Boston College Law Review

Volume 46
Issue 1 *Number 1*

Article 2

12-1-2004

The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment

Sam Kamin
skamin@law.du.edu

THE PRIVATE IS PUBLIC: THE RELEVANCE OF PRIVATE ACTORS IN DEFINING THE FOURTH AMENDMENT

SAM KAMIN*

Abstract: Because the Fourth Amendment regulates only governmental conduct, the behavior of private actors is almost wholly absent from academic Fourth Amendment literature. This Article argues that this exclusive focus on official conduct is myopic. Because the U.S. Supreme Court often looks to the conduct of *private* actors to determine the scope of permissible government conduct, a Fourth Amendment approach that ignores the invasions engaged in by these private actors is likely to concede questions regarding important civil liberties before the government even acts. This Article traces the development of Fourth Amendment jurisprudence, explaining the origins of the Court's current focus on private conduct. It then describes the current state of private intrusions upon privacy, arguing that emerging technologies have facilitated an exponential growth in the capacity of private actors to obtain and process private information. This expansion in private searching will likely lead courts to uphold similar invasions of privacy when government agents engage in the same kind of conduct. Finally, this Article proposes legal, legislative, and practical solutions to the current privacy crisis, and reluctantly concludes that only individual, practical steps are likely to produce effective privacy expansions in the near term.

INTRODUCTION

In early 2004, the U.S. Justice Department made headlines and inflamed privacy groups when it subpoenaed medical records from a

* © 2004 Sam Kamin, Assistant Professor of Law, University of Denver College of Law. This Article was made possible by a summer research grant from the University of Denver College of Law. Phillip Reinert and Brian Rodeno provided spectacular research assistance. Thanks are due to Viva Moffat, Mark L. Miller, Alan Chen, Thomas Russell, Christopher Slobogin, Phil Weiser, Marianne Wesson, Martin Katz, Phillip Gordon, and all the nice people at Pablo's on Sixth who make their café americanos strong. Needless to say, all errors and omissions remain the responsibility of the author. Some of the ideas contained in this Article appeared in a short essay in the *University of Denver Law Review*. *See generally* Sam Kamin, *Little Brothers Are Watching You: The Importance of Private Actors in the Making of Fourth Amendment Law*, 79 DENV. U. L. REV. 517 (2002).

number of abortion providers around the country.[1] The Bush administration claimed that the records were necessary to defend legal challenges to the late-term abortion ban that was signed into law the previous year.[2] A federal judge disagreed, however, and granted a Chicago hospital's motion to quash the subpoenas.[3] Undaunted, the Justice Department continues to press its subpoenas in several other states.[4]

The Bush administration's attempt to force the release of private medical records is only one in a series of high-profile actions that have drawn the ire of privacy groups. For example, in late 2002, the administration announced its plans for Total Information Awareness, a federal program that would combine information from public and private records to create a macro database of individually identifiable information.[5] Although negative publicity forced the administration to curtail its plans for Total Information Awareness,[6] there is evidence that the administration is still pursuing many of the program's goals by other means.[7]

Although these high-profile governmental attempts to obtain private information have rightly made headlines, I argue that a possibly greater threat to privacy has been largely ignored—the actions of private actors in gaining access to information to which they historically lacked access. In this Article, I argue that the focus on state actors—by the media, by scholars, and by interest groups—is myopic and ill-serves the interests of privacy. My thesis in this Article is that this ex-

---

[1] Erich Lichtblau, *Ashcroft Defends Subpoenas*, N.Y. TIMES, Feb. 13, 2004, at A27.

[2] Nat'l Abortion Fed'n v. Ashcroft, No. 04 C 55, 2004 WL 292079, at *1 (N.D. Ill. Feb. 6, 2004).

[3] *See id.*

[4] *U.S. Seeks Late-Term Abortion Records*, L.A. TIMES, Feb. 13, 2004, at A31.

[5] John Markoff, *Pentagon Plans a Computer System That Would Peer at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12.

[6] *See* Adam Clymer, *Senate Rejects Pentagon Plan to Mine Citizens' Personal Data for Clues to Terrorism*, N.Y. TIMES, Jan. 24, 2003, at A12.

[7] An editorial published in the *San Francisco Chronicle* in 2004, claimed the following:

> When retired Adm. John Poindexter left government service last year, it was widely believed that his misguided scheme to collect private data on U.S. citizens was gone for good, too. It was a bad assumption. The Poindexter-inspired drive to electronically surveil and compile dossiers on millions of Americans is apparently still in gear.

Editorial, *Data Mining Schemes*, S.F. CHRON., Feb. 27, 2004, at A26, 2004 WLNR 7625556; *see* Michael Sniffen, *Controversial Data-Mining Project Lives On*, CMP TECHWEB, Feb. 23, 2004, (claiming that "[t]he government is still financing research to create powerful tools that could mine millions of public and private records for information about terrorists despite an uproar last year over fears it might ensnare innocent Americans"), http://informationweek.com/story/showArticle.jhtml?articleID=18100004 (last visited Jan. 31, 2005).

clusive focus on state action ignores the fact that, as it is currently interpreted by the U.S. Supreme Court, the Fourth Amendment's coverage depends crucially on the scope of private actors' conduct.[8]

This is true not because private action is subject to the requirements of the Fourth Amendment; it is not.[9] Rather, private conduct is crucial because courts will examine that conduct to determine whether an individual has a reasonable expectation of privacy in an area that a government actor has invaded.[10] If an individual has allowed private actors access to that area, she generally will not be permitted to complain that her rights have been violated when the government seeks access to that area as well.[11] Thus, the consistent failure

---

[8] *See infra* notes 59–149 and accompanying text.

[9] *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989) (stating that "the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative"); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (finding that the Fourth Amendment's "origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies").

Private actors whose conduct is so intertwined with that of state law enforcement authorities that they may be considered state actors are the exception to this rule. *See* Jackson v. Metro. Edison Co., 419 U.S. 345, 351 (1974) (holding that, in general, the Constitution does not purport to govern private conduct, and that the behavior of private individuals will not be attributed to the state unless there is a "sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself"); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 508 (1985) (arguing that "[p]rivate behavior need comply with the Constitution only if the state is so intimately involved in the conduct—that is, if the nexus to the state is so great—that the state can be held responsible for the activity"). Professor Paul Brest provided the following explanation:

> The state action doctrine originated in the *Civil Rights Cases*, in which the Supreme Court held that the fourteenth amendment did not authorize Congress to prohibit discrimination by privately owned inns, conveyances, and places of amusement; rather, its purpose was to "provide modes of redress against the operation of state laws, and the action of state officers executive or judicial, when these are subversive of the fundamental rights specified in the amendment."

See Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296, 1300 (1982) (quoting the Civil Rights Cases, 109 U.S. 3, 11 (1883) (citation omitted)).

[10] Throughout, I use the word "area" to describe the thing being searched. I mean to include within this phrase those intangible places and things in which one might reasonably wish to maintain an expectation of privacy—e-mails, conversations, medical records—as well as tangible areas such as cars, houses, and offices. Of course, as I discuss below, the idea that tangible and intangible things or places are afforded the same protection is a relatively new idea. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928); *infra* notes 37–43 and accompanying text.

[11] *See infra* notes 74–84 and accompanying text.

of scholars and privacy advocates to examine the role of private conduct in defining the Fourth Amendment has the effect of ceding the legal battle for protection from government intrusion before that intrusion has even taken place.

This Article proceeds in four parts. First, in Part I, I trace the development of the Supreme Court's current understanding of the Fourth Amendment.[12] I follow the Court's jurisprudence from one based on a strict, historical reading of the text of the Fourth Amendment to an interpretation based on the concept of reasonable expectations of privacy. This latter test, developed in 1967, in *Katz v. United States*,[13] remains the fundamental Fourth Amendment paradigm today.

Next, in Part II, I discuss how the *Katz* standard has been applied in recent years.[14] I demonstrate that in determining whether or not a reasonable expectation of privacy exists when the government invades an area in which a defendant[15] asserts a right to privacy, courts pay particular attention to whether a private actor could have done what the government in fact did. If the answer to that question is yes, courts generally find no reasonable expectation of privacy, and hence, no Fourth Amendment protections. I will show that the Court's doctrine now focuses on the practical capacity of other actors to invade a defendant's privacy rather than on the legality of that conduct; even if government actors are acting in a way that could be punished if done by a private actor, courts will find no reasonable expectation of privacy if such an illegal invasion by a private actor was foreseeable.

In Part III, I show how recent technological innovations have made courts' focus on private conduct particularly troubling for those concerned about the reach of government surveillance.[16] As technologies make it easier for employers, insurers, and even simple snoops to gain access to previously private areas, members of the public have, to a large extent, taken for granted the fact that many eyes are watching them. Those who accept this private snooping may not realize, however, that by permitting these prying eyes to investigate them, they have essentially consented to government surveillance as well.

---

[12] *See infra* notes 19–58 and accompanying text.

[13] 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[14] *See infra* notes 59–149 and accompanying text.

[15] Fourth Amendment claims can be raised either by defendants seeking the exclusion of evidence in a criminal trial or by plaintiffs alleging a violation of their rights. For simplicity, I refer generically throughout to the Fourth Amendment claimant as a defendant.

[16] *See infra* notes 150–242 and accompanying text.

Finally, Part IV looks to the future.[17] I argue that the current scope of the Fourth Amendment is unlikely to change in the near term. If anything, the Supreme Court's recent decision in *Kyllo v. United States* is the apotheosis of the focus on private conduct to define the contours of the Fourth Amendment.[18] Similarly, I argue that laws designed to protect individuals from one another are unlikely to be useful in protecting individuals from their government. Because the courts have refused to find consistently that conduct by a government official that would contravene a civil statute violates an individual's reasonable expectation of privacy per se, such statutes are perhaps worse than useless in regulating government conduct. Because these statutes can give individuals the false sense that their privacy is protected, they may have the effect of providing less protection, rather than more, against governmental invasions of privacy. I argue instead that the only way for individuals to gain protection against governmental intrusions into their privacy is to actively seek to protect their private information from all prying eyes, public and private.

I. The Modern Understanding of the Fourth Amendment

A. *The Text*

Although a general right to privacy has been read into a number of the guarantees in the Bill of Rights,[19] the privacy rights of the people vis-à-vis the government are protected most fundamentally by the Fourth Amendment of the U.S. Constitution,[20] which provides:

> 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

---

[17] *See infra* notes 253–274 and accompanying text.

[18] *See* 533 U.S. 27, 40 (2001).

[19] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (finding a right to privacy in the penumbras of the First, Third, Fourth, Fifth, and Ninth Amendments of the U.S. Constitution).

[20] Various provisions of the Fourth Amendment have been incorporated into the Fourteenth Amendment's guarantee of due process of law, making it applicable to the states as well as the federal government. *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 655 (1961) (enforcing the exclusionary rule against the states).

> particularly describing the place to be searched, and the persons or things to be seized.[21]

The Amendment is generally interpreted as containing two clauses: one speaking to unreasonable searches and seizures, and the other discussing the requirements for the issuance of warrants. The relationship between these two clauses is murky at best and has been the topic of much controversy in the two-hundred-plus years since their drafting.[22] Faced with an essentially inscrutable text, the U.S. Supreme Court has generated a number of interpretive rules that find varying degrees of support in the text of the Amendment—the Amendment expresses a strong preference for searches conducted pursuant to judicially approved warrants;[23] all searches, whether subject to the war-

---

[21] U.S. CONST. amend. IV.

[22] *See, e.g.*, NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 100–03 (1937). Nelson B. Lasson writes that the confusion regarding the two clauses is essentially a result of misreporting by one of the drafters. *Id.* at 101–02. He notes that the House of Representatives originally approved a draft of what would become the Fourth Amendment that read,

> The rights of the people to be secured in their persons, their houses, their papers, and their other property, from all unreasonable searches and seizures, *shall not be violated by warrants issued without probable cause*, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.

Id. at 100 n.77 (emphasis added). Although the relationship between the two clauses is relatively straightforward in this draft, the House's Reporting Committee reported that the House approved the version with which we are now familiar, which contained amendments the House had in fact rejected. *Id.* at 101. *But see* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 718–19 (1999) (arguing that the evidence that the current version of the Fourth Amendment is not the one that was approved by the House of Representatives is "inconsistent").

[23] For example, in *Coolidge v. New Hampshire*, the Supreme Court stated the following:

> It is accepted, at least as a matter of principle, that a search or seizure carried out on a suspect's premises without a warrant is *per se* unreasonable, unless the police can show that it falls within one of a carefully defined set of exceptions based on the presence of "exigent circumstances."

403 U.S. 443, 474 (1971). Exceptions to the probable cause and warrant requirements include the following:

> [I]nvestigatory detentions, warrantless arrests, searches incident to a valid arrest, seizure of items in plain view, exigent circumstances, consent searches, vehicle searches, container searches, inventory searches, border searches, searches at sea, administrative searches, and searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.

Theodore P. Metzler et al., *Warrantless Searches and Seizures*, 89 GEO. L.J. 1084, 1084 (2001).

rant requirement or not, must generally be supported by probable cause;[24] and the ultimate constitutional test for every search is reasonableness.[25] Although each of these interpretations is now taken more or less as orthodoxy, these heuristics are inherently inconsistent, and none of them is entirely free from controversy.[26]

Thus, at its most fundamental levels—the relationship between the Amendment's two clauses and the degree of suspicion that must be shown before a warrantless search may be conducted—it becomes clear that the Fourth Amendment is hardly self-defining. These problems of construction are compounded by the fact that at the time of the Amendment's drafting, conceptions of privacy, crime, and policing were fundamentally different than they are today. For example, there were no organized police forces during the founding period. Rather, law enforcement was handled exclusively by part-timers and amateurs.[27] Although crime as we know it today clearly existed in co-

---

[24] *See, e.g.*, Chambers v. Maroney, 399 U.S. 42, 51 (1970) (stating that "[i]n enforcing the Fourth Amendment's prohibition against unreasonable searches and seizures, the Court has insisted upon probable cause as a minimum requirement for a reasonable search permitted by the Constitution"). *But see* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 624 (1989) (permitting alcohol and drug testing after railway accidents even in the absence of individualized suspicion); Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (permitting brief detentions for investigative purposes based upon the lesser standard of reasonable suspicion).

[25] *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) (Scalia, J.) (explaining that "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness'").

[26] *See, e.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 10–17 (1997) (arguing that the Founders were deeply skeptical of judicially-issued warrants and that the Fourth Amendment should be read as mandating that all searches be reasonable rather than as expressing a preference for warranted searches); *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757, 761 (1994) (arguing that the Supreme Court has misconstrued not only the relationship between the Fourth Amendment's two clauses, but also two other pillars of Fourth Amendment jurisprudence—the requirement of probable cause for all searches and the application of the exclusionary rule to all Fourth Amendment violations); Davies, *supra* note 22, at 591 (arguing that a general reasonableness test would have been unimaginable to the Founders).

[27] *See, e.g.*, Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 830–32 (1994). Professor Carol S. Steiker stated the following:

> Our twentieth-century police and even our contemporary sense of "policing" would be utterly foreign to our colonial forebears. Law enforcement in colonial times was, as legal historian Lawrence Friedman tells us, "a business of amateurs." Public order was maintained by a loose system of sheriffs, constables, and night watchmen. Most counties had a sheriff, appointed by the governor of the colony as the chief law enforcement officer, in charge not only of jails and prisoners, but of jury selection as well. But sheriffs had no professional law enforcement staffs under their direction. Instead, ordinary citizens who were employed in other trades or professions as their means of

lonial times, the physical fear of crime as a social phenomenon and as a political issue simply did not. Today, the primary conundrum of crime in the United States is generally seen as the importance of protecting the public from predation while protecting individuals from the invasive power of the state.[28] By contrast, crime in colonial times was feared not so much as a threat to individual safety, but as a threat to the moral and social order.[29] Furthermore, the main privacy con-

---

livelihood took turns serving as constables during the day or watchmen during the night. The constabulary "carried the main burden of law enforcement," as its members were required to patrol during the day as well as supervise the night watch. Serving as a constable was an unpopular task, however, and many towns had difficulty maintaining an adequate presence. The constables generally served without training, uniforms, weapons, or other accoutrements of modern law enforcement officers. They ordinarily did not receive stipends, but were sometimes compensated by private individuals for the return of stolen property. The night watch was equally amateurish: early attempts to have a paid watch in New York and Boston ultimately failed because it was so expensive; thus, the watch was generally staffed by requiring all citizens to take a turn "in the duty of watch and ward."

