of infrared searches is also unlikely to encourage discriminatory profiling. Discriminatory profiling is most likely to occur when police can readily observe the profiled characteristic (such as race) and use it as a proxy for criminality, such as during street and vehicle stops, airport security checks, or border crossings.¹⁷⁴ Police using infrared cameras, in contrast, are less likely to be aware of the suspect's race or ethnicity.¹⁷⁵ The immediate targets of the searches, after all, are buildings, not people. Further, unlike detentions and physical searches of pedestrians, drivers, and air travelers, infrared searches are unlikely to cause innocent suspects to feel inconvenienced, embarrassed, or stigmatized (feelings that often generate a profound sense of unfairness among the innocent targets of profiling). Indeed, in most cases the innocent subjects of infrared searches will never become aware that they have been searched.

C. DECISION-MAKING ERROR

Even if the forgoing analysis underestimates the costs or overestimates the benefits of unregulated infrared searches, we should still prefer the result in *Tessling* to that in *Kyllo*. Like many other novel search technologies, the uses and capabilities of infrared imaging are changing rapidly.¹⁷⁶ These are precisely the circumstances in which courts should be

¹⁷² See Steven D. Levitt & Sudhir Alladi Venkatesh, *An Economic Analysis of a Drug-Selling Gang's Finances*, 115 Q. J. ECON. 755 (2000).

¹⁷³ The former Canadian government's proposed legislation decriminalizing the possession of small quantities of marijuana suggests that Parliament may be becoming more amenable to such reform. See *An Act to amend the Contraventions Act and the Controlled Drugs and Substances Act and to make consequential amendments to other Acts*, Bill C-17, 38th Parl., (1st Sess. 2004) (Can.).

¹⁷⁴ See sources cited *supra* note 100.

¹⁷⁵ In cases where police do target members of a minority group in marijuana investigations, evidence of discrimination will often be readily apparent. In *R. v. Nguyen*, for example, the court found that a police officer engaged in unconstitutional racial profiling when he obtained from a local land registry office a list containing only the names of property owners with Vietnamese surnames. [2006] O.J. No. 272 ¶¶ 29-30 (Ont. S.C.) (Can.).

¹⁷⁶ See Jeffrey P. Campisi, *The Fourth Amendment and New Technologies: The Constitutionality of Thermal Imaging*, 46 VILL. L. REV. 241, 270-75 (2001) (discussing the state of current thermal imaging technology and future developments); George M. Dery, *Lying Eyes: Constitutional Implications of New Thermal Imaging Lie Detection Technology*,

reluctant to preempt the legislature's ability to craft (and adjust) a nuanced and flexible regulatory scheme.

The majority opinion in *Kyllo* illustrates the drawbacks of judicial interventionism in the realm of high technology. Anxious to set out a firm, bright-line rule capable of anticipating future technological developments,¹⁷⁷ Justice Scalia proclaimed that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."¹⁷⁸ The "general public use" criterion, however, is both vague and normatively troubling.¹⁷⁹ Since *Kyllo* was decided, infrared cameras have become more affordable, portable, and user-friendly; they are currently used in a wide variety of law enforcement, immigration, military, and civilian applications, including construction, manufacturing, testing, and inspection.¹⁸⁰ How are police, prosecutors, and courts to determine when infrared cameras are so ubiquitous as to be in "general public use"? And if the courts eventually decide that they are, would this mean that infrared cameras could never invade a reasonable expectation of privacy, even if they become capable of capturing detailed images of residential life?

If infrared imaging advances to this point, and if its use by the police threatens to generate significant avoidance or defensive costs, legislatures can intervene and regulate it. As infrared searches have the potential to impact a broad segment of society, the issue is best left to the legislative process. Technology enabling police to "see" what is going on inside a person's home is likely to prompt strong political opposition. In these circumstances, legislatures are more likely to achieve an optimal balance of privacy and security than the courts.¹⁸¹

31 AM. J. CRIM. L. 217 (2004) (discussing the use of infrared cameras to detect facial blood flow patterns consistent with deception).

¹⁷⁷ See *United States v. Kyllo*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

¹⁷⁸ *Id.* at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)) (citation omitted) (emphasis added).

¹⁷⁹ See *supra* note 27 and accompanying text.

¹⁸⁰ See, e.g., Advanced Infrared Resources, <http://www.infraredthermography.com/applicat.htm> (last visited Apr. 21, 2007); FLIR, <http://www.flir.com> (last visited Apr. 21, 2007).

¹⁸¹ For example, in an effort to minimize the intrusiveness of infrared searches, legislation could set out a list of "approved" infrared cameras, with detailed specifications for their use, as has been done in the context of blood alcohol screening and measuring devices. See *Canada Criminal Code*, R.S.C., ch. C 46 § 254 (1985).

V. LOCATION TRACKING

A similar analysis can be performed with respect to a very different surveillance technology: location tracking devices. Early iterations of this technology were considered in *Knotts*,¹⁸² *Karo*,¹⁸³ and *Wise*.¹⁸⁴ Recall that in *Knotts* and *Karo*, the United States Supreme Court held that tracking suspects with surreptitiously planted radio transmitters (beepers) did not invade a reasonable expectation of privacy, as long as the transmitters did not allow police to monitor constitutionally protected locations, such as residences.¹⁸⁵ In *Wise*, in contrast, the Supreme Court of Canada concluded that such tracking of a suspect's vehicle over public roads infringed on a reasonable expectation of privacy, albeit only in a "minimally intrusive" manner.¹⁸⁶

By today's standards, the technology used in these cases was rudimentary. The Court described the beeper used in *Wise* as follows:

The device consisted of a low power radio transmitter. From the strength of the signal, it was possible to determine the general location of the object to which the beeper had been fixed. By moving in the direction of the transmitter and adjusting the "RF gain control", the location could be more precisely determined. The device used in this case was not capable of indicating if the object being tracked was to the right, left, front or back of the receiver of the signal.