The constabulary and the watch differed from modern law enforcement structures not only in personnel, but in function; their duties often strayed quite far from our modern notions of peacekeeping and investigation. For example, one of the earliest colonial constables had duties that included announcing marriages approved by civil authority and serving as "Sealer of Weights and Measures" and "Surveyor of Land." Urban constables were generally charged with monitoring the condition of "streets, sidewalks, privies, [and] slaughterhouses." The night watchmen usually were required to call out the hour and the weather; sometimes they were entrusted with the care of street lamps as well. Indeed, it was not until well into the nineteenth century that some urban authorities declared that it had "become necessary that in every large town there should be several intelligent and experienced men devoting their time and skill to the pursuit and arrest of . . . robbers, housebreakers, pickpockets, and other felons." The duties of constables and night watchmen never developed into the job of investigative "policing" with which modern law enforcement agencies are charged.

Id. (citations omitted).

[28] *See generally* Herbert L. Packer, *Two Models of Criminal Process*, 113 U. PA. L. REV. 1 (1964) (arguing that two contrasting views of the criminal justice system inevitably compete—one based on crime control, efficiency and finality, the other on providing due process and individualized consideration).

[29] *See, e.g.*, LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 34 (1993). Professor Lawrence M. Friedman stated the following:

> Since crimes were sins, and sins crime, there was no sharp line between "victimless crimes" and crimes of predation or violence. The idea of a victimless crime is distinctly modern. An offense against God was an offense against society, and a positive threat to the social order. When Sodom and Gomorrah flouted God's will, his anger laid them waste.

cern of the Founders generally was not searches by police officers in pursuit of criminal prosecutions, but rather wide-ranging and unfettered searches by customs and tax inspectors or by officials of the Crown looking for materials deemed seditious.[30] In fact, during the founding period, Fourth Amendment claims were rarely even raised in the criminal context. At that time, the legality of a search usually was contested as a defense to a civil trespass action rather than in the course of a criminal prosecution.[31] One primary reason for this, of course, is the fact that the exclusionary rule is entirely an invention of the twentieth century;[32] it likely would have come as a surprise to the Founders that otherwise competent evidence would not be admitted in court because of the means by which it was obtained.

Thus, even if the text of the Fourth Amendment were clear in its terms (and it is not), applying in contemporary times a document

---

Id. Thus, according to Professor Friedman, crime was a threat not simply to its direct victims but to both the perpetrators and to society as a whole. *See id.*

[30] *See, e.g.*, William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 394 (1995). William J. Stuntz stated the following:

> Privacy protection in the past had little to do with ordinary criminal procedure. The Fourth and Fifth Amendments arose out of heresy investigations and seditious libel cases, not murders and robberies. In the late nineteenth century, when the Supreme Court first took a hand in crafting Fourth and Fifth Amendment law, the key cases involved railroad regulation and antitrust—again, a far cry from ordinary criminal litigation. In both the eighteenth and nineteenth centuries, the law's primary effect seems to have been to make it harder to prosecute objectionable crimes—heresy, sedition, or unpopular trade offenses in the seventeenth and eighteenth centuries, regulatory offenses in the late nineteenth century. To a surprising degree, the history of criminal procedure is not really about procedure at all but about substantive issues, about what conduct the government should and should not be able to punish.

Id. Similarly, Nelson B. Lasson cites as the main impetus for the protections of the Fourth Amendment, and its state analogues, a number of cases, both from the colonies and England, involving the enforcement of unpopular tax and sedition laws. LASSON, *supra* note 22, at 42–78.

[31] *See, e.g.*, Entick v. Carrington, 95 Eng. Rep. 807, 817 (K.B. 1765) (rejecting the defense of agents of the Crown in a trespass action on the ground that the search they conducted left too much discretion to those charged with its execution); Wilkes v. Wood, 98 Eng. Rep. 489, 498–99 (K.B. 1763) (finding that a general warrant is insufficient to permit an entry into plaintiff's home).

[32] *See, e.g.*, *Mapp*, 367 U.S. at 648 (stating that "in the Weeks case, this Court 'for the first time' held that 'in a federal prosecution the Fourth Amendment barred the use of evidence secured through an illegal search and seizure'") (quoting Wolf v. Colorado, 338 U.S. 25, 28 (1949)); Weeks v. United States, 232 U.S. 383, 398 (1914) (establishing for the first time that the exclusionary rule is a necessary corollary of the rights guaranteed in the Fourth Amendment).

written in a very different context and addressing very different concerns is a task necessarily requiring a certain amount of inventiveness on the part of jurists.[33] For example, how is one to determine, parsing the fifty-four words of the Amendment, whether or not police officers may conduct a warrantless search of a paper bag contained in the trunk of a suspicious automobile,[34] whether federal officers may "massage" a duffle bag in the luggage compartment of a bus,[35] or whether law enforcement officials may fly over private property in a borrowed aircraft to peer through the semi-opaque roof of a shed?[36] The short answer, of course, is that neither the text of the Amendment nor founding-era understandings of its meaning are likely to provide consistent answers to these questions. Rather, judges must turn elsewhere to determine the scope of the Amendment's protections in contemporary society. It is to these alternative means of interpreting the Fourth Amendment that I now turn.

B. *Interpreting the Text*

An early example of the hermeneutic difficulties posed by the Fourth Amendment is presented by the 1928 case of *Olmstead v. United States*.[37] In *Olmstead*, the government tapped the defendant's office telephone in a way that constituted no trespass upon his property.[38] The connections were all made either in the common basement of an

---

[33] Of course, all of the Constitution's provisions are applied in a context unimaginable to the Founders. One could argue, for example, that one of the problems in interpreting the Commerce Clause today is the way interstate and foreign commerce has changed since 1789. *See generally* Randy E. Barnett, *New Evidence of the Original Meaning of the Commerce Clause*, 55 ARK. L. REV. 847 (2003) (discussing the difficulties of interpreting the Commerce Clause in a modern age). The Founders were aware, however, of interstate and foreign commerce in a way in which they simply were not familiar with the modern conceptions of crime and law enforcement.

[34] *See, e.g.*, United States v. Ross, 456 U.S. 798, 820–22 (1982) (finding that when police officers have probable cause to believe that contraband may be found in a car's trunk, they may search any closed containers within the trunk that might contain the contraband).

[35] *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000) (finding that the physical manipulation of carry-on baggage in an overhead compartment was a search for purposes of the Fourth Amendment).

[36] *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451–52 (1989) (plurality opinion) (finding that because the officers were in Federal Aviation Administration approved air space, they were only doing what a member of the public could have done, and the defendant had thus assumed the risk that his illegal crop would be discovered).

[37] *See* 277 U.S. 438, 464 (1928).

[38] *Id.* at 457.

apartment building or on public wires.[39] Based on conversations overheard via the wiretap, the officers obtained enough information to prosecute defendant Roy Olmstead and obtain a conviction.[40] Olmstead appealed, arguing as he had at trial that the tapping of his phone was a search, and that because the search was conducted without a warrant, it was presumptively unconstitutional and its fruits must be suppressed.[41]

Relying on a literal reading of the text of the Fourth Amendment, the government argued that the Constitution simply was not implicated when the government eavesdropped on the defendant's phone calls. The Supreme Court agreed:

> The [Fourth] Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects. The description of the warrant necessary to make the proceeding lawful, is that it must specify the place to be searched and the person or *things* to be seized.
>
> . . . .
>
> . . . The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.[42]

The Court arrived at this conclusion by means of a very close reading of the text of the Amendment. An electronic interception of a conversation fails to qualify as a search both because of the area searched and the method used. The thing "searched" is—unlike persons, houses, papers, and effects—intangible. When the Constitution speaks of the things that are protected from unreasonable search and seizure, it speaks of substantial things on which hands can be laid. Similarly, the method used by law enforcement—listening remotely by wire—is neither a search nor a seizure because it does not involve the physical tak-

---

[39] *Id.* As we have seen, the absence of a physical trespass on the defendant's property historically was viewed as critically important, given the historical link that existed between the Fourth Amendment and property rights. *See supra* notes 27–31 and accompanying text. As we shall see, however, in the latter half of the twentieth century, courts have moved away from a property-based Fourth Amendment jurisprudence. *See infra* notes 132–143 and accompanying text.

[40] *See Olmstead*, 277 U.S. at 455.

[41] *See id.* at 471 (Brandeis, J., dissenting).

[42] *Id.* at 464.

ing, touching, and inspecting that the text of the Amendment appeared to envision.

As a reading of a text, this interpretation of the Fourth Amendment is almost entirely unassailable. In fact, the concept of either searching or seizing a conversation is one that strains any ordinary understanding of those words. As an attempt to understand the text in context, however—to recover the spirit behind the text—the *Olmstead* reading is somewhat cramped.[43] To the extent that the Fourth Amendment was written to be a check on the capacity of law enforcement officials to conduct broad, invasive investigations based on little or no suspicion, the *Olmstead* Court's reading does the Amendment little justice. So long as law enforcement officials snoop by means not imagined by the Founders or investigate areas not explicitly mentioned in the Amendment's text, it would seem their actions will not offend the Constitution. Nonetheless, it would be thirty-eight years before the Court abandoned this narrow reading of the Fourth Amendment.

C. Katz v. United States—*A Paradigm Shift*

In 1967, the Supreme Court's decision in *Katz v. United States*[44] established a new approach to the question of when a government investigation becomes a search, an approach that remains critical to understanding the Fourth Amendment today. In *Katz*, the Court dealt again with government wiretapping, this time of a public phone booth by federal agents anxious to show that defendant Charles Katz was using the phone booth to make book on sporting events.[45] The wiretap was achieved by placing a recording device on the outside of the booth and activating it only when Katz was seen entering the booth.[46] Katz's phone calls were recorded, thus allowing the government to obtain enough evidence to secure a conviction for violation of the federal bookmaking statutes.[47]

On appeal from this conviction, Katz argued that the telephone booth was an area entitled to Fourth Amendment protections.[48] The

---

[43] *See generally* WILLIAM N. ESKRIDGE, JR., DYNAMIC STATUTORY INTERPRETATION (1994); William N. Eskridge, Jr., *Fetch Some Soupmeat*, 16 CARDOZO L. REV. 2209, 2218 n.43 (1995) (citing articles and arguing that "[m]ost theorizing about statutory interpretation since 1982 has emphasized the ways in which statutes evolve").

[44] *See* 389 U.S. 347, 351 (1967).

[45] *Id.* at 348.

[46] *See id.* at 348–49.

[47] *Id.* at 348.

[48] *Id.* at 349.

government, relying on *Olmstead*, argued to the contrary—because no physical search or seizure was made and because no tangible thing was searched or seized, the Fourth Amendment simply was not implicated by placing a listening device on top of the phone booth.[49]

In a decisive shift from *Olmstead*, the Court agreed with the defendant that the Fourth Amendment was implicated when the telephone booth was tapped.[50] But the Court went beyond merely holding that an intangible search can implicate the Fourth Amendment in the same way that a tangible search can; rather, it fundamentally changed the way in which the Amendment's protections are conceived:

> Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a "constitutionally protected area." The Government has maintained with equal vigor that it was not. But this effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case. *For the Fourth Amendment protects people, not places.* 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.[51]

Katz demonstrated that the Supreme Court was no longer inclined to limit the Amendment to a narrow reading of its text. Rather than focusing on the particular area or thing searched and attempting to determine whether that was an area or a thing meant to be protected by the Founders, the Court found that the proper focus of Fourth Amendment analysis is on the individual whose person or property is searched and on the society in which that person lives. If the defendant has acted to keep the area searched private, and if society is willing to acknowledge the reasonableness of that expectation of privacy,[52] then

---

[49] *Katz*, 389 U.S. at 349, 352.

[50] *Id.* at 351–52.

[51] *Id.* (citation omitted) (emphasis added).

[52] In his concurrence, Justice John Marshall Harlan expressed the Supreme Court's new test in terms of these two elements, stating, "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expecta-

the Fourth Amendment is implicated when that area is investigated by law enforcement.[53] If a defendant has not taken steps to keep her actions private or if society is not prepared to validate an expectation of privacy, however, then the Fourth Amendment is not implicated, even if the search involves one of the areas—houses, persons, papers, and effects—explicitly protected by the Amendment's text.[54]

D. *Criticisms of* Katz

Although the *Katz* approach is certainly less faithful to the text of the Fourth Amendment than was *Olmstead*, commentators have argued over the last three and a half decades about whether the new standard affords greater or lesser protection to individuals than did the older, more textual approach. In fact, during this time, *Katz* has been subject to serious criticisms from both the right[55] and the left.[56] Those on the left have seen it as an insufficient guarantee against invasions of privacy because the Amendment's protections are apparently made contingent

---

tion be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring). This is the current understanding of the test. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing *Katz*, 389 U.S. at 360–62 (Harlan, J., concurring)) (discussing Justice Harlan's concurrence in explicating *Katz*).

[53] *See Katz*, 389 U.S. at 351–52.

[54] *See id.*

[55] *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (explaining that "the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable,"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable" (citations omitted)); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 186, 188 (describing the conception of privacy as treated by *Katz* as "too obvious to merit extended discussion" and arguing that the contradictions created by the *Katz* formulation are based on "threadbare arguments"); *see also Griswold*, 381 U.S. at 508–09 (Black, J., dissenting) (arguing that a move from concrete conceptions such as searches and seizures to more nebulous ones such as privacy was unlikely to be protective of individual rights).

[56] *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1294–95 (1981) (arguing that the *Katz* test created "a new graduated approach to the fourth amendment that is based on the recognition of degrees of privacy expectations," which, at least under the Burger Court, "resulted in a dangerous narrowing of the fourth amendment's substantive scope"); Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049, 1066 n.64 (1999) ("Though *Katz* itself seemed to extend the Fourth Amendment's reach, the Court's protection of privacy since *Katz* has been less than generous. The reason this is so, according to commentators, is that Justice Harlan's conception of reasonableness is not defined well enough to delineate clearly protected zones.") (citing Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1752 n.2 (1994); and Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 905 n.104 (1996)).

on the very government practices the Amendment is supposed to regulate. For example, consider what would happen if the government were simply to announce that all phones would henceforth be tapped and monitored at random.[57] Certainly if people were made aware of this change in government conduct, it would be unreasonable for them to presume that their conversations were private, and no search would occur when the government eavesdropped on these conversations. Therefore, if *Katz* is taken literally, the government could, by fiat, expand the scope of permissible searches almost without limit.

Conversely, conservatives have argued that the test in *Katz* is both results-driven and malleable. These critics, Justice Antonin Scalia principal among them, have contended that there is nothing in either the text or the history of the Fourth Amendment to justify the *Katz* approach and that only a standard grounded in the text and original understanding of the Fourth Amendment can provide both judicial integrity and consistent results.[58]

II. *KATZ V. UNITED STATES* IN PRACTICE—A FOCUS ON PRIVATE ACTION

Despite the widespread criticism of *Katz v. United States*, it remains the principal standard for evaluating whether government conduct constitutes a search.[59] Of course, the *Katz* formulation, like the Fourth Amendment it interprets, is hardly self-applying. In the more than thirty years that have passed since *Katz* was decided, the Court has slowly fleshed out this doctrine, not in a systematic way, but by accretion. There have been few monumental Fourth Amendment decisions since *Katz*; rather, the contours of the doctrine to which it has given rise have slowly come into relief. In this Part, I discuss this doctrinal development, pointing out the importance the Supreme Court has

---

[57] Sadly, this example is becoming less and less hypothetical. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") greatly expanded the power of government to conduct wiretaps against citizens. *See* Pub. L. No. 107-56, 115 Stat. 272 (2001); Stephen R. McAllister et al., *Life After 9/11: Issues Affecting the Courts and the Nation*, 51 U. KAN. L. REV. 219, 230–31 (2003) (discussing roving wiretaps).