The evidence in this case was that the device was used intermittently as a back-up for visual surveillance of the appellant's car . . . particularly to attempt to locate the vehicle when visual surveillance failed. Since the device was not capable of pinpointing the vehicle with any degree of precision, physical surveillance was always required to fix its proximate position.¹⁸⁷

Tracking devices are now much more powerful and precise. Two sophisticated technologies are already in widespread use: the Global Positioning System (GPS) and wireless telephone networks.¹⁸⁸ Like

¹⁸² *United States v. Knotts*, 460 U.S. 276 (1983).

¹⁸³ *United States v. Karo*, 468 U.S. 705 (1984).

¹⁸⁴ *R. v. Wise*, [1992] 1 S.C.R. 527 (Can.).

¹⁸⁵ See discussion *supra* notes 37-40 and accompanying text.

¹⁸⁶ *Wise*, [1992] 1 S.C.R. at 538.

¹⁸⁷ *Id.* at 534-35. The capabilities of the devices used in *Knotts* and *Karo* were roughly similar. See *Karo*, 468 U.S. at 707 n.1; *Knotts*, 460 U.S. at 277. In both cases, a beeper was used as a supplement to, and not a complete substitute for, traditional physical surveillance.

¹⁸⁸ There are a number of other widely-used technologies that allow police to determine suspects' locations, including public transit passes and toll road transponders, both of which record the time and the pass holders' identity at points of ingress and egress. Unlike GPS and wireless telephone networks, however, these technologies are not capable of tracking suspects' movements on a continuous basis. See generally Brendan I. Koerner, *Your Cellphone Is a Homing Device*, LEGAL AFF., Jul.-Aug. 2003, at 30, available at

traditional beepers, these technologies use radio waves to establish a connection between devices at unknown locations and devices at known locations. The newer technologies, however, have two critical advantages over beepers. Unlike a beeper, which must remain within a certain distance of its tracking receiver, GPS and wireless phone tracking devices are linked to an extensive, permanent network of transceivers. This allows police to track suspects from a remote, stationary location, thus eliminating the need for mobile, physical surveillance.¹⁸⁹ Second, because GPS devices and wireless phones can send data to and receive data from multiple network nodes simultaneously, the suspect's precise location can be determined mathematically.¹⁹⁰ As noted in *Wise*, a beeper's location can only be inferred imprecisely by gauging the strength of its signal.¹⁹¹

The GPS network consists of at least two dozen satellites, which are owned by the United States government and were initially used for exclusively military purposes and are now freely available for a variety of civilian navigational uses.¹⁹² GPS devices can determine location with a great deal of precision. Depending on the equipment used, distances

http://www.legallaaffairs.org/issues/July-August-2003/feature_koerner_julaug03.msp. Video monitoring systems are capable of continuous surveillance, so long as suspects' movements occur within the range of the camera network. See generally Renée M. Pomerance, *Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the "Inviolable Personality,"* 9 CAN. CRIM. L. REV. 273 (2005), Justice Gérard La Forest, Address to George Radwanski, Privacy Comm'r of Can., Opinion: Video Surveillance (Apr. 5, 2002), available at http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp.

¹⁸⁹ See *State v. Jackson*, 76 P.3d 217, 223-24 (Wash. 2003).

¹⁹⁰ Specifically, a GPS device determines its location by measuring the time it takes for radio signals to travel to the device from at least four different satellites. Location can then be derived through the processes of trilateration or multilateration. See AHMED EL-RABBANY, INTRODUCTION TO GPS: THE GLOBAL POSITIONING SYSTEM 1-2, 8-9 (2002). The location of a non-GPS equipped wireless phone can be calculated in a similar fashion, using the time differences obtained from multiple base stations. It can also be determined using triangulation by measuring the angles of the signals received by two or more base stations. See Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-09 (2004) [hereinafter *Who Knows Where You've Been?*]. Yet another technique, known as "fingerprinting," permits location to be pinpointed by analyzing the distortion patterns corresponding to differing locations in a single base station's receiving range. See David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 4-5 (2003).

¹⁹¹ *R. v. Wise*, [1992] 1 S.C.R. 527, 534-35 (Can.).

¹⁹² See generally ELLIOT D. KAPLAN, UNDERSTANDING GPS: PRINCIPLES AND APPLICATIONS (1996). The government first granted civilians access to GPS in 1983. See April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 666 (2005).

covered, and other variables, they can currently determine location (longitude, latitude, and altitude) to within a few meters.¹⁹³ The accuracy of GPS tracking has improved steadily over the years, and further improvement is expected. Police may either surreptitiously install GPS receivers on suspects' vehicles or possessions¹⁹⁴ or obtain real-time or historical data generated by commercial GPS devices, such as those installed in vehicles and wireless phones.¹⁹⁵

Wireless telephones are also capable of being conscripted by police for use as tracking devices, even when they are not equipped with GPS devices. Whenever they are turned on, wireless (cell) phones automatically and periodically communicate with a network of base and switching stations.¹⁹⁶ These communications, which are carried on a dedicated channel separate from the voice and data communications sent or received by the phone's user, connect the phone to the network and allow it to switch channels when it moves from one cell area to another.¹⁹⁷ The accuracy of non-GPS wireless phone tracking varies widely, depending on a number of factors, including the sophistication of the technology and the number of stations within range of the phone. Many contemporary systems can determine location (longitude and latitude) to within fifty meters,¹⁹⁸ and future systems will undoubtedly be even more precise.¹⁹⁹ As with GPS tracking, police

¹⁹³ One of the leading manufacturers of commercial GPS receivers boasts that its devices are accurate to within fifteen meters, on average. Garmin: What is GPS?, <http://www.garmin.com/aboutGPS> (last visited Apr. 21, 2007). GPS devices can also determine an object's velocity (if it is in motion) and correlate its location with time. EL-RABBANY, *supra* note 190, at 8-9, 18-19.

¹⁹⁴ See, e.g., Stacy Finz & Michael Taylor, *Peterson Tracking Device Called Flawed, Defense Wants Evidence Shut Out of Trial*, S.F. CHRON., Feb. 12, 2004, at A17. A number of companies sell GPS devices designed to be surreptitiously installed on vehicles. See Covert GPS Vehicle Tracking Systems LLC, <http://www.covert-gps-vehicle-tracking-systems.com> (last visited Apr. 21, 2007); Datalogger GPS & Cellular Tracking Products, Spook Tech, <http://www.spooktech.com/trackingeqmt/datalogger.shtml> (last visited Apr. 21, 2007).

¹⁹⁵ See EL-RABBANY, *supra* note 190, at 10.

¹⁹⁶ *Who Knows Where You've Been?*, *supra* note 190, at 309; Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, N.Y. TIMES, Dec. 10, 2005, at A1.

¹⁹⁷ *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 750-51 (S.D. Tex. 2005).

¹⁹⁸ The 911 emergency response system is one example such a system. See How 911 Works, BellSouth, <http://contact.bellsouth.com/email/bbs/phase2/how911works.html> (last visited Apr. 21, 2007).

¹⁹⁹ The improvement of non-GPS wireless telephone location technology, as well as the increasing use of GPS in wireless phones, has been encouraged by legislation mandating compliance with standards for "wireless 911" systems, which automatically determine the location of people making emergency calls from wireless phones. See Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 615 (2000); *In re Application*

for *Pen Register*, 396 F. Supp. 2d at 755 (“This inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year.”); FCC 911 Service, 47 C.F.R. § 20.18 (2006); Darren Handler, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA. J.L. & TECH. 1, 6-9 (2005); Phillips, *supra* note 190, at 3-5.

The United States Congress has also required wireless service providers to facilitate law enforcement by ensuring that their systems can record the location of the antenna tower connected to a telephone at the beginning and end of each call. *See* 47 U.S.C. § 1002; U.S. Telecom Ass’n v. Fed. Comm’ns Comm’n, 227 F.3d 450, 462-64 (D.C. Cir. 2000); Third Report & Order, In the Matter of Communications Assistance for Law Enforcement Act, 14 F.C.C. Rec. 16794 (Aug. 31, 1999) [hereinafter Third Report & Order]. Notably, however, the Federal Communications Commission rejected the argument that providers must also be able to pinpoint the phone’s location throughout a call’s duration. *See* Third Report & Order, 14 F.C.C. Rec. at 16816 ¶ 46.

To date, Canadian regulators have not imposed specific requirements for wireless 911 location tracking, other than to require new providers to meet the capacities of established ones. *See* Gordon Gow, *Public Safety Telecommunications in Canada: Regulatory Intervention in the Development of Wireless E9-1-1*, 30 CAN. J. COMM. 65 (2004). Consequently, Canada has lagged behind the United States in the development of wireless 911 systems. While municipal governments and wireless and wireline service providers have voluntarily cooperated to develop systems, few providers are currently able to transmit precise location information to emergency operators. *See* COLIN J. BENNETT & LORI CROWE, REPORT TO THE PRIVACY COMMISSIONER OF CANADA, LOCATION BASED SERVICES AND THE SURVEILLANCE OF MOBILITY: AN ANALYSIS OF PRIVACY RISKS IN CANADA 9-14 (2005), available at <http://web.uvic.ca/polisci/bennett/pdf/LBSFINAL.pdf>.

For law enforcement purposes, Canadian wireless service providers are required to be capable of recording the most accurate location information available to them. This obligation stems from unpublished licensing conditions, *see* Solicitor General’s Enforcement Standards for Lawful Interception of Telecommunications (Rev. Nov. 95) (Can.), imposed by Ministerial fiat pursuant to § 5 of the Canada Radiocommunication Act, R.S.C. 1985, ch. R 2. *See* INDUS. CAN., SPECTRUM MANAGEMENT AND TELECOMMUNICATIONS POLICY: SPECTRUM LICENSING POLICY FOR CELLULAR AND INCUMBENT PERSONAL COMMUNICATIONS SERVICES (PCS) 10-11 (2003), available at [http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/pcspolicy_dec16_e_final.pdf/\\$FILE/pcspolicy_dec16_e_final.pdf](http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/pcspolicy_dec16_e_final.pdf/$FILE/pcspolicy_dec16_e_final.pdf); RICHARD-PHILIPPE MARTEL, OFF. OF THE PRIVACY COMM’R OF CAN., PRIVACY ON THE AIR (1998), available at http://www.privcom.gc.ca/speech/archive/02_05_a_981203_e.asp?V=Print#Wireless%20Mobile%20Communication%20Technologies%20Reveal%20Where%20We%20Go.

Improvements in wireless telephone tracking are also being spurred by commercial marketing strategies, including the placement of advertising and other content tied to profiles and real-time locations on consumers’ phones. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third-Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 382-84 (2006); Phillips, *supra* note 190, at 12; Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT L.J. 381, 381-82 (2003). In the United States, however, wireless carriers may not provide personally identifiable location information to commercial third parties in the absence of customers’ explicit consent. *See* Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 222(f).

may obtain wireless telephone location data in real time²⁰⁰ or from historical records maintained by service providers.²⁰¹ They may also use commercial wireless networks to track devices surreptitiously placed on vehicles or other objects.²⁰²

The question, then, is whether courts should find that these “second generation” radio tracking systems invade a reasonable expectation of privacy. As in the case of infrared searches, the conventional, morally grounded approach is not particularly helpful. Consider first the public exposure doctrine. By definition, people who venture into public spaces (such as streets and highways) voluntarily subject their movements and behaviors to observation. It can be argued that it is unreasonable to expect one’s public activities to remain private. Indeed, at least one court has relied on this argument in concluding that cell phone tracking does not trigger Fourth Amendment protection.²⁰³

As many commentators have pointed out, however, the public exposure doctrine fails to account for the fact that electronic tracking threatens the sense of anonymity that people often enjoy in public spaces.²⁰⁴ While we necessarily take the risk that our public behavior will be observed by others, these observations are typically sporadic and fleeting. As I discuss in more detail below, GPS and wireless telephone tracking systems allow authorities to surreptitiously monitor and record people’s movements in a systematic and detailed manner over an indefinite period of time. This kind of intensive surveillance is not analogous to the passing observations of strangers. Applying the public exposure doctrine to modern tracking technologies may thus fail to confer a normatively attractive degree of privacy.