[58] *See, e.g.*, Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1034–35 (1992) (Scalia, J.) (criticizing *Katz* as being circular, in that expectations of privacy are defined in terms of what a court finds to be reasonable); Kyllo v. United States, 533 U.S. 27, 34 (2001) (Scalia, J.) (critiquing *Katz* as a standard for whether or not a search has occurred).

[59] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 32–33 (2001) (discussing *Katz* as the appropriate standard for evaluating the extent of the Fourth Amendment).

attached to the conduct of private actors in determining the extent of constitutional rights.

A. *Abandoned Property*

If an individual has abandoned his property, there is obviously no longer even a subjective expectation of privacy in it, let alone one that society is willing to recognize as reasonable. Although this argument is relatively uncontroversial in the abstract, it leaves unanswered the question of what it means to abandon property. Consider, for example, the 1988 case of *California v. Greenwood*.[60] Acting on information indicating that Billy Greenwood might be engaged in narcotics trafficking, police twice obtained from his regular trash collector garbage bags left by Greenwood on the curb in front of his house.[61] On the basis of items in the bags that were indicative of narcotics use, the police obtained warrants to search the house and discovered controlled substances during the subsequent search.[62] On appeal from Greenwood's conviction, the Supreme Court held that no search occurred when the officers went through the contents of Greenwood's trash bags and that the subsequent, warranted search need not be suppressed as fruit of the poisonous tree:

> Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the

---

[60] 486 U.S. 35, 40–41 (1988).

[61] *Id.* at 37–38.

[62] *Id.* In this case, as in many of the others discussed below, the question before the Supreme Court was whether the first investigation done by law enforcement, in this case looking through the collected trash, constitutes a search. If not, then the Fourth Amendment does not regulate the challenged conduct and the information thus obtained may later be used in obtaining a warrant. If, however, the first investigation is a search, it must comply with the Fourth Amendment or else the evidence derived from it becomes inadmissible.

> express purpose of having strangers take it," respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.[63]

This is perhaps the clearest statement from the Court that when an individual has made a part of his life transparent to the public, he has made it available to the government as well. The defendant simply could not have had an expectation of privacy in his discarded trash because he could reasonably foresee that members of the public would go through it. Because he knowingly allowed the possibility that others would gain access to his trash, he was not permitted to object when the government sought to do the same thing.

Furthermore, the Supreme Court has held that when a private actor actually invades a defendant's reasonable expectation of privacy, the government may subsequently do so as well, at least to the extent that the private actor already has. For example, in 1984, in *United States v. Jacobsen*,[64] the Supreme Court upheld a search by federal drug agents that followed the opening of a sealed package by private freight transporters.[65] After employees of Federal Express had opened a sealed package in their possession and discovered that it contained a white powder, they resealed it and contacted law enforcement officials.[66] The federal officers then re-opened the package and conducted a field test that indicated that the white powder was cocaine.[67]

---

[63] *Id.* at 40–41 (citations omitted) (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)). In his dissent, Justice William Brennan argued that the mere fact that the bags might be rifled through was not enough to cause the defendant to lose his reasonable expectation of privacy in them:

> The mere *possibility* that unwelcome meddlers *might* open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home; or the possibility of a private intrusion negates an expectation of privacy in an un-opened package; or the possibility that an operator will listen in on a telephone conversation negates an expectation of privacy in the words spoken on the telephone.

486 U.S. at 54 (Brennan, J., dissenting). As resonant as this argument might be, the Supreme Court has continued to focus on the possibility of a private search, not necessarily its legality.

[64] 466 U.S. 109, 126 (1984).

[65] *Id.* at 111. Employees of the shipper testified that the package had been inadvertently torn by a forklift and had subsequently been opened pursuant to a written company policy regarding insurance claims. *Id.*

[66] *Id.*

[67] *Id.* at 111–12.

In upholding the re-opening of the package and the field test, the Court re-emphasized that the private search did not implicate the Fourth Amendment,[68] and that law enforcement officials are not obligated to avert their gaze from information supplied to them by third parties.[69] The Court went on to hold that although the defendant had enjoyed a reasonable expectation of privacy in the package before it was opened by the shippers, that expectation was severed when the package was actually opened:

> [I]n this case the fact that agents of the private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable. The reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed at the time that invasion occurred.[70]

Thus, although the government officials could not have been the first to open the package—because the defendant had a reasonable expectation of privacy at the time he sent it—they were permitted to reopen it because any expectation of privacy they thereby invaded had been lost by the initial, private intrusion. The fact that the private actor did something the government would not have been permitted to

---

[68] *Id.* at 113–14.

[69] *See Jacobsen*, 466 U.S. at 130.

[70] *Id.* at 114–15. The Court went on to state that the field cocaine test did not amount to a search because it revealed nothing about the contents of the container except whether it contained a particular kind of contraband, a fact in which the defendant could not have a reasonable expectation of privacy. *Id.* at 121; *see also* United States v. Place, 462 U.S. 696, 707 (1983) (finding that a sniff by a drug detecting dog, because it discloses only whether or not an individual possesses contraband, is not a search for Fourth Amendment purposes). *See generally* Sam Kamin, *Law and Technology: The Case for a Smart Gun Detector*, LAW & CONTEMP. PROBS., Winter 1996, at 221 (arguing that a scan with an advanced metal detector that could indicate in real time whether or not an individual is armed would not constitute a Fourth Amendment search).

do[71] simply did not convert the subsequent, otherwise reasonable, police conduct into a search that implicated the Fourth Amendment.[72]

Thus, whether or not an individual enjoys a reasonable expectation of privacy is not always a question over which she necessarily has much control. Jacobsen wrapped his package tightly, making it as impervious to discovery as was possible.[73] Nonetheless, that expectation of privacy was lost when the Federal Express employees broke into it; Jacobsen's expectation of privacy was lost through no fault of his own. Although Greenwood could have taken greater efforts to protect his own privacy, Jacobsen simply could not. Jacobsen initially had a subjective expectation of privacy that society was willing to recognize as reasonable. Because of the conduct of other, private actors, however, Jacobsen could not object when the government merely mimicked this private invasion of his privacy.

B. *Information Knowingly Exposed to Others*

Just as one does not have a reasonable expectation of privacy in those things he has physically abandoned, the Supreme Court has held in a number of different contexts that an individual does not have a reasonable expectation of privacy in personal information that is knowingly supplied to a third party. This is so even if that information is supplied for a very limited purpose and is expected to be kept from others. For example, in *United States v. Miller*, agents of the federal government subpoenaed the defendant's bank records, not from the defendant himself, but from his bank.[74] In upholding the validity of the subpoena, the Supreme Court held that the defendant did not have a reasonable expectation of privacy in those records because he had voluntarily given them to a third party:[75]

---

[71] The Court's statement that the initial search "might" have violated the Fourth Amendment if conducted by state actors seems generous; assuming the package was not torn completely open by the forklift, it remained a closed container for which probable cause and a warrant would have been required before a government search would have been permissible. *See Jacobsen*, 466 U.S. at 114. It is not surprising, therefore, that at no point did the government argue that if that search had been conducted by government officials it would have been constitutional.

[72] Of course, the Court's focus on the reasonableness of official conduct is hardly unusual. *See, e.g.*, Colorado v. Connelly, 479 U.S. 157, 167 (1986) (holding that a mentally disturbed defendant's confession was voluntary because the pressure he felt came from the voices in his head, not from police coercion).

[73] *See Jacobsen*, 466 U.S. at 111.

[74] 425 U.S. 435, 436 (1976).

[75] *Id.* at 443. Unlike many of the other cases discussed in this Article, *Miller* involved the issuance of a subpoena *duces tecum* rather than a search warrant. *Id.* at 436. Grand jury

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.[76]

Similarly, in *Smith v. Maryland*, the telephone company installed, at police request, a pen register on the defendant's phone line.[77] A pen register is a device that creates a list of the phone numbers called from a particular line.[78] The Court held that the installation and use of the pen register was not a search for Fourth Amendment purposes.[79] The Court reasoned that information regarding which numbers were called by the defendant was made available to a third party and was therefore not treated privately by the defendant:

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." . . . Telephone users, in sum, typically know that they must convey numerical information to the

---

subpoenas are governed by a different set of rules than search warrants; the governing rules are generally those pertaining to the issuance of civil warrants rather than those of the Fourth Amendment. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 11 (1973) (finding that "[t]he Fourth Amendment provides protection against a grand jury subpoena *duces tecum* too sweeping in its terms 'to be regarded as reasonable'") (quoting Hale v. Henkel, 201 U.S. 43, 76 (1906)). In *Miller*, however, the Supreme Court addressed whether a reasonable expectation of privacy exists in the material subpoenaed. 425 U.S. at 442.

[76] *Miller*, 425 U.S. at 443.

[77] 442 U.S. 735, 737 (1979).

[78] *Id.* at 736 n.1.

[79] *Id.* at 745–46.

> phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[80]

Although the opinions in *Smith* and *Miller* are perfectly consistent with the conclusion in *Greenwood*, the Court has not uniformly held that what is exposed to one is exposed to all. For example, in *Minnesota v. Olson*,[81] the Court upheld the Fourth Amendment rights of an overnight house guest in a third party's home, finding that although he had surrendered some of his privacy to his host, he had surrendered it only to his host:

> That the guest has a host who has ultimate control of the house is not inconsistent with the guest having a legitimate expectation of privacy. . . . The point is that hosts will more likely than not respect the privacy interests of their guests, who are entitled to a legitimate expectation of privacy despite the fact that they have no legal interest in the premises and do not have the legal authority to determine who may or may not enter the household.[82]

This reasoning is directly counter to that of *Smith* and *Miller*. In *Olson* the Court reasoned that although a houseguest surrenders some of her privacy to another, that does not mean that she loses any expectation of privacy vis-à-vis others.[83] In contrast, in *Smith* and *Miller*, the Court reasoned that surrendering information to anyone is to risk surrendering it to all.[84]

---

[80] *Id.* at 742–43 (citations omitted). Of course, the Court's statement that "subjective expectations of privacy cannot be scientifically gauged" is demonstrably false. *See id.* at 743. Researchers can test, and to a certain extent have tested the extent to which the public considers various invasions of their privacy to be reasonable. *See generally* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993) (reporting the results of a survey of which law enforcement practices unreasonably infringe on individual privacy and liberty).

[81] 495 U.S. 91, 99 (1990).

[82] *Id.*

[83] *Id.* at 99–100.

[84] *Smith*, 442 U.S. at 742–43; *Miller*, 425 U.S. at 443.

Miller and *Smith* have never been repudiated and represent the logical extension of the line of cases that begins with *Katz*. In *Katz*, the Court stated that what one knowingly exposes to the public even in one's own home is not protected by the Fourth Amendment. By the time we reach *Miller* and *Smith*, however, the question is not whether the individual has given away her privacy by making her life an open book. Rather, in these cases, the Court asked whether any other person has been given (or has gained) access to the information the government is seeking to obtain. If the answer is yes, the Court has held that the area simply is not protected by the Fourth Amendment. Although the Court's reasoning in these cases is hardly a model of consistency, it is clear that an individual who knowingly shares information with anyone, for any purpose, runs the risk of losing any expectation of privacy in that information.

C. *The Plain View Doctrine*

One of the principal implications of *Katz*, one in fact envisioned by the decision's own language,[85] was that even objects within the home are not protected by the Fourth Amendment if they have been knowingly exposed to others.[86] This corollary to *Katz* has come to be known as the plain view doctrine—as it is usually stated, if the police are in a place they are legally entitled to be,[87] and they observe contraband or evidence of a crime that has been exposed to view, the Fourth Amendment is not implicated by this viewing.[88] Because the Fourth Amendment only governs searches and seizures,[89] and because a search or sei-

---

[85] *See, e.g.*, 389 U.S. 347, 351–52 (1967) ("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." (citation omitted) (emphasis added)).

[86] *See id.*

[87] *See, e.g.*, Illinois v. Andreas, 463 U.S. 765, 771 (1983) (stating that "[t]he plain-view doctrine is grounded on the proposition that once police *are lawfully in a position* to observe an item first-hand, its owner's privacy interest in that item is lost; the owner may retain the incidents of title and possession but not privacy") (emphasis added); Texas v. Brown, 460 U.S. 730, 737 (1983) (finding that "the police officer must lawfully make an 'initial intrusion' or otherwise *properly be in a position* from which he can view a particular area") (emphasis added) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971)).

[88] Furthermore, the police may seize the object if they have probable cause to believe that it is either contraband or evidence of criminal activity. *See, e.g.*, Horton v. California, 496 U.S. 128, 140–41 (1990). Law enforcement officials, however, may generally seize only those objects that may be reached from a place they are legally entitled to be. *Id.* at 138–39.

[89] For a critique of this doctrine, see *Kyllo*, 533 U.S. at 32. For Justice Scalia, inquiring whether an individual enjoys a reasonable expectation of privacy ought to determine

zure does not even occur, in the constitutional sense, unless a reasonable expectation of privacy is invaded, this conduct need not even comport with the Fourth Amendment's reasonableness requirement.[90]

One thing that becomes clear in the Court's plain view cases, however, is that the Court does not literally mean its statement that in order for a plain view examination to fall outside the dictates of the Fourth Amendment the officers must be lawfully in a position from which to observe evidence in plain view.[91] Consider, for example, the case of *United States v. Dunn*.[92] In *Dunn*, officers of the Drug Enforcement Administration observed a drug lab inside a barn on the defendant's property.[93] Although it was true that the officers did not enter the barn in order to make this observation, it could hardly be said that the officers were "somewhere they were legally entitled to be":

> The ranch was completely encircled by a perimeter fence, and contained several interior barbed wire fences, including one around the house approximately 50 yards from the barn, and a wooden fence enclosing the front of the barn, which had an open overhang and locked, waist-high gates.

---

whether the search that occurred was reasonable, not whether it ought to be termed a search:

> One might think that the new validating rationale would be that examining the portion of a house that is in plain public view, while it is a "search" despite the absence of trespass, is not an "unreasonable" one under the Fourth Amendment. But in fact we have held that visual observation is no "search" at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.

Id. (citations omitted).

[90] *See* Michael Campbell, *Defining a Fourth Amendment Search: A Critique of the Supreme Court's Post-*Katz *Jurisprudence*, 61 WASH. L. REV. 191, 191 (1986) (arguing that "[b]ecause government actions that are neither searches nor seizures are not governed by the amendment, and therefore need not be 'reasonable,' the definitions of search and seizure limit the scope of the amendment's protection of individual rights"). Of course, government conduct must comport with the other applicable provisions of the Constitution; a policy of conducting plain view searches only of cars registered to blacks or women, although it would not violate the Fourth Amendment, would almost certainly violate the Equal Protection Clause. *See, e.g.*, Whren v. United States, 517 U.S. 806, 813 (1996) (refusing to invalidate pretextual stops and holding that "the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment").

[91] *See Andreas*, 463 U.S. at 771–72.

[92] 480 U.S. 294, 305 (1987).

[93] *Id.* at 297–98.

> *Without a warrant, officers crossed the perimeter fence, several of the barbed wire fences, and the wooden fence in front of the barn.*[94]

Had a member of the public attempted to do the same thing, the individual likely would have been liable to a suit in trespass and to possible criminal prosecution as well. Nonetheless, the Court held that the officers did not conduct a search when they observed the drug lab in the barn.[95] Thus, the Court must mean something other than "lawfully entitled" when it describes the conduct of the officers prior to making their plain view observation. In later cases, it has become clear that what the Court means is that the officers have not engaged in a Fourth Amendment violation prior to observing evidence in plain view.