The intimacy doctrine is similarly unhelpful. People’s public movements typically reveal only mundane information about them. Of course, this is not always true. Many people would not want it known that

²⁰⁰ Investigators seeking prospective wireless telephone location data usually obtain it from service providers; however, they may also have the ability to gather it directly. See *In re Application for Pen Register*, 396 F. Supp. 2d at 755 (citing U.S. DEP’T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 44-45 (2005 ed.)).

²⁰¹ See, e.g., *id.* at 748-49.

²⁰² See *id.* at 755 (citing Robert Stabe, *Electronic Surveillance—Non-Wiretap* § 3.31, in U.S. DEP’T OF JUSTICE, FEDERAL NARCOTICS PROSECUTIONS).

²⁰³ See *United States v. Forest*, 355 F.3d 942, 950-52 (6th Cir. 2004).

²⁰⁴ See Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1371-74 (2004); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 575-76 (1998); Otterberg, *supra* note 192, at 685-86; Pomerance, *supra* note 188, at 291.

they had visited a psychiatric institution, a gay bar, an adult video store, an extramarital lover's home, or a political or religious meeting. Arguably, using location tracking technologies to obtain this kind of information invades a reasonable expectation of privacy because it relates to a "biographical core of personal information" revealing "intimate details" of "lifestyle or private decisions."²⁰⁵

The problem with this argument, however, is that while intimate personal information may be obtained by sophisticated tracking technologies, it may also be obtained by unsophisticated, conventional surveillance. No reasonable expectation of privacy is triggered when the police discover extremely sensitive personal information simply by observing a suspect in public spaces. Yet it is reasonable to argue, as I elaborate in detail below, that electronic tracking should not be permitted without a warrant. Measuring the intimacy of the information that tracking technologies reveal, in other words, is of little assistance in deciding whether these technologies invade a reasonable expectation of privacy.²⁰⁶

A. PRIVACY COSTS

As in the case of infrared searches, cost-benefit analysis is more helpful. Consider first the social costs associated with recognizing a reasonable expectation of privacy in relation to tracking devices. Doing so would cause policing to become more expensive, less effective, or both. Contemporary technologies permit police to monitor suspects' movements with a great deal of precision,²⁰⁷ over a vast spatial expanse,²⁰⁸ and for very long periods of time.²⁰⁹ The financial costs to police of using these technologies, moreover, are relatively modest.²¹⁰

²⁰⁵ *R. v. Plant*, [1993] 3 S.C.R. 281 (Can.).

²⁰⁶ See BENNETT & CROWE, *supra* note 199, at 36-37.

²⁰⁷ See *supra* notes 193 and 198 and accompanying text.

²⁰⁸ As its name suggests, the geographic reach of GPS tracking is global. In Canada and the United States (as well as much of the rest of the world), wireless telephone networks are increasingly extensive. Only the very least densely populated parts of North America are exempt from coverage.

²⁰⁹ In the case of a surreptitiously planted GPS device, continuous surveillance is possible for the length of its battery's life. One company boasts that the batteries in its device may last up to thirty days. See TrimTracXS Internet GPS Car Tracking System—Real Time GPS Tracking, <http://www.brickhousesecurity.com/slimtrak-realtime-gps-tracking-car-locator.html> (last visited Apr. 21, 2007). If switched on, the GPS transceivers installed by vehicle manufacturers can function for an indefinite period, though service providers do not generally monitor the vehicle unless the subscriber initiates a service request, the vehicle is involved in an accident, or the provider is compelled by a court order. See, e.g., OnStar, OnStar Privacy Statement, http://www.onstar.com/us_english/jsp/privacy_policy.jsp (last visited Apr. 21, 2007). Wireless phone monitoring is possible

The most obvious substitute for prospective²¹¹ electronic tracking is visual surveillance. If police are interested only in obtaining location information, electronic tracking is far superior to visual surveillance. Compared to visual surveillance, electronic tracking requires less manpower, is more reliable (there is typically less danger of “losing” the target), and carries a lower risk of detection. These advantages multiply when police track the movements of several people at once. Without electronic assistance, tracking multiple people would typically require a substantial deployment of manpower. With electronic tracking, it could require only a single officer manning a video monitor.

If the police want to do more than simply track a suspect’s location (for instance, if they also want to interdict a drug transaction), or if the location information generated by electronic tracking is insufficiently precise, they may still need to deploy officers on the ground to conduct visual surveillance. In such cases, however, electronic tracking may still be helpful. Supplementing visual surveillance with electronic tracking allows police to use fewer officers and follow suspects from greater distances and more discreet vantage points.

The social costs of recognizing a reasonable expectation of privacy in retrospective²¹² electronic tracking are even greater than for prospective tracking, as there is no ready “low tech” substitute for retrospectively tracking a suspect’s movements. Retrospective location information is most commonly obtained from wireless telephone service providers. A suspect’s whereabouts at a given time in the past can sometimes be determined by other means, such as questioning the suspect or other people or obtaining credit card, banking, or other transactional records. Questioning may tip off the suspect, however, and result in the loss or destruction of evidence. More importantly, none of these methods provides the kind of continuous, historical record of the suspect’s movements

whenever the device is turned on.

²¹⁰ The costs associated with electronic tracking depend on a variety of factors, including the sophistication of the technology and whether police use their own systems or co-opt those of commercial service providers. As discussed in the text below, in most circumstances these costs are very likely to be significantly lower than those associated with analogous forms of surveillance.

²¹¹ By “prospective” tracking, I mean situations where police target suspects for surveillance and then capture location information from that time forward. Police may either track suspects in real-time or analyze location data at any time after it has been recorded.