The Court came very close to stating this explicitly in its 1971 opinion in *Coolidge v. New Hampshire*.[96] After surveying a number of its plain view cases, the Court summarized them as follows:

> What the "plain view" cases have in common is that the police officer in each of them had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused. The doctrine serves to supplement the prior justification—whether it be a warrant for another object, hot pursuit, search incident to lawful arrest, or some other legitimate reason for being present unconnected with a search directed against the accused . . . .[97]

In other words, so long as her conduct does not otherwise constitute a violation of the Fourth Amendment, the mere observation of evidence in plain view does not convert an officer's conduct into an illegal search. This position—that plain view requires that the officer's conduct prior to the plain view observation comply with the Fourth Amendment—is now the view of most of the federal circuit courts of appeals.[98]

---

[94] *Id.* at 294 (syllabus) (emphasis added).

[95] *Id.* at 304.

[96] 403 U.S. at 466.

[97] *Id.*

[98] For example, some of the federal circuit courts of appeals have cited the U.S. Supreme Court's 1990 decision, *Horton v. California*, for its proposition that the plain view rule is satisfied if "the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed." *See, e.g.*, United States v. $557,933.89, More or Less, in U.S. Funds, 287 F.3d 66, 81 (2d Cir. 2002) (citing *Horton*, 496 U.S. at 136–37); United States v. Jones, 187 F.3d 210, 219 (1st Cir. 1999) (quoting *Horton*, 496 U.S. at 136); United States v. Elwood, 993 F.2d 1146, 1152 n.28 (5th Cir. 1994) (citing *Horton*, 496 U.S. at 136); *see also* United States v. Elkins, 300 F.3d 638, 653 (6th Cir. 2002)

One of my central theses is that this subtle, semantic shift in how the Court defines plain view—moving from a conception of plain view based on the legality of the official conduct to one based on whether the officer has committed a Fourth Amendment violation prior to making the plain view observation—is crucial. Because the foreseeability, not the legality, of official conduct has become the central inquiry in determining whether a reasonable expectation of privacy exists, laws designed to protect individual privacy from private actors are unlikely to increase the scope of privacy from the government. As *Dunn* eloquently demonstrates, the mere fact that a public official has failed to comply with a civil or criminal statute designed to protect individuals from one another will, at most, be relevant in determining whether that official has invaded a reasonable expectation of privacy; it will certainly not be dispositive of that issue. Furthermore, as I argue below, such laws very well may be counterproductive. To the extent that they lull individuals into a false sense of security regarding their privacy, these laws may be a greater threat to privacy than the absence of such laws would be.

1. Rejection of the Inadvertence Rule

Prior to 1990, at least a plurality of the Supreme Court had held that discoveries of evidence in plain view had to be inadvertent to be permissible;[99] in other words, the rule stated that although an officer may lawfully discover contraband or evidence of crimes in plain view, the officer may not affirmatively seek it out.[100] The Court finally rejected this rule in *Horton v. California*,[101] holding that inquiry into the minds of law enforcement officers was not constructive and that the

---

(finding that the relevant question was whether the "Fourth Amendment prohibited [the officer] from walking" to the place where the plain view observation was made). Some of the federal circuit courts of appeals have defined lawful presence in terms of whether an independent Fourth Amendment violation had taken place. *See, e.g.*, United States v. Collins, 321 F.3d 691, 694 (8th Cir. 2003); United States v. Tucker, 305 F.3d 1193, 1202–03 (10th Cir. 2002); Perry v. Sheahan, 222 F.3d 309, 316 (7th Cir. 2000).

[99] *See, e.g.*, *Coolidge*, 403 U.S. at 466 (Stewart, J., joined by Douglas, Brennan, and Marshall, JJ.) (explaining that "the 'plain view' doctrine has been applied where a police officer is not searching for evidence against the accused, but nonetheless inadvertently comes across an incriminating object").

[100] The seeming rationale for this rule was that although the Constitution cannot require officers to avert their eyes when they see evidence of wrongdoing, it does not permit them to seek out that evidence if they have some reason to believe it will be found. *See id.*

[101] 496 U.S. at 141.

inadvertence rule encouraged dishonesty in law enforcement officials.[102]

After *Horton*, law enforcement officials were permitted to do what many had suspected them of doing all along, namely, engaging in searches for evidence in plain view. Thus, an officer may now walk along a public street, peering into every car window the officer comes across.[103] Because one cannot have a reasonable expectation of privacy in something she has left on the seat of her car—if she really wanted that object to remain private, she would have placed it in the glove box or trunk of the car—no search occurs when an officer conducts such an investigation. Because no search is conducted when an officer conducts a plain view investigation,[104] no suspicion whatsoever is required; an officer need not even have a hunch that evidence of a crime will be found in order to conduct a plain view search. In doing away with the inadvertence requirement, the Supreme Court has moved its plain view jurisprudence even further from a focus on what the officer is doing toward an examination of what anyone else might do. Because a member of the public may walk down the street snooping in the windows of parked cars, an officer may do so as well.[105]

---

[102] *Id.* at 138. The Supreme Court has, in other contexts, avoided adopting rules that would create an incentive for police deception. *See, e.g.*, Bond v. United States, 529 U.S. 334, 342 (2000) (Breyer, J., dissenting) (arguing that "a Fourth Amendment rule that turns on [the officer's] purpose could prevent police alone from intruding where other strangers freely tread"); *Whren*, 517 U.S. at 814 (finding that the "Fourth Amendment's concern with 'reasonableness' allows certain actions to be taken in certain circumstances, *whatever* the subjective intent" of the officer).

[103] *See, e.g.*, *Brown*, 460 U.S. at 740. In *Texas v. Brown*, the Supreme Court stated the following:

> The general public could peer into the interior of Brown's automobile from any number of angles; there is no reason Maples should be precluded from observing as an officer what would be entirely visible to him as a private citizen. There is no legitimate expectation of privacy shielding that portion of the interior of an automobile which may be viewed from outside the vehicle by either inquisitive passersby or diligent police officers.

Id. (citations omitted).

[104] *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 325 (1987) (finding that although the slightest moving or opening of an object discovered in plain view is a search, no search occurs when officers merely make observations of objects left available to their view).

[105] One recent case, however, has called into question the Supreme Court's rejection of the inadvertence rule. In *Bond v. United States*, the Court appeared to return to an interpretation of the Fourth Amendment based in part on the intent of the officer. 529 U.S. at 338–39. In that case, a federal officer boarded a stopped bus and manipulated the defendant's soft-sided luggage in an overhead bin to determine whether it contained contraband. *Id.* at 335–36. In holding that the manipulation of the bag constituted a search and was thus presumptively unconstitutional in the absence of a search warrant, the Court distinguished

2. Technologies to Improve Plain View

We have seen that in cases where the officer merely sees contraband with the naked eye, the application of the plain view doctrine or one of its analogs will validate the search.[106] Cases often arise, however, involving law enforcement officials who have augmented their

---

between the sort of invasions of privacy a passenger expects when he places his bag in an overhead compartment from the sort of invasion visited on Bond's bag in this case:

> [A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.

Id. at 338–39. The dissent objected to this distinction, pointing out that in the past, the Court had inquired into whether what the officer was doing was something a member of the public could have done as well, rather than whether the officer had the same intention that the member of the public did:

> Of course, the agent's *purpose* here—searching for drugs—differs dramatically from the intention of a driver or fellow passenger who squeezes a bag in the process of making more room for another parcel. But in determining whether an expectation of privacy is reasonable, it is the *effect*, not the purpose, that matters.

Id. at 341 (Breyer, J., dissenting). Even applying the dissent's standard to the facts of the case, however, the majority's reasoning seems sound. The majority explained that the sort of manipulation done by the officers was different in kind from the sort of touching one expects on a public bus, not merely because of the officers' intent, but because that intent drove them to manipulate the bags differently. *Id.* at 338–39. Although one's bag might be pushed, compressed, moved, or otherwise abused by one's fellow passengers, one does not expect these passengers to do the sort of invasive manipulation that would reveal a bag's contents. The officers did a different search than members of the public would have done, and it was this practical difference, rather than any difference in the officers' state of mind, that made the difference in the case.

[106] The courts have extended the plain view doctrine to cover senses other than vision. Thus, if an officer, in the course of a properly circumscribed frisk for weapons, feels something that is immediately apparent as contraband, the discovery of the contraband is not itself a search requiring independent constitutional justification. *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 369, 378–79 (1993) (applying the plain view doctrine to the sense of touch). Similarly, if an officer is somewhere she is lawfully entitled to be and smells something that indicates that criminal activity is afoot, or hears a sound that leads her to believe that such activity is occurring, no further search has occurred. *See, e.g.*, United States v. Roby, 122 F.3d 1120, 1124–25 (8th Cir. 1997) (applying the plain view doctrine to the sense of smell); United States v. Jackson, 588 F.2d 1046, 1051–52 (5th Cir. 1979) (applying the plain view doctrine to the sense of hearing).

In each of these cases, the court's rationale is that the suspect, by exposing incriminating evidence to the sense of touch, hearing, or smell of the officer, has indicated that the suspect does not have a reasonable expectation of privacy in it. Because the officer is merely doing what another member of the public might do, she conducts no search when her senses indicate the presence of contraband.

senses with devices designed to facilitate the discovery of evidence of criminal wrongdoing. To take perhaps the most innocuous example, an officer peering into a car window from the sidewalk on a sunny day clearly has not conducted a search and may make this investigation without any prior suspicion that he will discover evidence of criminal activity. When the officer conducts the same investigation on a moonless evening, however, and must use a flashlight to see in the window, a more complicated case is presented.

Nonetheless, the federal courts have consistently held that the use of simple devices to improve the senses does not elevate an otherwise permissible investigation to the level of a search. For example, more than seventy-five years ago in *United States v. Lee*, the U.S. Supreme Court held that the "use of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution."[107] Although the issue has rarely reached the Supreme Court since, the lower federal courts have unanimously held that the use of simple devices such as flashlights,[108] binoculars,[109] step-ladders,[110] and the like simply does not transform police investigations into searches.

A more difficult question is presented by law enforcement's use of more sophisticated technologies. Take, for example, the 1986 case of *California v. Ciraolo*.[111] Hoping to gain evidence of marijuana cultivation, police officers flew over the defendant's property in a borrowed private plane and observed the plants growing there.[112] The plants were eight to ten feet high and were seen and photographed growing in a fifteen- to twenty-five-foot plot in the defendant's yard.[113] Based on this observation, a search warrant was obtained, the plants were seized, and the defendant was convicted for their cultivation.[114]

On appeal, the government argued that no search occurred when the officers overflew the shed, and the Court agreed:

---

[107] 274 U.S. 559, 563 (1927).

[108] *See, e.g.*, United States v. Ocampo, 650 F.2d 421, 427 (2d Cir. 1981) (stating that "the agent's use of a flashlight did not keep the cash in the bag from being in 'plain view' and therefore seizable under the logic of *Coolidge v. New Hampshire*") (citation omitted).

[109] *See, e.g.*, United States v. Allen, 633 F.2d 1282, 1290–91 (9th Cir. 1980) (finding that use of ordinary binoculars does not constitute a Fourth Amendment "search").

[110] *See, e.g.*, United States v. Bellina, 665 F.2d 1335, 1345 (4th Cir. 1981) (finding that an officer's use of a stepladder "did not infringe in any way the defendants' legitimate expectation of privacy").

[111] 476 U.S. 207, 213–14 (1986).

[112] *Id.* at 209.

[113] *Id.*

[114] *Id.* at 209–10.

> That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible. . . .
>
> The observations by [the officers] in this case took place within public navigable airspace, in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana. That the observation from aircraft was directed at identifying the plants and the officers were trained to recognize marijuana is irrelevant. Such observation is precisely what a judicial officer needs to provide a basis for a warrant. Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed.[115]

A number of aspects of *Ciraolo* are noteworthy. First, although the Court states that it does not require the officers to turn a blind eye to criminal activity observed from a public thoroughfare, that hardly describes what the officers in this case were doing. The officers had acquired a plane for the express purpose of flying over the defendant's property to look down at it to find criminal evidence.[116] Although the inadvertence rule had been rejected by the time *Ciraolo* was decided,[117] to justify this decision on the ground that deciding otherwise would effectively require officers to ignore criminal evidence that they stumble upon seems entirely beside the point.[118]

---

[115] *Id.* at 213–14 (citations omitted).

[116] *Ciraolo*, 476 U.S. at 209. It appears that the police, lacking a plane for overflight purposes, proceeded to charter one in order to investigate the tip regarding the defendant's marijuana cultivation. *See id.*

[117] *See supra* notes 44–54 and accompanying text.

[118] Of course, the *Bond* decision, taken to its logical conclusion, would call into question a number of the Court's landmark cases, including *Ciraolo*. *See Bond*, 529 U.S. at 338–39; *Ciraolo*, 476 U.S. at 213–14. Although the officers were indeed flying where a member of the public could have flown, their interest in the defendant's illicit plants caused them to fly in a way calculated to find the marijuana, a manner of flight that a member of the public was unlikely to undertake. As I argue above, however, the Court has thus far not extended *Bond* beyond its holding. *See supra* note 102 and accompanying text.

Note also that *Ciraolo* was decided in part on the somewhat surprising basis that the police officers were in Federal Aviation Administration navigable airspace at the time they observed the marijuana growing on the defendant's property.[119] Given that the Federal Aviation Administration is charged with protecting the public safety rather than privacy,[120] this may seem an unusual ground for the decision. Yet the implication of this observation, as the dissent points out,[121] is that the police in this case were merely doing what members of the public could do; they were only flying where a member of the public could fly. Because the defendant failed to protect himself from this foreseeable invasion of his privacy by protecting his property from aerial surveillance, he cannot have a reasonable expectation of privacy in the crops he was growing therein.[122] As we have seen, however, even if the police were somewhere members of the public could not legally go, the result would not likely have been different; the Court's focus is generally on what members of the public could do as a practical matter, not what they are permitted to do as a legal matter.

Note finally that the Court's focus is on the risks that the defendant has exposed himself to from members of the public rather than on any actual diminution of his privacy. *Ciraolo* is thus different from *Smith* and *Miller*, in which the defendants had already made their information available to others and from *Jacobsen*, in which a third party

---

[119] 476 U.S. at 213 (noting that "[t]he observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace").

[120] *See* FED. AVIATION ADMIN., MISSION, VISION, VALUES, *at* http://www.faa.gov/aboutfaa/Mission.cfm (last visited Jan. 31, 2005) (claiming that the Federal Aviation Administration's mission is "[t]o provide the safest, most efficient aerospace system in the world").

[121] *Ciraolo*, 476 U.S. at 223 (Powell, J., dissenting). In his dissent in *Ciraolo*, Justice Lewis Powell stated the following:

> The Court's holding . . . must rest solely on the fact that members of the public fly in planes and may look down at homes as they fly over them. The Court does not explain why it finds this fact to be significant. One may assume that the Court believes that citizens bear the risk that air travelers will observe activities occurring within backyards that are open to the sun and air.

Id. (citation omitted).

[122] Some courts and commentators have described this rationale as an outgrowth of the assumption-of-risk doctrine—if an individual has not protected himself against a foreseeable, private invasion of privacy, then he has assumed the risk of a similar invasion of privacy by law enforcement officials. *See, e.g.*, *Smith*, 442 U.S. at 744 (finding that Smith had "assumed the risk that the [phone] company would reveal to the police the numbers he [had] dialed" from his home telephone); Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 135 (2002) (claiming that "[u]nder the assumption of risk theory, the disclosure of information to a third party denies Fourth Amendment protection to what might otherwise be private information").

had deprived the defendant of his privacy.[123] In *Ciraolo*, there was no intimation that members of the public regularly or even occasionally overflew the defendant's rural property. Nonetheless, the Court found no invasion of a reasonable expectation of privacy because the officers were doing what a member of the public might do.