²¹² By “retrospective” tracking, I mean situations where police obtain location information for a period during which they had not tracked a suspect’s location. Retrospective location information thus always derives from either records kept by third parties or less commonly, suspects themselves (as in the case of information inputted by suspects into their own GPS devices).

available from wireless providers.²¹³ If retrospective location tracking is held to invade a reasonable expectation of privacy, police lacking grounds to obtain a warrant would have to resort to much more costly, risky, and intrusive methods, such as undercover questioning.²¹⁴

B. PRIVACY BENEFITS

Would the widespread use of location tracking technologies create substantial avoidance or defensive costs? While it is difficult to be definitive, the answer is most likely “yes.” As mentioned, people who venture out into public spaces subject themselves to observation by others, including police. People take this into account, of course, often behaving differently in public than they would in private.²¹⁵

The chilling effects of this kind of observation are limited, however. While subject to observation, in most public spaces we enjoy anonymity. Others may see us doing something stigmatizing, but if they do not know who we are, this information is unlikely to be used against us. This anonymity frees people, as Melvin Gutterman has put it, to “merge into the ‘situational landscape.’”²¹⁶ Contemporary electronic tracking technologies threaten this freedom. Police could monitor an area for active transceivers (such as those embedded in wireless telephones or GPS-equipped vehicles), and if a person’s location or movements attracted their attention for some reason, his identity could be determined by cross-referencing the transceiver’s identification number with subscriber databases.

As discussed, public scrutiny is also typically brief and episodic. Our public behavior may be observed, but any one observer will generally only obtain a small fragment of information about us. If our activities are subject to prolonged, unwanted observation, we can usually take steps to preserve our privacy. Surreptitious visual observation is difficult, and in

²¹³ Wireless providers currently keep records (for varying lengths of time) of subscribers’ locations that are accurate to within approximately three hundred yards. See Richtel, *supra* note 196. European Union member states recently agreed to enact legislation requiring telecommunications service providers to retain records of telephone and Internet communications envelope data (including location data) for six to twenty-four months. See Parliament & Council Directive 2006/24/EC, 2006 O.J. (L105), 54 (E.C.). To date, there have not been any concrete proposals to enact similar legislation in the United States or Canada.

²¹⁴ The effectiveness of GPS and wireless telephone tracking, it should be noted, may be blunted by defensive measures. Criminals may switch off GPS chips in their cell phones, inspect possessions for planted tracking devices, use anonymous wireless phone services, or conduct business in places beyond the range of tracking systems. These measures impose costs, however, and may thereby diminish the rate of criminal activity.

²¹⁵ See Stigler, *supra* note 14, at 627.

²¹⁶ Gutterman, *supra* note 24, at 706.

most cases, people can confront or elude their observer. With GPS and wireless telephone tracking, in contrast, people generally do not know whether they are being monitored. These systems are also able to continuously track people's movements over both an extensive geographic space and lengthy period of time. This kind of surveillance may reveal patterns, associations, and activities that would not be apparent to casual observers.²¹⁷

Further, even when we observe non-anonymous, stigmatizing public behavior (for example, seeing a neighbor entering an adult video store), the person observed may be able to credibly deny the transgression to others.²¹⁸ Location tracking technologies, however, can generate reliable, permanent records, which dramatically diminish people's ability to successfully challenge harmful accusations.

Lastly, for most non-criminals, the risk of being subjected to prolonged visual surveillance by police is highly remote. Police resources are limited, and they are thus unlikely to monitor people who are not strongly suspected of criminal activity.²¹⁹ But as I have discussed, contemporary tracking systems can inexpensively and continuously monitor many subjects over an extensive geographic space. This could enable efficient monitoring of people who are only very weakly suspected of criminal activity. Police could use GPS or wireless telephone systems, for example, to track the movements of anyone carrying a transceiver in a "high crime" area or in the proximity of a suspected criminal or terrorist.

The non-anonymous, continuous, surreptitious, geographically and temporally extensive, reliable, and inexpensive character of GPS and wireless telephone tracking has the potential, therefore, to induce a much greater chill on productive behavior than visual observation. If there is a realistic possibility that police may monitor and record visitations to psychiatric clinics, AIDS testing centers, needle exchanges, women's shelters, mosques, and the like, then some people who would otherwise have engaged in socially beneficial activities in these places will not do

²¹⁷ See *State v. Jackson*, 76 P.3d 217, 262 (Wash. 2003); Otterberg, *supra* note 192, at 696-98; see also Blitz, *supra* note 204, at 1409-10; Nissenbaum, *supra* note 204, at 576-77.

²¹⁸ See *R. v. Duarte*, [1990] 1 S.C.R. 30, 51 (Can.) ("[I]f people in society come to believe [that participant surveillance] is widespread and done without probable cause, they may begin to fall silent on many occasions when previously they would have felt free to speak, confident in the belief that they could challenge the credibility or memory of the trusted colleague who would betray them." (citing *Commonwealth v. Schaeffer*, 536 A.2d 354, 365 (Pa. 1987))).

²¹⁹ See generally Otterberg, *supra* note 192, at 695 ("[T]hat the technology functions completely without police presence makes it less limited by the practical constraints of available human resources—and thus increases the potential for police abuse.").

so.²²⁰ The avoidance costs associated with location tracking are potentially quite substantial.

If the possibility of being monitored does not cause a person to avoid valuable activities, that person may nevertheless expend resources to prevent surveillance. Like criminals, non-criminals may attempt to thwart electronic location tracking, especially when they are engaged in sensitive activities. People may, for example, turn off their wireless phones or GPS devices. In doing so, however, they would forgo the many benefits conferred by these technologies. This must count as a significant cost of failing to regulate electronic tracking.