The same day that it decided *Ciraolo*, the Court also decided *Dow Chemical Co. v. United States*.[124] In *Dow Chemical*, the Court rejected the defendant's argument that the government's warrantless, sophisticated aerial photography of its chemical plant was a search.[125] Using language that the Court would echo in its *Kyllo v. United States* decision, the Court held that although

> [i]t may well be . . . that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. . . . the photographs here are not so revealing of intimate details as to raise constitutional concerns.[126]

Defendants should not be expected to shield themselves from invasions by unknown threats, the Court seemingly reasoned; by contrast, when the risk is one that defendants face from their peers, their failure to protect themselves from it is an indication that they do not have a reasonable expectation of privacy.

Furthermore, the Court explicitly rejected Dow's contention that the use of aerial photography constituted a search because, had it been done by a competitor, such an invasion would violate state trade secret laws.[127] Repeating the proposition that state tort law does not define the contours of the Fourth Amendment,[128] the Court rejected this argument in short order.[129] The Court stated that government investigations raise the specter of different harms than those raised by unfair competition in the private sector,[130] and that the fact that gov-

---

[123] *Compare Ciraolo*, 476 U.S. at 213, *with Jacobsen*, 466 U.S. at 114–15, *Smith*, 442 U.S. at 742–43, *and Miller*, 425 U.S. at 443.

[124] 476 U.S. 227, 239 (1986).

[125] *Id.*

[126] *Id.* at 238.

[127] *Id.* at 232.

[128] *Id.*

[129] *Dow Chemical*, 476 U.S. at 232.

[130] *See id.* at 232. *But see* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (plurality opinion) (finding that a helicopter overflight from 400 feet did not violate the defendant's reasonable expectation of privacy, but that "[w]e would have a different case if flying at

ernment conduct would have been tortious or criminal if done by a private actor is but one factor to be considered in determining whether that conduct violates a reasonable expectation of privacy.[131]

D. *The State of the Law:* Kyllo v. United States

In its 2000 term, the U.S. Supreme Court decided a case that commentators anticipated would force the Justices to confront head-on the question of how emerging technologies would affect the scope of the Fourth Amendment. In *Kyllo v. United States*,[132] the Supreme Court invalidated an investigation based in part on the use of a thermal imaging device to measure the heat coming off a suspected marijuana cultivator's home. Instead of confronting the technology question directly, however, the Court looked to the past, principally to *Katz* and *Dow Chemical*, in search of answers.[133]

Federal law enforcement officials suspected Danny Kyllo of growing marijuana inside his home using high-intensity grow lamps.[134] To confirm these suspicions, the officers used a thermal imaging device,

---

that altitude had been contrary to law or regulation"). In *Riley*, five Justices rejected the plurality's view that Federal Aviation Administration regulations should control the question of a reasonable expectation of privacy. *See Riley*, 488 U.S. at 452–68 (O'Connor, J., concurring; Brennan, Marshall, Stevens, JJ., dissenting; Blackmun, J., dissenting). For example, in her concurrence, Justice Sandra Day O'Connor stated the following:

> In determining whether Riley had a reasonable expectation of privacy from aerial observation, the relevant inquiry after *Ciraolo* is not whether the helicopter was where it had a right to be under FAA regulations. Rather, consistent with *Katz*, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not "one that society is prepared to recognize as 'reasonable.'"

Id. at 454 (O'Connor, J., concurring) (quoting *Katz*, 389 U.S. at 361).

[131] *See Dow Chemical*, 476 U.S. at 232.

[132] 533 U.S. at 40.

[133] *See id.* at 32, 34. *Kyllo* has already generated an enormous literature on its implications for privacy and technology. *See generally* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119 (2002); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002); Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013 (2001); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393 (2002); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, LAW & CONTEMP. PROBS., Spring 2002, at 125.

[134] *Kyllo*, 533 U.S. at 29.

the Agema Thermovision 210, to measure the heat patterns coming off of Kyllo's building.[135] The thermal scan conducted from the street in front of Kyllo's house revealed that "the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in [Kyllo's] triplex."[136] Based in part on this information, the officers sought and obtained a warrant to search Kyllo's home. More than one hundred marijuana plants were found, and Kyllo was indicted on one count of manufacturing marijuana in violation of federal law.[137] Kyllo entered a conditional guilty plea and appealed, arguing that the thermal scan of his house was a search and should be presumed to be unconstitutional in the absence of a warrant.[138]

On appeal, the Supreme Court held that the use of a technology to obtain information regarding the interior of a home is a search, at least when the technology in question "is not in general public use."[139] This language, lifted almost verbatim from *Dow Chemical*,[140] makes absolutely clear the importance of private conduct to the definition of reasonable expectations of privacy. Once individuals can be fairly charged with an awareness of a technology and its implications, the Court reasoned, they are responsible for protecting themselves from its possible invasions.[141] If they fail to do so, they cannot complain when the government later uses that technology to discover information about them; the question of whether individuals have "knowingly expose[d]"[142] an area to the public turns, therefore, on whether or not they failed to protect themselves from a known threat.

---

[135] *Id.*

[136] *Id.* at 30.

[137] *Id.*

[138] *Id.*

[139] *Kyllo*, 533 U.S. at 40 (finding that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant").

[140] *See Dow Chemical*, 476 U.S. at 238 (stating that "[i]t may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant").

[141] *See Kyllo*, 533 U.S. at 40.

[142] *Katz*, 389 U.S. at 351.

E. *Conclusion*

For much of American history, there was a marriage between the contours of the Fourth Amendment and the contours of private law.[143] For example, at common law, it was a defense to an action brought in trespass that the defendant was a public official engaged in a legal search; that which was trespass was constitutionally impermissible and that which was constitutionally permissible was no trespass.[144] This marriage continued well into the twentieth century.

To a large extent, however, the twentieth century witnessed a growing disconnect between private ordering and public ordering. As many of the cases cited above clearly indicate, the scope of property law simply no longer determines the contours of the Fourth Amendment.[145] Time and again, the Supreme Court stated that although the existence of private law—property, tort, or contract—may be relevant in determining whether a reasonable expectation of privacy exists, that law is not dispositive of the constitutional question.

Furthermore, the above cases make clear that, to a large extent, private law has been replaced as an ordering principle with private conduct; courts now focus on what a member of the public could do rather

---

[143] *See, e.g.*, Boyd v. United States, 116 U.S. 616, 627 (1886).

[144] *See* Olmstead v. United States, 277 U.S. 438, 457 (1928); Entick v. Carrington, 95 Eng. Rep. 807, 817 (K.B. 1765).

[145] *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1979) (finding that "[e]xpectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest"); United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (finding that shared authority over property, rather than "mere property interest," is the proper standard for determining the permissible scope of third-party consent to search); Warden v. Hayden, 387 U.S. 294, 304 (1967); Silverman v. United States, 365 U.S. 505, 511 (1961) (finding that "[i]nherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law"); Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy or Security?*, 33 WAKE FOREST L. REV. 307, 309–27 (1998) (tracing the property right basis of the Fourth Amendment from its origins in *Boyd* and *Entick* through its demise in the last third of the twentieth century). The Supreme Court in *Warden v. Hayden* stated the following:

> *The premise that property interests control the right of the Government to search and seize has been discredited.* Searches and seizures may be "unreasonable" within the Fourth Amendment even though the Government asserts a superior property interest at common law. We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.

387 U.S. at 304 (emphasis added).

than on what the law would permit the individual to do.[146] As the law stands today, if an individual has exposed her trash to her neighbors, she has exposed it to the police as well;[147] if she has shared information with her bank or phone company, she has exposed it to the police as well;[148] if she has inadvertently made part of her property visible to those flying overhead, she has exposed it to the police as well.[149]

Thus, as I have argued from the outset, although the Fourth Amendment does not govern private conduct, that conduct is far from irrelevant in defining the scope of the Fourth Amendment. The more that an individual exposes to private actors, the more difficult it becomes to keep that same information from governmental actors should they seek to gain access to it as well. Even if the government official was doing something that a private individual could be sued or prosecuted for doing, that fact will not be dispositive of the Fourth Amendment inquiry. In determining the current scope of our rights, therefore, it becomes relevant just how much information that an individual might think of as private has actually been exposed to or shared with others.

III. The Extent of Private Snooping

Clearly, if the contours of the Fourth Amendment are defined in part by private, intrusive conduct, it is important to understand the extent of that conduct. In this Part, I demonstrate that, largely owing to advances in surveillance and information technology, Americans are currently subject to scrutiny—from their employers, insurers, advertisers, and even their neighbors—as they never have been before.[150]

Although such invasions of privacy are impossible to catalogue exhaustively, I set forth some of the examples that have made news and have particularly concerned privacy advocates in recent years. I focus in this Part on the following three broad categories of private conduct: workplace surveillance,[151] consumer information misuse,[152] and medical privacy intrusions.[153] With respect to each example, I discuss how technology has facilitated the acquisition of personal information by

---

[146] *See, e.g.*, *Greenwood*, 486 U.S. at 40; *Dunn*, 480 U.S. at 301; *Ciraolo*, 476 U.S. at 213–14.

[147] *See supra* notes 60–63 and accompanying text.

[148] *See supra* notes 74–80 and accompanying text.

[149] *See supra* notes 111–123 and accompanying text.

[150] *See generally* Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America (2000) (arguing that to live in the modern era is to be subject to surveillance).

[151] *See infra* notes 159–188 and accompanying text.

[152] *See infra* notes 189–210 and accompanying text.

[153] *See infra* notes 211–241 and accompanying text.

private actors and the implications of these private actors' conduct for the contours of the Fourth Amendment.

One thing that becomes clear as we study these areas of law is that there are no blanket privacy protections provided by federal statute;[154] rather, different areas—the workplace, consumer information, medical information—are each covered, in varying degrees, by an alphabet soup of federal legislation. For example, the Video Privacy Protection Act (the "VPPA")[155] guards records of video rentals from unauthorized public disclosure; the Health Insurance Portability and Accountability Act ("HIPAA")[156] governs the disclosure of medical information to those other than health care providers; and the Children's Online Privacy Protection Act ("COPPA")[157] regulates commercial websites' ability to collect personal information from minors. Rather than creating an omnibus privacy act, Congress has reacted to high-profile privacy concerns by attempting to remedy specific privacy threats.[158] As a result, each context presents its own legal issues and must be analyzed independently.

A. *Workplace Surveillance*

The average American who works full time spends nearly forty-three hours per week at work;[159] in other words, between Monday and Friday the average worker now spends nearly as many waking hours at work as at home. Furthermore, as the average amount of time workers spend at work has gone up, so too has the surveillance to which these workers are subjected.[160] As employers attempt to maintain and in-

---

[154] *See, e.g.*, Rita Heimes, Foreword, *Internet Privacy Law, Policy, and Practice: State, Federal, and International Perspectives*, 54 ME. L. REV. 95, 96 (2002) (explaining that "[w]hile the EU has established broad standards for individual privacy protection, the United States government focused only on narrow categories of sensitive data") (citation omitted).

[155] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000).

[156] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[157] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2000).

[158] I have argued elsewhere that legislatures do much the same thing in the context of criminal justice policy. *See* FRANKLIN E. ZIMRING, GORDON HAWKINS & SAM KAMIN, PUNISHMENT AND DEMOCRACY, THREE STRIKES AND YOU'RE OUT IN CALIFORNIA 181–216 (2001) (arguing that legislatures inevitably attempt to solve the last criminal justice problem, not the next one).

[159] U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2002, at 375 tbl.575 (2003) (showing that the average full time worker worked 42.9 hours in 2001).

[160] *See generally* Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739 (1992); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002).

crease the productivity that has fueled the American economy in recent years,[161] they are increasingly turning to technologies that allow them to keep tabs on their employees' activities while at work.

It is true, of course, that employers have always had an incentive to supervise their employees closely; an unsupervised employee can steal, shirk, or otherwise cost the employer money. As the American economy has moved from one based on manufacturing to one based on the service sector and information technologies,[162] however, employers have largely shifted the focus of their surveillance. No longer are their primary concerns workplace safety and preventing simple theft. Rather, employers are now increasingly concerned with insulating themselves from litigation, preventing the misappropriation of their intellectual property, and limiting unproductive work time.[163] As their concerns have changed, so have the tools available to employers to ensure employee compliance with workplace rules.

1. State of the Art

As with each of the other areas of private conduct discussed in this Part, workplace surveillance has been both changed immeasurably and facilitated by the advent of technologies designed specifically for that purpose. The most obvious example of this technology-powered surveillance is management's monitoring of the computers it provides to its employees. More than half of the American workforce now spends at least some part of the day in front of a computer,[164] and as anyone who

---

[161] *See* U.S. CENSUS BUREAU, *supra* note 159, at 392 tbl.601 (showing that between 1980 and 2001 business sector productivity increased nearly 50% while manufacturing productivity rose nearly 100%).

[162] *See id.* (showing that between 1980 and 2001 the percentage of all workers employed in the production of goods dropped from 28.4% to 19.0% while service jobs rose from 19.8% to 31.0% of the economy).

[163] *See, e.g.*, ROSEN, *supra* note 150, at 79–90 (cataloguing the widespread use of technology to monitor employees in the American workforce and describing the threat of sexual harassment litigation as one of the main justifications offered for the surveillance); John M. Conlin, *The Case for Watching Employees on the Web*, DENV. BUS. J., Jan. 28, 2000, at 14B ("It is a statistical certainty that sooner or later Internet misuse will create a serious problem for most organizations. It might be as simple as productivity loss or as serious as multi-million dollar lawsuits or corporate espionage."); Kristen Bell DeTienne & Richard D. Flint, *The Boss's Eyes and Ears: A Case Study of Electronic Employee Monitoring and the Privacy for Consumers and Workers Act*, 12 LAB. LAW 93, 96 (1996) ("Employers . . . justify electronic monitoring as a necessary protection against potential liability. Under the legal theory of respondeat superior, employers can be liable for various injuries caused by their employees.").

[164] U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2004–2005, at 407 tbl.617 (2004) (reporting that 53.5% of those employed used a computer at their main job). One recent study reported that out of a total U.S. workforce of 140,000,000

has spent much time in front of an Internet-connected computer can attest, it is often far too easy to find distractions online.[165] Not surprisingly, an entire industry has sprung up to help employers monitor their employees' use of these work computers.[166] Employers can now purchase software that allows them to record every keystroke their employees make, view anything that has appeared on their employees' screens, and maintain a copy of every e-mail their employees send and receive from their computers.[167]

Furthermore, it is becoming increasingly clear that employers are taking full advantage of these surveillance technology options. For example, a recent report by the American Management Association found that nearly half of private firms monitor their employees' e-mail, and 62.8% monitor their employees' Internet connections.[168] Of the companies surveyed, 77.7% monitored their employees' telecommunications, and 27% had dismissed an employee based at least in part on information obtained from such monitoring.[169] Of course, workplace surveillance is not limited to the monitoring of employees' work

---

workers, nearly 40,000,000 were regular users of the Internet and e-mail at work. Andrew Schulman, Privacy Found., *The Extent of Systematic Monitoring of Employee E-mail and Internet Use, at* http://www.sonic.net/~undoc/extent.htm (July 9, 2001) (quoting figures from the U.S. Department of Labor).

[165] *See, e.g.*, Ian Ayers, *Lectures v. Laptops*, N.Y. TIMES, Mar. 20, 2001, at A25 (stating that the distractions of the Internet are so great that the author has installed filtering software on his office computer to limit his *own* use of the Internet while at work).

[166] *See, e.g.*, Boehmer, *supra* note 160, at 739 (opining that "[t]he vast arsenal of technology now available to employers for the day-to-day gathering and analysis of information about their employees is impressive, as well as frightening"); Dan McIntosh, *e-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539, 541 (2000) (explaining that "[a]ccompanying the growing use of . . . new business tools is the development of equally advanced means of allowing employers to electronically monitor their use by employees").

[167] For example, SpectorSoft, a software company, offers a product on its website that will perform all of these functions. *See* SPECTORSOFT, *Spector Pro 5.0, at* http://www.spectorsoft.com/products/SpectorPro_Windows/index.html (last visited Jan. 31, 2005) (pledging that their software "Records Every Exact Detail of Their PC and Internet Activity"); *see also* Karen J. Bannan, *Watching You, Watching Me*, PC MAG., July 2002, at 100–04 (describing and reviewing a number of products that perform essentially the same functions).

[168] AM. MGMT. ASS'N, 2001 AMA SURVEY, WORKPLACE AND MONITORING SURVEILLANCE: SUMMARY OF KEY FINDINGS 1 (2001), *available at* http://www.amanet.org/research/pdfs/ems_short2001.pdf.

[169] *Id.* at 1–2; *see also* Elise M. Bloom et al., *Competing Interests in the Post 9–11 Workplace: The New Line Between Privacy and Safety*, 29 WM. MITCHELL L. REV. 897, 898 (2003) (explaining that "[s]ince September 11 [2001], sales of Internet and e-mail monitoring software have risen dramatically").

computers.[170] Currently, more employees than ever are being drug-tested,[171] having their phone conversations tape recorded,[172] and having their work activities videotaped.[173] If the previous Part of this Article was correct, then this expansion of employee surveillance in the workplace should correspond to a diminished expectation of privacy in the workplace for Fourth Amendment purposes. As the next section will demonstrate, the cases reported in this area indicate exactly that.

2. Fourth Amendment Implications

Federal law does little to explicitly regulate employer surveillance of employees. For example, although the Electronic Communications Privacy Act of 1986 (the "ECPA") prevents the interception and monitoring of electronic communications by private individuals,[174] almost all employer monitoring of employees is likely exempted from this legislation.[175] Furthermore, although many states have passed laws that reinforce the protections of the ECPA,[176] in most cases, the greatest

---

[170] *See generally* S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 826 n.5 (1998) (cataloguing lower court cases involving polygraph testing, psychological profiling, drug testing, and physical searching of employees).

[171] *See, e.g.*, AM. CIVIL LIBERTIES UNION, PRIVACY IN AMERICA: WORKPLACE DRUG TESTING, *at* http://www.aclu.org/WorkplaceRights/WorkplaceRights.cfm?ID=9925&c=34 (Mar. 12, 2002) (reporting that between 1987 and 2002 drug testing of employees went up 277%).

[172] *See, e.g.*, Jeffrey L. Seglin, *As Office Snooping Grows, Who Watches the Watchers?*, N.Y. TIMES, Jun. 18, 2000, § 3, at 4 (reporting that the monitoring of employees' work phones is widespread and that "[e]xcept for the shouting, it is becoming clear that the debate over employee privacy is over").

[173] AM. MGMT. ASS'N, *supra* note 168, at 1.

[174] 18 U.S.C. § 2510 (2000) (prohibiting the interception or disclosure of "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce").

[175] *See, e.g.*, McIntosh, *supra* note 166, at 549 (describing the Business Use, Consent and Provider exceptions to the ECPA and stating that "the exceptions have been applied favorably to employers and thus, have posed significant hurdles to employee claims under the ECPA that allege unlawful interception or access of workplace communications"). Similarly, the Federal Wiretap Act has been held not to prohibit employer interception of e-mails and monitoring of web traffic, at least so long as the interception is of stored data rather than data in transit. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994); Philip L. Gordon, *Job Insecurity? When It Comes to Workplace Surveillance of Electronic Communications, Employers Are Free to Establish the Rules of the Game*, 79 DENV. U. L. REV. 513, 513 (2002) (discussing how judicial interpretation of the Federal Wiretap Act essentially eliminates statutory protection for workplace Internet and e-mail use).

[176] Given that the federal law preempts inconsistent state laws, the only way states can avoid having their statutes preempted by ECPA is to provide identical or greater protection than is provided by federal law. *See, e.g.*, United States v. McKinnon, 721 F.2d 19, 21 n.1 (1st

restraint on workplace surveillance is the employer's own statement of what it will and will not do.[177] Although an employer may not snoop upon its employees if it has promised or contracted not to do so, an employer who informs workers that their activities are subject to surveillance will likely have a free hand in conducting that surveillance.[178]

Under *Katz*, law enforcement officials conduct a search when they invade an individual's reasonable expectation of privacy.[179] In the workplace context, the determination of whether the employee has a reasonable expectation of privacy has often involved an analysis of whether the individual was able to protect the area in question from others[180]—whether the employee had the capacity to lock files, to exclude others from the employee's work space, and so on.[181] Of course, evidence that a person's employer has engaged in exactly the sort of

---

Cir. 1983) (finding that a state wiretap statute must provide greater protection than the federal statute in order to avoid being preempted).

[177] *See, e.g.*, Jeffrey Benner, *Privacy at Work? Be Serious*, WIRED NEWS, *at* http://www.wired.com/news/business/0,1367,42029,00.html (Mar. 1, 2001). In an article for *Wired News*, Jeffrey Benner stated the following:

> [I]f an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an "expectation of privacy." In short, once the company stakes its claim over its cyber-dominion, its employees have no right to privacy there.

Id.

[178] Furthermore, even if legislation were passed regulating the extent to which employers monitor their employees, such legislation would likely only be a default rule, one that employers, with their generally superior bargaining power, would almost certainly be able to bargain around. *See, e.g.*, Lee Kovarsky, *Tolls on the Information Superhighway: Entitlement Defaults for Clickstream Data*, 89 VA. L. REV. 1037, 1043 (2003) ("That employers may monitor e-mail and web surfing to promote productivity and protect against industrial espionage has become more of a fact of life than a controversy, and employers would likely contract around any default rule to the contrary.") (citation omitted). It is difficult to imagine a regime in which employers were completely forbidden from engaging in this type of surveillance, even with the consent of their employees.

[179] *See supra* notes 44–54 and accompanying text.

[180] *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 714–15, 722 (1987) (finding that the Fourth Amendment can be implicated by a public employer's search of an employee's workplace, but that when the search is conducted by a public employer for a work-related reason, neither a warrant nor probable cause is required).

[181] *See, e.g.*, United States v. Anderson, 154 F.3d 1225, 1229 (10th Cir. 1998) (finding that the defendant had a reasonable expectation of privacy in those private effects he brought to the office where he kept his office door closed and his window covered); United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991) (finding "a privacy interest in an office reserved for one's exclusive use at a place of employment to be reasonable, especially when asserted against a forcible entry after work hours").

surveillance that the government is later attempting to conduct—whether it be the reading of e-mails, the searching of hard drives, or the tracking of web traffic—generally makes it very difficult for an employee to claim a reasonable expectation of privacy in the workplace.

For example, in *Muick v. Glenayre Electronics*, the Seventh Circuit Court of Appeals found that a private employee did not have a reasonable expectation of privacy in a computer given to him by his employer for work purposes.[182] At the request of federal law enforcement officials who suspected Albert Muick of possessing child pornography,[183] Muick's employer seized his work computer until a warrant could be issued for its contents.[184] A subsequent warranted search of the computer revealed the presence of child pornography, and Muick was convicted of violating federal laws forbidding the possession of such material.[185]

On appeal, the Seventh Circuit held that because Muick had been told that his computer remained the employer's property and that the employer had explicitly reserved the right to examine its contents at any time and without notice, it was unreasonable for him to have an expectation of privacy in the information stored on that computer—"[The employer] had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have

---

[182] 280 F.3d 741, 743 (7th Cir. 2002) (Posner, J.).

[183] Interestingly, a very large percentage of the reported cases in this area involve computer searches for child pornography. In his book on the loss of privacy in the modern era, Jeffrey Rosen critiques the expansion of gender discrimination law as contributing to a general decrease in privacy in the work place:

> Most Americans . . . will never be deposed in a sexual harassment suit, either as a plaintiff, a defendant, or a witness. Nevertheless, many Americans have their e-mail or Internet browsing habits monitored at work, and one of the most common justifications of employee monitoring offered by courts and management lawyers is the fear of liability for sexual harassment.

See ROSEN, *supra* note 150, at 12. My review of cases involving criminal prosecutions that follow workplace searches, however, reveals that they nearly uniformly involve searches for child pornography. Although Rosen may be correct about the majority of employer surveillance, when law enforcement officials search a worksite, it is almost always to search for child pornography. In a later article, I hope to explore further this relationship between substantive criminal law and the issues that new criminal statutes will raise in the realm of criminal procedure.

[184] Surprisingly, the court found that the employer was not a state actor although it seized the computer at the government's request. *Muick*, 280 F.3d at 742–43. Nonetheless, the court went on to consider the Fourth Amendment implications of the seizure. *Id.* at 743.

[185] *Id.* at 742.

had and so scotches his claim."[186] Although most reported federal cases involving workplace searches have involved job-related searches by public employers,[187] the handful of cases involving searches of private work spaces by law enforcement officials have largely been resolved in the same way as *Muick*.[188]

In brief, these cases reveal that the increased capacity of employers to surveil their employees has, in fact, led directly to a decreased expectation of privacy vis-à-vis the government. Employees who are subject to private surveillance in the workplace are generally defenseless when the government seeks to collect data from their workplace as well.

B. *Commercial Information Misuse*

There are many laudable reasons to allow retailers to collect and even share information about those with whom they do business.[189]

---

[186] *Id.* at 743.

[187] *See, e.g.*, United States v. Simons, 206 F.3d 392, 398, 400 (4th Cir. 2000) (applying the *O'Connor* exception to the warrant requirement to a search by CIA administrators of an employee's computer, notwithstanding the fact that the administrators conducted the search "to acquire evidence of criminal activity"); *see* United States v. Slanina, 283 F.3d 670, 678 (5th Cir. 2002), *vacated on other grounds sub nom.* Slanina v. United States, 537 U.S. 802 (2002) (following *Simons* and finding that "*O'Connor*'s goal of ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal"); United States v. Fernandes, 272 F.3d 938, 942–43 (7th Cir. 2001) (finding the *O'Connor* standard applicable to a post-firing search of a prosecutor's office); *see also Taketa*, 923 F.2d at 673–75 (holding that an initial search of a law enforcement officer's office was subject to the *O'Connor* exception to the warrant requirement, but that a subsequent, unwarranted videotaping of that office was not).

[188] *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1132, 1134 (10th Cir. 2002) (finding no reasonable expectation of privacy in a college professor's work computer when the university had a written computer policy stating that it reserved the right to "view or scan any file or software stored on the computer or passing through the network, and will do so periodically"); *see also* Dir. of Thrift Supervision v. Ernst & Young, 795 F. Supp. 7, 10 (D.D.C. 1992) (holding that employees and partners of private accounting firm have no reasonable expectation of privacy in work-related diaries kept in their offices for business purposes). In *United States v. Bailey*, the United States District Court, Nebraska, stated that the defendant had

> no expectation of privacy in the work computer owned by someone else because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer. Such repeated warnings about consent to search, followed by such repeated acknowledgments, categorically and without more defeat Bailey's claim of privacy.

272 F. Supp. 2d 822, 824 (D. Neb. 2003).

[189] For a more detailed analysis of the benefits of information sharing, see generally THE FIN. SERVS. ROUNDTABLE, CUSTOMER BENEFITS FROM CURRENT INFORMATION SHARING BY FINANCIAL SERVICES COMPANIES (2000), *available at* http://www.netcaucus.org/books/privacy2001/pdf/ernstyoungreport.pdf.

For example, Amazon.com, the online retailer that I use most often, knows a lot about me. It knows what books, compact discs, and clothing I have purchased. It can probably conclude from my late interest in infant clothing that I have recently had a child. It knows what items I have considered buying based on what I have placed in my virtual shopping cart but not actually purchased. Allowing Amazon.com to collect and analyze this information can be a very good thing. If I have purchased two compact discs from a particular artist in the past, I might want to know that the artist has recently released a new album. I might also want to know that people who enjoy the band whose compact discs I have purchased seem to like another band's releases as well. Similarly, I might want to be alerted to sales on merchandise I have perused in the past but not purchased. If I am bound to be targeted by online retailers, and I am, it would be nice if that advertising could be relevant to my previously expressed preferences.

Of course, there is also a downside to Amazon.com having this information about me. It could choose to share this information with others without my permission. It could reveal it to the public either accidentally or in order to embarrass me. Its employees could misuse my private information for their own purposes. All of these risks prompted Scott McNealy, the CEO of Sun Microsystems, to infamously remark when queried about his company's privacy policy, "You already have zero privacy—get over it."[190]

1. State of the Art

Many of the concerns regarding the misuse of consumer information involve the enormous databases of information that retailers and advertisers are able to compile.[191] Perhaps the most well-known case of purported commercial information misuse was the DoubleClick incident of 1999.[192] DoubleClick, a direct marketer that pro-

---

[190] John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A1.

[191] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003) ("Both on- and offline, businesses are collecting and warehousing staggering amounts of personal information about American citizens and compiling it into electronic dossiers designed to predict the way people think and behave. More than 1000 data-mining companies collect and sell data about U.S. consumers.").

[192] *See, e.g.*, *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001). For a discussion of the facts of the case, see Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 439–43 (2002). *See generally* Amy S. Weinberg, *These Cookies Won't Crum-*

vided advertisements for websites, compiled browsing information on more than one hundred million web users.[193] When DoubleClick acquired a company that gathered information on individuals' offline purchasing trends, it announced that it would be combining its two databases in a way that might make it possible to identify, by name, the buying and surfing habits of individuals included in both databases.[194] Although a consolidated lawsuit challenging the company's plans was eventually dismissed for failure to state a claim,[195] negative publicity forced DoubleClick to curtail its plans.[196]

The desire of advertisers to obtain, store, and mine demographic information on potential customers was hardly extinguished, however, with the public firestorm that surrounded the DoubleClick case. Directed advertising remains the dream of those who advertise online. For example, the *New York Times*'s website recently announced that it would allow advertisers to reach its readers based on the type of story those readers most often accessed.[197] So, for example, a sporting goods manufacturer might be interested in advertising to those readers who had clicked on three or more sports articles in a given period of time.[198] There is little reason to think that negative publicity alone

---

ble—Yet: The Corporate Monitoring of Consumer Internet Activity, In Re DoubleClick Inc. Privacy Litigation, *154 F. Supp. 2d 497 (S.D.N.Y. 2001)*, 21 TEMP. ENVTL. L. & TECH. J. 33 (2002).

[193] *DoubleClick Unveils an Initiative to Protect Users' Online Privacy*, WALL ST. J., Feb. 15, 2000, at B6.

[194] Andrea Petersen, *A Privacy Firestorm at DoubleClick: Web Highflier's Executives Blinded by a Backlash, Are Scrambling to Recover*, WALL ST. J., Feb. 23, 2000, at B1 (explaining that "[w]hat makes privacy advocates so crazy is that a combined DoubleClick-Abacus database can now connect Web sites someone visits with that person's real name and address").

[195] The plaintiffs in the *DoubleClick* litigation brought their claims under the following three acts: the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2701–2711 (2000), the Wiretap Act of 1968, 18 U.S.C. §§ 2510–2522 (2000), and the Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (2000). *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d, at 500. All three of the claims were dismissed by the federal district court, and the parties reached a settlement agreement prior to plaintiffs' appeal of that ruling. *Id. See generally* Weinberg, *supra* note 192.

[196] Andrea Petersen, *DoubleClick Reverses Course After Privacy Outcry*, WALL ST. J., Mar. 3, 2000, at B1 (explaining that "[i]n a stunning about-face, online advertising firm DoubleClick Inc. says it will not connect people's names, addresses and other personal information with the data it collects about where they go on the Web, at least until government and industry set privacy standards").