We must next ask whether the judicial regulation of tracking technologies is likely to prevent inefficient law enforcement expenditures. Unlike infrared cameras, which are used to detect only one form of criminal activity (indoor marijuana cultivation), electronic tracking is used in many different types of investigations. Most of these involve crimes that everyone agrees should be prohibited. Like wiretapping, however, electronic tracking captures a great deal of information about innocent activity. This creates a risk that police will use tracking technologies to monitor non-criminal behavior. Before the widespread adoption of statutory and constitutional protections against warrantless wiretapping, it was not uncommon for authorities to use it to monitor and intimidate members of unorthodox political groups.²²¹ There is also evidence that public video surveillance systems are frequently used to observe and harass minorities, women, and the poor.²²² Of course, regulating surveillance technologies cannot guarantee that they will not be misused; it does, however, make it difficult to establish the kind of extensive surveillance networks that facilitate widespread abuse.

²²⁰ GPS and wireless telephone tracking systems are being integrated with sophisticated mapping systems that correlate location with virtually any other kind of information relevant to police or emergency services personnel, such as crime statistics, business and housing types, and vehicle traffic data. See Phillips, *supra* note 190, at 5.

²²¹ See, e.g., COMM'N OF INQUIRY CONCERNING CERTAIN ACTIVITIES OF THE ROYAL CANADIAN MOUNTED POLICE, CERTAIN R.C.M.P. ACTIVITIES AND THE QUESTION OF GOVERNMENTAL KNOWLEDGE, THIRD REPORT/COMMISSION OF INQUIRY CONCERNING CERTAIN ACTIVITIES OF THE ROYAL CANADIAN MOUNTED POLICE (1981); David Berry, *The First Amendment and Law Enforcement Infiltration of Political Groups*, 56 S. CAL. L. REV. 207 (1982); Athan G. Theoharis, *FBI Surveillance: Past and Present*, 69 CORNELL L. REV. 883 (1984); *Developments in the Law—The National Security Interest and Civil Liberties: IV. Covert Government Surveillance*, 85 HARV. L. REV. 1244 (1972).

²²² See, e.g., CLIVE NORRIS & GARY ARMSTRONG, MAXIMUM SURVEILLANCE SOCIETY: THE RISE OF CCTV 108-16 (1999); John Fiske, *Surveilling the City: Whiteness, the Black Man and Democratic Totalitarianism*, 15 THEORY, CULTURE & SOC'Y 67 (1998).

There are other tools available to minimize abuses of surveillance technologies,²²³ especially when it is clear that police have targeted subjects for personal or political ends. Abuses are much more difficult to detect, however, when minorities are targeted in legitimate criminal investigations. As discussed, discriminatory profiling is most common in face-to-face confrontations between police and minorities, as in street and vehicle stops. These encounters often cause innocent suspects to feel embarrassed, stigmatized, and unfairly treated.

As in the case of infrared searches, police engaged in electronic tracking may not be aware of the race or ethnicity of the people being monitored. The unique identifier of the monitored transceivers, however, can be linked to users' identities, which can in turn be linked to databases containing information on race, ethnicity, and religious affiliation. Police can also supplement electronic tracking with visual surveillance, such as when they judge an individual's movements to be suspicious. In such cases, they may disproportionately select minorities for further investigation or surveillance. So while electronic tracking is less likely to cause discriminatory profiling than street or vehicle stops, it is more likely to do so than infrared searches.

To summarize, failing to regulate GPS and wireless telephone tracking is likely to impose substantial costs on society. Although it is difficult to assess the magnitude of these costs, a strong argument can be made that they probably outweigh the benefits of non-regulation. In any case, it is clear that unregulated electronic tracking is much more costly than unregulated infrared searching. Infrared searches reveal very little about what is happening inside people's homes. They simply indicate that an area, room, or building is substantially hotter than its surroundings. Combined with other information, this may provide a simple and reliable indicator that a structure is being used for a specific, criminal purpose. GPS and wireless telephone tracking systems, in contrast, reveal a great deal of information about non-criminal behavior. The disclosure of this information to the state has the potential to lead to substantial avoidance and defensive costs²²⁴ as well as abusive and discriminatory policing.

C. DECISION-MAKING ERROR

The forgoing analysis has demonstrated that both the benefits and costs associated with the unrestrained governmental use of location tracking

²²³ See, e.g., 18 U.S.C. § 3126 (2000); Canada Criminal Code, R.S.C., ch. C 46 § 195 (1985).

²²⁴ See Song, *supra* note 15, at 11.

technologies are substantial. Which legal institution—legislatures or courts—is best placed to decide which side of the ledger should prevail? As in the case of infrared imaging, tracking technologies are changing quickly. As discussed, contemporary GPS and wireless tracking systems are much more powerful and precise than the primitive beepers considered in *Knotts*, *Karo*, and *Wise*. And while it is clear that tracking devices will continue to become more accurate and prevalent, their future development cannot be predicted with anything approaching certainty. We do not know, for example, how precise or unobtrusive they may eventually become.²²⁵ Nor can we predict all of the ways in which they will be used by individuals and commercial service providers.²²⁶ Legislatures are better equipped to respond to this kind of technological flux than courts. As discussed, they have better access to technical information and are better placed to weigh voters' preferences on privacy and security concerns.

It is distinctly possible, however, that giving legislatures exclusive authority to regulate electronic tracking may disproportionately harm the interests of minorities and waste law enforcement resources. If this is true, and the private and social costs of these harms are not fully visible to legislators, then there may be a representation reinforcement justification for judicial intervention. As a result of their familiarity with the criminal investigative process and their political independence, judges may be better attuned to the disparate impacts of tracking technologies on minorities than legislators.

If legislatures are better placed than courts to weigh the overall benefits and costs of electronic tracking systems, but courts are more likely to account for disproportionate harms to minorities, how should judges go about determining the existence and extent of constitutional protection from this kind of surveillance? There is no easy answer to this question. It is sensible to begin, however, by examining how legislatures in the United States and Canada have dealt with location tracking technologies.

To date, Congress has not imposed any substantive limitations on the use of location tracking devices.²²⁷ Police are therefore free to use them

²²⁵ See, e.g., MOHINDER S. GREWAL ET AL., GLOBAL POSITIONING SYSTEMS, INERTIAL NAVIGATION, AND INTEGRATION 71-73 (2001); Alan Cameron & Josh Landers, *Taking Up Position in Covert Surveillance*, GPS WORLD, Aug. 2001, at 10; Michael Shaw, *Modernization of the Global Positioning System*, GPS WORLD, Sept. 2000, at 36.

²²⁶ See, e.g., Steven Levy, *A Future With Nowhere to Hide?*, NEWSWEEK, June 7, 2004, at 76; *The Policeman on Your Dashboard*, ECONOMIST, Sept. 17, 2005, at 12; *Something to Watch Over You*, ECONOMIST, Aug. 17, 2002, at 61.

²²⁷ However, Congress has restricted the use of location tracking in limited circumstances. The wireless 911 statute specifies that location information collected during 911 calls can only be disclosed for emergency response purposes. See Wireless

without either obtaining a warrant or establishing individualized suspicion.²²⁸ *Karo* established, however, that a reasonable expectation of privacy is triggered when the installation or monitoring of a tracking device intrudes on a constitutionally-protected area, such as a private residence. In such cases, police must obtain a warrant.²²⁹

Communication and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288 (codified at 47 U.S.C. § 222(f)). Congress has also declared that the envelope data supplied in response to pen/trap orders for wireless devices must not include location data, except insofar as location can be determined from telephone numbers. See 47 U.S.C. § 1002(a)(2)(B).

²²⁸ The few courts that have considered the question of whether warrantless GPS or wireless telephone tracking in public spaces violates the Fourth Amendment have all held that it does not. See *United States v. Forest*, 355 F.3d 942, 951-53 (6th Cir. 2004) (concluding that the use of cell site data to determine that a suspect had traveled from one municipality to another did not invade a reasonable expectation of privacy); *In re Application of the U.S. for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005) (holding that the issuance of a court order for retrospective cell site data associated with calls did not invade a reasonable expectation of privacy as location information was voluntarily disclosed to the service provider); *United States v. Moran*, 349 F. Supp. 2d 425, 467-68 (N.D.N.Y. 2005) (holding that use of a GPS tracking device on a suspect's vehicle did not invade a reasonable expectation of privacy). However, in *State v. Jackson*, the Washington Supreme Court concluded that the warrantless use of GPS tracking devices violates the state's constitution. 76 P.3d 217, 259-64 (Wash. 2003); see also *United States v. Berry*, 300 F. Supp. 2d 366, 367-68 (D. Md. 2004) (noting the similarities and differences between beepers and GPS tracking devices, but declining to decide whether monitoring of a GPS device constituted search); *People v. Lacey*, No. 2463N/02, 2004 WL 1040676, at *4-8 (N.Y. Co. Ct. May 6, 2004) (concluding that installation of a GPS device constituted a search under both federal and state constitutions, but denying application on the basis that defendant lacked standing).

²²⁹ A provision of the Electronic Communications Privacy Act authorizes courts to grant warrants for tracking devices that may move across district boundaries. See 18 U.S.C. § 3117(a). The provision does not speak to the standard for authorizing such warrants. Most courts have held that they must be issued under the authority of Rule 41 of the *Federal Rules of Criminal Procedure*, which authorizes searches for evidence on the basis of probable cause. See *In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. on Tel. Nos. [Sealed] and [Sealed] and Prod. of Real Time Cell Site Info.*, 402 F. Supp. 2d 597 (D. Md. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In re Application of the U.S. for an Order Authorizing (1) the Use of a Pen Register and a Trap and Trace Device*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005), *reconsideration denied*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005). But see *Application for an Order for Disclosure*, 405 F. Supp. 2d 435 (holding that the government may obtain the location of the connecting antenna tower at the beginning and end of calls on the basis of the "specific and articulable facts" standard set out in the Stored Communications Act (codified at 18 U.S.C. § 2703)). In *United States v. Karo*, the United States Supreme Court expressly declined to comment on whether electronic tracking in constitutionally protected areas could be justified by reasonable suspicion. 468 U.S. 705, 718 n.5 (1984).

A dramatic distinction exists in United States law, then, between tracking in public spaces, which is unregulated, and tracking in private spaces, which requires a warrant. Yet as we have seen, the use of GPS and wireless telephone tracking in public spaces creates substantial social costs. If the decision whether to regulate these technologies is left to Congress, there is a risk that it will fail to act in a fully representative fashion. But if judges intervene and recognize a reasonable expectation of privacy, there is a risk that they will overestimate the benefits and underestimate the costs of regulation.

One way to mitigate both of these risks is for courts to recognize an expectation of privacy, but require only that police justify tracking on the basis of reasonable suspicion.²³⁰ This would significantly diminish the potential for discriminatory profiling while maintaining law enforcement's ability to track when they have only a moderate degree of suspicion. If Congress determined that the social costs of GPS and wireless telephone

²³⁰ This standard is typically expressed in United States legislation and jurisprudence as "specific and articulable facts." *See, e.g.*, Stored Communications Act, 18 U.S.C. §§ 2703(c)-(d) (authorizing government access to non-content subscriber records held by a service provider); *Terry v. Ohio*, 392 U.S. 1, 21 (1968) (authorizing "stop and frisk" searches). In Canada, the same standard is expressed variously as "articulable cause," *see, e.g.*, *R. v. Simpson*, [1993] 12 O.R.3d 182, 199, 200-04 (Ont. C.A.) (Can.), "reasonable grounds to suspect" or "reasonable grounds to detain," *see, e.g.*, *R. v. Mann*, [2004] 3 S.C.R. 59 ¶¶ 30, 33, 45 (Can.), or "reasonable suspicion." *See, e.g.*, Canada Criminal Code, R.S.C., ch. C 46 §§ 492.1, 492.2 (1985).