[197] Stefanie Olsen, *NYTimes.com Gears Ads to Surfers' Habits*, *at* http://news.com.com/NYTimes.com+gears+ads+to+surfers+habits/2100-1023_3-984575.html (Feb. 13, 2003) (explaining that "[t]he theory [behind targeted advertising] is that if marketers can match their products to already-interested parties . . . then everybody wins").

[198] *See id.*

will be sufficient to slow this trend toward data accumulation and targeted advertising in the near future.

2. Fourth Amendment Implications

Currently, consumers are protected against the misuse of their information mainly by the negative publicity surrounding the misuse of this information.[199] Federal law governs this area only tangentially and in some cases actually facilitates the sharing and selling of this information.[200] Just as the greatest restraint on what employers may do in the employment context is the employer's own promises on that point, so in the e-commerce area, one of the greatest constraints on how an electronic retailer may gather and share the information it gathers is the company's own stated privacy policy. For example, when Northwest Airlines revealed earlier last year that it had given the National Aeronautic and Space Administration data on as many as ten million passengers, one of the Airline's principal defenses was that it had not violated its own privacy policy.[201] Distinguishing itself from JetBlue Airways, which had earlier admitted to violating its own privacy policy, Northwest officials defended their actions by arguing that they had given the information directly to a government agency that had an obligation to safeguard that information and that such disclosure was not inconsistent with its stated policies.[202]

Furthermore, it is difficult to see why courts will not treat the information compiled on consumers by retailers, advertisers, and direct marketers, both online and elsewhere, like they treated the banking and phone records in *Miller* and *Smith*, respectively.[203] Because consumer information has been conveyed willingly to a third party—because you know that your online retailer maintains these records, for

---

[199] For example, the Gramm-Leach-Bliley Act of 1999 allows companies to share consumer information with affiliated entities, and to share it with unaffiliated entities unless consumers opt out of the Act's provisions. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in relevant part at 15 U.S.C. § 6802 (2000)). *See* McClurg, *supra* note 191, at 133–37.

[200] *See* McClurg, *supra* note 191, at 133–37.

[201] *See* Matthew L. Wald, *Airline Gave Government Information on Passengers*, N.Y. TIMES, Jan. 19, 2004, § 1, at 16.

[202] *See Airline Addresses Data-Sharing Denials*, N.Y. TIMES, Jan. 19, 2004, at A10.

[203] *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1141 (2002) (explaining that "[c]ommunications service providers frequently store their customers' communications. These probably fall under the third-party record rule of *Smith v. Maryland* and *United States v. Miller* because third parties maintain the information.") (citations omitted).

example—it is very unlikely that the government will be held to invade a reasonable expectation of privacy when it attempts to access these records.[204] If anything, there is likely to be less protection for consumer information than for the arguably more sensitive information regarding one's phone calls and finances.

Thus far, there has been a relative dearth of reported cases involving the Fourth Amendment protections afforded to information collected by commercial entities. In fact, all of the reported cases in this area have dealt with privacy interests in the context of an Internet service provider ("ISP").[205] Furthermore, in each case the court concluded that there is no expectation of privacy in information one shares with an ISP. For example, in *United States v. Hambrick*,[206] a Virginia district court held that individuals have no reasonable expectation of privacy in information they have freely chosen to share with their ISPs:

> [W]hen Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. Mr. Hambrick also selected [his] screen name. . . . When the defendant selected his screen name it became tied to his true identity in all MindSpring records. MindSpring employees had ready access to these records in the normal course of MindSpring's business, for example, in the keeping of its records for billing purposes, and nothing prevented MindSpring from re-

---

[204] This concern is neither merely hypothetical nor limited to the online context. A relatively well-known example comes from my home state of Colorado. *See* Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1063 (Colo. 2002). During a raid on a drug lab, officers found two books on the making of methamphetamine along with a mailing envelope from a local bookstore. *Id.* at 1048. Utilizing first a subpoena and then a search warrant, law enforcement officials attempted to obtain evidence of what books were sent to the house and to whom. *Id.* at 1049. The bookstore fought the requests, and the Colorado Supreme Court ultimately decided that the requests for the information violated the First Amendment rights of the store's clients. *Id.* at 1063.

[205] *See* 17 U.S.C. § 512(k)(1)(A) (2000) ("[T]he term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, *without modification to the content of the material as sent or received.*") (emphasis added); Monica Vir, Note, *The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks?*, 29 RUTGERS COMPUTER & TECH. L.J. 193, 193 n.1 (2003) (citing 17 U.S.C. § 512(k)(1)(A)) (indicating that "[e]xamples of Internet service providers include America Online ('AOL') and CompuServe").

[206] 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999).

> vealing this information to nongovernmental actors. Also, there is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant's personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.[207]

Just as Miller waived an expectation of privacy in his personal data by sharing it with his bank, so Hambrick waived any expectation of privacy in his personal information by sharing it with his ISP.[208] To date, each of the courts that has considered the question has ruled the same way.[209]

Furthermore, each time the issue has arisen, the courts have held that the existence and possible violation of a relevant federal statute—either the ECPA or the Cable Communications Policy Act (the "CCPA")—neither created a reasonable expectation of privacy nor required suppression as a remedy. For example, in *Hambrick*, the Court found the following:

> Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of "reasonably objective" for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act. Additionally, the ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental en-

---

[207] *Id.*

[208] *See id.*

[209] *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (citing California v. Greenwood, 486 U.S. 35, 39 (1988); Katz v. United States, 389 U.S. 347, 351 (1967); and *Smith*, 42 U.S. at 743–44) ("When defendant entered into an agreement with Road Runner for Internet service, he knowing revealed all information connected to [his] IP address. . . . He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information."); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) (citing *Kennedy*, 81 F. Supp. 2d at 1110) (reaching the same conclusion); *see also* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 73 n.48 (2000) (collecting cases).

> tities. For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information.[210]

Hambrick and the cases decided along similar lines demonstrate that the courts will afford little protection to information disseminated for commercial purposes. Even if that information is disclosed to a single entity for a narrow purpose, even if that information is protected by a privacy statute if accessed by a private actor, and even if the government conduct in question would violate that statute, the courts are unlikely to find a reasonable expectation of privacy.

C. *Medical Information*

The information we share with our medical professionals reveals the most intimate details of our lives.[211] Our private habits both legal and illegal, sexual practices, family characteristics, and psychological history can all be relevant to medical treatment. We reveal things to our doctors that we might not reveal to our spouses, families, or friends,

---

[210] 55 F. Supp. 2d at 507 (citation omitted); *see Kennedy*, 81 F. Supp. 2d at 1111. In *United States v. Kennedy*, the United States District Court held the following:

> This court need not decide whether the [Cable Communication Policy Act] was violated in the instant action because even if it were, defendant still would not be entitled to suppression of the evidence as a remedy for the violation. As with the ECPA, the CCPA speaks nothing of an exclusionary remedy, only a civil remedy.

81 F. Supp. 2d at 1111.

Interestingly, it is not at all clear what the result would be if Congress in fact had decided, as part of a regulatory regime, that a particular class of data or information is entitled to Fourth Amendment protections. This conclusion would, ostensibly, be an interpretation of the Fourth Amendment, an interpretation the Supreme Court would not be required to validate. For example, the Supreme Court has rejected Congress's conclusions regarding when conduct substantially impacts interstate or foreign commerce. *See* United States v. Lopez, 514 U.S. 549, 567–68 (1995). Similarly, the Court might reject Congress's conclusion that a particular expectation of privacy is reasonable. *See id.*

[211] *See, e.g.*, Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 302 (2003) ("Medical information is almost always sensitive. Having the world learn about one's Prozac prescription can be embarrassing; having the world learn about one's HIV-positive status can be life-shattering.").

and that we certainly do not want our employers, neighbors, insurance companies, or law enforcement officials to become aware of. Because of its sensitivity, the wrongful or careless disclosure of medical information strikes a very resonant chord with those concerned about their privacy.

There is mounting evidence that information shared with health care providers and insurers is being sought and obtained by private entities that have no legitimate interest in its use. The Health Privacy Project, a research institute associated with Georgetown University, lists some egregious recent examples on its website:

> Terri Seargent, a North Carolina resident, was fired from her job after being diagnosed with a genetic disorder that required expensive treatment. . . . [S]he suspected that her employer, who is self-insured, found out about her condition, and fired her to avoid the projected expenses.
>
> . . . .
>
> An Atlanta truck driver lost his job in early 1998 after his employer learned from his insurance company that he had sought treatment for a drinking problem.
>
> Joan Kelly was automatically enrolled in a "depression program" by her employer, Motorola, after her prescription drugs management company reported that she was taking antidepressants.[212]

1. State of the Art

Like the misuse of commercial information, one of the main threats to medical privacy is the maintenance of large databases of information.[213] When a patient's file was a physical object that remained

---

[212] HEALTH PRIVACY PROJECT, MEDICAL PRIVACY STORIES 1 (2003), *available at* http://www.healthprivacy.org/usr_doc/storiesupd.pdf (last updated Nov. 10, 2003) (citations omitted). Professor Paul M. Schwartz stated the following:

> In the United States approximately 140 million people, or nearly two-thirds of the population under sixty-five, receive medical benefits through their job. Because these benefits are an increasingly costly part of the overall package of compensation, employers have a great incentive to weed out workers with expensive health care needs.

See Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 26 (1997) (citations omitted).

[213] *See, e.g.*, DeVries, *supra* note 211, at 302 (explaining that "[w]hile digital technology can save money and allow life-saving medical information to be instantly sent between

in the doctor's office, the possibility of prying eyes discovering its contents was relatively low, and the risks of widespread disclosure were almost non-existent.[214] As the information conveyed to doctors increasingly becomes stored electronically and aggregated with others' information, however, the possibilities of misuse multiply almost exponentially.[215]

Despite these risks, there are also great benefits to aggregating and digitalizing medical information. These processes make possible the sharing of medical information between different healthcare providers virtually instantaneously, thereby facilitating the delivery of medical care wherever the patient seeks it.[216] Furthermore, extensive databases of medical information may allow medical research to be conducted in ways unimaginable before widespread information shar-

---

hospitals and doctors, the same technology also heightens the possibility of mistake or misuse").

[214] *But see* HEALTHY PRIVACY PROJECT, *supra* note 212, at 4–5 (containing examples of disclosure of medical records based on misplaced or lost physical files).

[215] *See, e.g.*, DeVries, *supra* note 211, at 307–08 (arguing that "[t]he underlying problem of informational privacy in the digital age is the ability to access and aggregate vast amounts of otherwise harmless personal data into a form that can do real damage to the individual's sense of self-determination and autonomy"). Professor Julie E. Cohen stated the following:

> Collections of information about, and identified to, individuals have existed for decades. The rise of a networked society, however, has brought with it intense concern about the personal and social implications of such databases—now, in digital form, capable of being rapidly searched, instantly distributed, and seamlessly combined with other data sources to generate ever more comprehensive records of individual attributes and activities.

Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000).

[216] *See, e.g.*, Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497, 1501 (2002). Professor Peter D. Jacobson offered the following explanation:

> [S]haring [medical information] among medical professionals may be crucial for monitoring the quality of care and for maintaining continuity of care. For example, physicians and pharmacists must have accurate data on all pharmaceuticals a patient takes to prevent adverse drug-drug interactions. The American Hospital Association (AHA) argues that health professionals need a full picture of the patient's health, not a small amount of information about one specific condition, to avoid complications.

Id. (citation omitted); *see also* Schwartz, *supra* note 212, at 53 (arguing that "[t]he multifunctional patient record has the potential to heighten the efficiency of the health care business. It also is capable of leading to improvements in medical science.").

ing became possible.[217] Like the databases of consumer information discussed in the previous section, therefore, the problem is not with the information's aggregation and use per se, but rather with the enormous potential for misuse that coincides with it.

2. Fourth Amendment Implications

Federal law now expressly regulates medical information privacy; HIPAA became effective on April 14, 2003.[218] HIPAA creates Privacy and Security Rules applicable to "protected health information" held or transmitted by covered entities and their affiliated businesses.[219] HIPAA's coverage is both extensive[220] and strict—unless an exception to the privacy provisions applies, "a covered entity may not use or disclose protected health information."[221]

Prior to the passage of HIPAA there was a wide split of authority in both the state[222] and federal[223] courts regarding whether or not in-

---

[217] *See, e.g.*, Jacobson, *supra* note 216, at 1501–02 (arguing that a positive use of medical information databases can be the facilitation of medical research).

[218] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of chapters 26, 29, and 42 of the United States Code). For a good summary of the law's provisions, see generally U.S. DEP'T OF HEALTH & HUMAN SERV., SUMMARY OF THE HIPAA PRIVACY RULE (2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf (last revised May 2003).

The Supreme Court has long implied that the right to privacy it identified in *Roe v. Wade* and *Griswold v. Connecticut* governs medical information and decision making. *See* Whalen v. Roe, 429 U.S. 589, 599–600 (1977) (citing *Roe*, 410 U.S. 113, 153 (1973); and *Griswold*, 381 U.S. 479, 484 (1965)) (concluding that the state statute at issue was not sufficiently invasive to infringe on a right the plaintiff might have to medical information privacy).

[219] 45 C.F.R. § 160.103 (2004).

[220] The Act provides a federal floor for the protection of medical privacy. States remain free to provide greater protections. *See* 45 C.F.R. § 160.203 (2003); *see also* Nat'l Abortion Fed'n v. Ashcroft, No. 04 C 55, 2004 WL 292079, at *2–3 (N.D. Ill. Feb. 6, 2004) (finding that subpoenas issued in a federal action may be quashed under Illinois privacy law, though they would be permitted under HIPAA).

[221] 45 C.F.R. § 164.502(a) (2003).

[222] *Compare* Commonwealth v. Riedel, 651 A.2d 135, 139 (Pa. 1994) (finding a reasonable expectation of privacy in medical information), *with* People v. Perlos, 462 N.W.2d 310, 316 (Mich. 1990) (finding no reasonable expectation of privacy in medical information), Tims v. State, 711 So.2d 1118, 1122 (Ala. Crim. App. 1997) (finding no reasonable expectation of privacy in medical information), *and* State v. Fears, 659 S.W.2d 370, 375–76 (Tenn. Crim. App. 1983), *cert. denied*, 465 U.S. 1082 (1984) (finding no reasonable expectation of privacy in medical information).

[223] *Compare* F.E.R. v. Valdez, 58 F.3d 1530, 1535 (10th Cir. 1995) (finding a reasonable expectation of privacy in medical records), *and* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) (finding that "[t]here can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection"), *with* Webb v. Goldstein, 117

dividuals had a reasonable expectation of privacy in their medical information, particularly in information that was held by third-parties. For example, in the Rhode Island case of *State v. Guido*,[224] the defendant was involved in a serious car accident and was taken to a hospital where his blood was drawn pursuant to normal hospital protocols.[225] Three days later a subpoena *duces tecum* was requested and issued for defendant's medical records from the hospital.[226] The records were turned over to the authorities and indicated that the defendant's blood alcohol level was more than twice the legal limit at the time he was admitted to the hospital; the defendant was subsequently indicted for driving under the influence with serious bodily injury resulting.[227]

Both prior to trial and following his conviction, Salvatore Guido challenged the introduction of medical records to indicate that he was intoxicated.[228] On appeal, the Rhode Island Supreme Court affirmed the conviction, analogizing the medical records to the banking records at issue in *Miller*:

> In this case we conclude that defendant had no legitimate expectation of privacy in the medical records. We reach this conclusion largely on the basis that these records were produced by medical personnel for *their* use in providing medical treatment. These were not defendant's personal papers created or kept by him. The defendant can demonstrate neither ownership nor possession. For those reasons the records here more closely resemble the telephone records lawfully subpoenaed in *State v. McGoff*, or the bank records subpoenaed in *United States v. Miller*.[229]

In *State v. Hardy*, the Texas Court of Criminal Appeals came to the same conclusion in a lengthy opinion reciting similar facts.[230] The

---

F. Supp. 2d 289, 295–96 (E.D.N.Y. 2000) (finding no reasonable expectation of privacy on the part of a parolee in medical records released in connection with a rape investigation).