Courts could require governments to meet an even lower standard to justify GPS and wireless telephone tracking. The standard of mere "relevance" to a criminal investigation is used, for example, for a number of statutory search powers in the United States. *See, e.g.*, 12 U.S.C. §§ 3402, 3407, 3408 (authorizing orders for financial records); 18 U.S.C. § 3123 (authorizing orders for pen registers and trap and trace devices). Recall, however, that these provisions were enacted after the Supreme Court ruled that these searches did not invade a reasonable expectation of privacy under the Fourth Amendment. As long as the application meets the formal requirements set out in the statute, courts must grant the authorization; they have no authority to undertake an independent evaluation of the relevance of the information sought. *See United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995); *In re United States*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994). Recall as well that while violations of these statutes may result in criminal sanctions, exclusion of evidence is not a remedy. *See supra* notes 137 and 141.

Even this very limited form of regulation would provide significant protection against discriminatory profiling. Requiring police to go to court to obtain an authorization imposes substantial logistical and economic restraints on their ability to arbitrarily select suspects for investigation. It also makes it virtually impossible to engage in the kind of mass surveillance of public spaces that GPS and wireless telephone tracking technologies make possible. There would likely be little difference in practice, then, between the standards of reasonable suspicion and relevance. Police are unlikely to invest the time and resources required to obtain a court authorization unless they have at least a reasonable suspicion that tracking will reveal evidence of criminal activity.

tracking justified the use of the probable cause standard, it would be free to legislate accordingly. Such a decision would be the product of a richer information environment than is generally available to courts.

This is essentially the approach taken by the Supreme Court of Canada in *Wise*. However, that decision considered first generation tracking technology. The question that Canadian courts now face is whether the legislative response to *Wise*, which authorizes tracking warrants on reasonable suspicion, complies with § 8 of the Charter when applied to GPS and wireless telephone tracking.²³¹ As the argument presented above suggests, the answer to this question should be “yes.” While GPS and wireless telephone tracking systems impose greater costs on society than the beepers considered in *Wise*, they also have greater benefits. Requiring warrants, even on the modest standard of reasonable suspicion, severely limits the risk of widespread stereotyping and discrimination. With this protection in place, the task of estimating the costs and benefits of tracking technologies and choosing an appropriate scheme to regulate them is best left to Parliament.

VI. CONCLUSION

The reasonable expectation of privacy test does not require a radical overhaul. Courts have cast it as a rough cost-benefit calculus and have generally crafted reasonable compromises between privacy and crime control interests. The test can undoubtedly be improved, however, and economic analysis can play an important role in this process, especially as

²³¹ Canada Criminal Code, R.S.C. ch. C 46 § 492.1. Another live question is whether this provision authorizes the monitoring of tracking devices that were not installed by government agents. The provision permits agents “to install, maintain, and remove a tracking device in or on any thing, including a thing carried, used or worn by any person . . . and to monitor, or to have monitored, a tracking device installed in or on any thing.” *Id.* “Tracking device” is defined as “any device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.” *Id.* While the first clause refers to the installation of the device by police, the subsequent clauses use the verb “install” in the passive voice, implying that it may be effected by non-state agents. *See id.* From a policy perspective, there would seem to be little reason to differentiate between devices installed by police and those used by commercial service providers. To date, there have been no reported decisions on either the interpretation or constitutionality of § 492.1 in the context of GPS or wireless telephone tracking. *See generally* R. v. Gerrard, No. CR-01-000176, CR-02-000154, 2003 W.C.B.J. LEXIS 225 (Ont. S.C. Feb. 12, 2003) (Can.) (considering police use of the general investigative warrant provision in § 487.01 of the Code (which requires reasonable and probable grounds) to install and monitor a GPS tracking device); R. v. T. & T. Fisheries Inc., [2005] P.E.I.J. No. 74 (P.E.I. P.C.) (Can.) (analyzing a § 492.1 warrant used by police to install and monitor a GPS tracking device).

emerging technologies threaten the vitality of traditional conceptions of privacy based on secrecy and intimacy.

The chief contribution of economics in this area is to provide a more rigorous and productive alternative to the moral conception of privacy that courts have conventionally relied on in making reasonable expectation of privacy decisions. Unlike the moral approach, the economic approach does not justify protecting privacy for its own sake, but rather because privacy often enhances social welfare by diminishing avoidance, defensive, and suboptimal enforcement costs. Economic analysis also suggests, however, that courts should refuse to recognize a reasonable expectation of privacy when doing so would generate few of these costs, but would significantly enhance deterrence. Economics and public choice theory can also reduce decision-making error by identifying the circumstances in which courts should be especially deferential to legislative choice, such as where a search technology is novel, technically complex, and undergoing rapid change, and its costs are borne by a broad swath of the population.

By these standards, infrared searches do not invade a reasonable expectation of privacy. They provide police with a powerful investigative tool, thereby enhancing the deterrence of crime, without producing (to any significant extent) the costs associated with the avoidance of productive activity, the prevention of privacy intrusions, the enforcement of inefficient criminal prohibitions, or the profiling of vulnerable minorities. The economic approach confirms that the Supreme Court of Canada in *Tessling* (and not the majority of the United States Supreme Court in *Kyllo*) correctly concluded that warrantless infrared searches are constitutional. It also suggests that courts should defer to legislatures in deciding whether and how to regulate future, potentially more intrusive infrared technologies, so long as these technologies do not disproportionately harm minorities.

The case for recognizing a reasonable expectation of privacy in relation to GPS and wireless telephone tracking is much stronger. The privacy costs associated with these technologies are substantially greater than for infrared searches. Location tracking has the potential to produce substantial avoidance and defensive costs. It may also increase the risk of discriminatory profiling. In addition, the case for legislative deference is weaker for GPS and wireless telephone tracking than for infrared searches. The complexity and rapid development of tracking technologies militate in favor of legislative regulation, but legislatures are unlikely to fully account for disproportionate impacts on minority suspects. The best solution may therefore be for courts to recognize a minimal expectation of privacy that would require warrants based on reasonable suspicion. This would provide considerable protection against discriminatory profiling without usurping

the legislature's capacity to determine the need for more extensive regulation.