[224] 698 A.2d 729, 734 (R.I. 1997).

[225] *Id.* at 732.

[226] *Id.*

[227] *Id.*

[228] *Id.* at 732–33.

[229] *Guido*, 698 A.2d at 734 (citations omitted). In *State v. McGoff*, the Rhode Island Supreme Court analogized to *United States v. Miller* in finding that no reasonable expectation of privacy exists in records maintained by one's telephone company. 517 A.2d 232, 234 (R.I. 1986).

[230] 963 S.W.2d 516, 525–26 (Tex. Crim. App. 1997).

Texas court, however, found *United States v. Jacobsen*[231] to be more analogous than *Miller*:

> A subpoena for blood alcohol and drug information about the driver in an automobile accident is somewhat analogous to the chemical test in *Jacobsen*. A subpoena directed solely at blood alcohol and drug tests would, like the chemical test in *Jacobsen*, be a very narrow investigatory method designed to elicit evidence for a very narrow purpose.[232]

Other courts, in different contexts, *have* found a reasonable expectation of privacy in medical information, particularly when medical records are searched or seized as part of a broad investigation conducted without probable cause. For example, in *Doe v. Broderick*,[233] the Fourth Circuit was confronted with a search of the records of a methadone clinic as part of an investigation of a nearby armed robbery.[234] One of the clinic's patients subsequently brought suit under 42 U.S.C. § 1983, alleging that the search of the clinic violated his Fourth Amendment rights.[235] The Fourth Circuit found that there was a reasonable expectation of privacy in the records, although they were maintained by a third party:

> There is no question that Doe maintained a genuine subjective expectation of privacy in his records and files kept at the methadone clinic. The more interesting issue is whether a patient's expectation of privacy—Doe's expectation of privacy—in his treatment records and files maintained by a substance abuse treatment center is one that society is willing to recognize as objectively reasonable and thus comes within ambit of the Fourth Amendment's protections. We think it is.[236]

The court distinguished *Miller* on the ground that the Supreme Court's decision in that case was influenced by the Bank Secrecy Act

---

[231] 466 U.S. 109, 119–21 (1984); *see supra* notes 60–73 and accompanying text.

[232] *Hardy*, 963 S.W.2d at 525–26. In *Commonwealth v. Riedel*, the Pennsylvania Supreme Court came to a slightly different conclusion. *See* 651 A.2d at 141. Finding that there is a reasonable expectation of privacy in medical records, the court concluded that a search of those records was not unreasonable when a police officer merely wrote to the hospital to request those records rather than relying on a subpoena to obtain them. *Id.*

[233] 225 F.3d 440, 450 (4th Cir. 2000).

[234] *Id.* at 444.

[235] *Id.* at 445.

[236] *Id.* at 450 (citations omitted).

which required the bank to keep and maintain certain records.[237] "The relevant statute here . . . does quite the opposite, making access to the records more difficult for criminal investigation purposes. Under these circumstances, we think that the statute is a fitting indication that society is willing to recognize Doe's expectation of privacy as objectively reasonable."[238] Thus, although the court had been unwilling to find that the existence of a federal statute forbidding the dissemination of drug treatment information created a cause of action under § 1983, the court was willing to consider the statute's existence as relevant in determining whether or not a reasonable expectation of privacy existed in the drug treatment records.[239]

The implementation of HIPAA is unlikely to change this legal landscape significantly. In the Justice Department abortion subpoena case discussed in the Introduction,[240] the federal judge who ordered the subpoena quashed under Illinois law found that the subpoenas comported with HIPAA's provision for the release of medical records "in the course of any judicial or administrative proceeding . . . in response to an order of the court."[241] Thus, once again, the mere existence of a statute regulating or even punishing the disclosure of sensitive information was held insufficient to prohibit the government from acquiring that information in a criminal proceeding. Particularly when express provision is made for the use of sensitive material in a legal proceeding, courts are very unlikely to find that such disclosure violates the Constitution.

---

[237] 12 U.S.C. § 1829b (2000).

[238] *Broderick*, 225 F.3d at 450 (citation omitted) (citing 42 U.S.C. § 290dd(2) (2000)). The statute at issue prohibits, in most circumstances, the disclosure of "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research." 42 U.S.C. § 290dd-2(a). The statute also states that unless an exception applies, "no record referred to in subsection (a) of this section may be used to initiate or substantiate any criminal charges against a patient or to conduct any investigation of a patient." *Id.* § 290dd-2(c). Finally, the statute provides for criminal penalties for anyone violating its provisions. *Id.* § 290dd-2(f).

[239] *See Valdez*, 58 F.3d at 1535 (noting that defendants in a § 1983 action concede that plaintiffs have a reasonable expectation of privacy in medical records kept by a psychiatrist where that psychiatrist's office is searched in a Medicaid fraud investigation); United States v. Burzynski Cancer Research Inst., 819 F.2d 1301, 1310 (5th Cir. 1987) (finding on similar facts that patients "have a privacy interest" in their medical records but that the search and seizure of them on the facts presented was reasonable).

[240] *See supra* notes 1–18 and accompanying text.

[241] *Nat'l Abortion Fed'n*, 2004 WL 292079, at *2 (quoting 45 C.F.R. § 164.512(e)(1) (2003)).

D. *Summary*

As I stated at the outset of this Part, my goal was not to catalogue systematically the myriad ways in which individuals are under surveillance in the United States today—given recent events and developments, such an analysis would be virtually impossible in any single article.[242] Rather, this Part was meant to highlight some of the most serious threats to individual privacy posed not by government actors but by private actors. It is clear that private surveillance, information sharing, and information acquisition are widespread and growing, and that technological innovation will only accelerate the capacity of private actors to gain access to our "private" information.

Technological development in each of these areas is neither an unmitigated good nor an unmitigated evil, however. As the benefits and costs of digitization, aggregation, data-mining, and the like are evaluated, one factor that is often excluded from the calculus is the unconscious externality of increased government surveillance. As even this brief selection of topics and cases makes clear, courts are considering the pervasiveness of private intrusions when determining whether a reasonable expectation of privacy exists, and they often use those private invasions to validate invasive governmental conduct.

IV. How to Increase Privacy Protections

In this Part, my focus moves briefly from the descriptive and analytical to the prescriptive. I argue that if the discussion above is accurate, increased privacy protections will come in one of the following three ways: the Supreme Court will abandon its adherence to an assumption-of-risk reading of the Fourth Amendment, thereby delinking private and governmental conduct; civil privacy protections will be extended to cover more people and to offer greater protections, resulting in fewer and fewer non-governmental intrusions on privacy; or individuals will begin to take practical steps to protect themselves from invasions of privacy, making it more difficult for any actor—governmental or private—to acquire their private information. I cover each of these possibilities in turn, concluding that only the last is likely to provide much solace for privacy advocates in the near future.

---

[242] *See, e.g.*, Ethan Brouner, *Collateral Damage*, N.Y. Times, Feb. 22, 2004, § 7, at 10 (reviewing eight new books dedicated to the subject of privacy in contemporary America).

A. *Moving Beyond Assumption of Risk*

As discussed above, what I describe as the current crisis in American privacy law dates from the Supreme Court's 1967 decision in *Katz v. United States*.[243] At the time it was decided, *Katz* was rightly seen as a privacy boon, another Warren Court decision extending individual rights.[244] *Katz* overturned *Olmstead v. United States*, announced that privacy was an individual, portable right, and extended Fourth Amendment protections to areas and activities to which they had never previously applied.[245] Over time, however, the shifting meaning of the Fourth Amendment that was adopted in *Katz* has come to be seen as a threat as well as a benefit to civil liberties.[246]

No clear alternative to *Katz*'s conception of the Fourth Amendment has yet emerged, however. Although proposed alternative conceptions of privacy rights have ranged from a return to a textually-based interpretation of the Fourth Amendment,[247] to the passage of a constitutional amendment explicitly establishing a right to privacy,[248] to the creation of a federal agency to monitor privacy,[249] to an appeal to *Lochner*-era formalist interpretation,[250] no consensus has yet devel-

---

[243] 389 U.S. 347, 361 (1967).

[244] *See, e.g.*, Michael E. Tigar, *The Supreme Court 1969 Term—Foreword: Waiver of Constitutional Rights: Disquiet in the Citadel*, 84 HARV. L. REV. 1, 12–13 (1970) (praising the Court for moving from a Fourth Amendment based on property rights to one in which "[t]he emphasis is placed on the will of the actor").

[245] *See supra* notes 44–54 and accompanying text.

[246] *See supra* notes 55–56 and accompanying text.

[247] *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 92–94 (1998) (Scalia, J., concurring) (arguing for a return to a reading of the Fourth Amendment based on the text of the Amendment as it would have been understood by the Founders).

[248] *See, e.g.*, Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 77 (1994) (attributing a call for such an amendment to Harvard Law Professor Laurence H. Tribe).

[249] *See, e.g.*, Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 236 (1993). Robert M. Gellman provided the following explanation:

> Of the four major privacy studies identified in the last twenty years, three recommend the establishment of a permanent new federal agency with responsibilities including privacy policy. The fourth study, the earliest of the four, rejected the notion of a privacy regulatory agency, although it did recommend institutional change within one cabinet department to implement and oversee recommended new privacy policies.

Id.

[250] Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 561 (1996) (arguing that although "[e]ach of the *Lochner* era approaches has defects," they "can be integrated into a vibrant and effective theory of the Fourth Amendment").

oped regarding how to improve on the *Katz* formulation. Thus, *Katz* is apparently here to stay, seemingly unloved by conservatives and liberals alike, but not so intolerable to either group that a consensus for replacing it has emerged. Perhaps part of the doctrine's current appeal is its malleability—it means whatever a majority of the Court thinks it means. Although the doctrine has been criticized precisely because of its imprecision, as long as both sides are able to utilize the doctrine equally to gain a majority of the Court's votes, they are equally unwilling to pursue its fundamental change.

Although the Court is thus unlikely to distance itself from the *Katz* formulation any time soon, it does not follow that its Fourth Amendment doctrine is entirely irredeemable. For example, the doctrine established in *Smith v. Maryland*[251] and *United States v. Miller*[252] that the exposure of information to anyone, even for a limited purpose, releases any expectation of privacy in that information, could be overturned without requiring an unlikely overhaul of the Court's entire Fourth Amendment jurisprudence. In place of this assumption-of-risk view of privacy,[253] the Court should adopt the reasoning it has employed elsewhere that societal expectations of privacy ought to be validated rather than ignored. As discussed above, in *Minnesota v. Olson*, the Court held that an overnight guest had a reasonable expectation of privacy in the home he was visiting and thus could object to evidence illegally seized from that home.[254] The Court reasoned that although the guest surrendered some of his privacy to his host, guests generally expect their hosts to honor their privacy.[255] In reaching this conclusion, the Court described its holding as "merely recogniz[ing] the everyday expectations of privacy that we all share."[256]

Had the Court applied these "everyday expectations of privacy" to the *Miller* and *Smith* cases, the result would likely have been very different. For example, the Court might reasonably conclude from the fact that nearly all people with the means to do so keep their money in bank accounts that they reasonably expect their privacy in their banking information to be respected. Just as the overnight guest

---

[251] 442 U.S. 735, 737 (1979).

[252] 425 U.S. 435, 436 (1976).

[253] *See, e.g.*, Skok, *supra* note 209, at 61 (noting that "[c]ourts employing assumption of risk analysis focus on the Supreme Court's decisions in *United States v. Miller* and *Smith v. Maryland*") (citations omitted).

[254] 495 U.S. 91, 99 (1990).

[255] *Id.*

[256] *Id.* at 98.

is aware of a risk that his host will betray him, yet nonetheless enjoys a reasonable expectation of privacy in another's home, so the bank patron, aware of the (relatively minute) risk of betrayal, ought to be entitled to a reasonable expectation of privacy in his financial records.

In his dissent in *California v. Greenwood*, Justice William Brennan made essentially this point, arguing the following:

> The mere *possibility* that unwelcome meddlers *might* open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home; or the possibility of a private intrusion negates an expectation of privacy in an unopened package; or the possibility that an operator will listen in on a telephone conversation negates an expectation of privacy in the words spoken on the telephone.[257]

Justice Brennan rightly saw the assumption-of-risk argument as something of a *reductio ad absurdum*. If we accept the premise that the possibility of a private intrusion negates a reasonable expectation of privacy, then, because private intrusion is almost always possible, nothing can ever be private.

In determining whether or not an expectation is in fact one that society is willing to validate, rather than one that is merely possible, the Court ought to be guided by more than its own intuitions regarding societal expectations of privacy.[258] As discussed above, the question of whether a particular area is widely perceived as private is an empirical one, one that social scientists can answer, and to a certain extent have answered.[259] Thus, calling on judges to consider societal expectations truly is more than an invitation for them to turn their personal views of privacy into law. By investigating current societal norms—as expressed through survey research, public referenda, and actual practices—judges can, as they did in *Olson*, both increase the scope of rights and confirm *Katz*'s promise that those expectations of

---

[257] 486 U.S. 35, 54 (1988) (Brennan, J., dissenting).

[258] Of course, this is exactly what many conservatives have accused the Court of doing in its post-*Katz* jurisprudence. *See, e.g.*, *Carter*, 525 U.S. at 97 (1998) (Scalia, J., concurring) (opining that "the only thing the past three decades have established about the Katz test . . . is that, unsurprisingly, those 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable") (citations omitted).

[259] *See generally* Slobogin & Schumacher, *supra* note 80 (reporting the results of a survey regarding the perceived invasions of a number of common searches).

privacy that society is willing to validate as reasonable will be protected in the face of expanding government surveillance.

Of course, the assumption-of-risk theory of reasonable expectation of privacy has not been limited to the *Smith* and *Miller* cases. Those two cases are merely an extension of the doctrine the Court announced in a number of other cases—*Ciraolo, Dunn, Greenwood,* and even *Katz* itself—that the police need not avert their eyes from what a person exposes or allows to be exposed to others.[260] It is a broad jump from this premise, however, to the finding that society is willing to accept police officers peering down from the skies, trespassing onto private property, rummaging through trash, or peering into homes with advanced imagers. The assertion that the mere possibility of such intrusion destroys an expectation of privacy follows from neither the text nor the principle of *Katz.*

B. *Increased Privacy Protection*

The second possible solution to the current conundrum of privacy law in the United States is affording greater protections to individuals from private invasions of privacy. If trespass laws are further expanded to cover invasions of privacy as well as physical invasions, if employees are able to contract for greater protection from surveillance by their employers, if websites offer enforceable protection for the information revealed by their users, then the bounds of private conduct will be circumscribed and the scope of permissible government conduct will likely contract as well.

The problem with the extension of civil privacy protections, however, is that the fit between the lawfulness of the conduct government

---

[260] In fact, what has been described as the assumption-of-risk theory has not been limited to this context. For example, in *Hoffa v. United States,* the Supreme Court held that no search or seizure occurs when a federal agent poses as a confidant of a criminal defendant, noting that "[n]either this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." 385 U.S. 293, 302 (1966). In *United States v. White,* the Supreme Court extended *Hoffa* to cover agents wearing hidden microphones, finding the following:

> If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.

White, 401 U.S. 745, 751 (1971).

agents are engaged in and whether or not the government is violating a reasonable expectation of privacy is hardly perfect. As the cases discussed in Parts II and III make clear, the existence of a property right or other civil protection is only one factor a court will consider in determining whether a reasonable expectation of privacy has been invaded.[261] Thus, even if privacy protections continue to be extended—offering individuals greater protection against their employers, neighbors, insurers, and the like—this extension may prove to be of little use against government actors who violate these provisions.[262]

For example, in *Greenwood*, the defendant argued that the search of his garbage that led to his conviction was illegal under California law and that this fact ought to insulate him against the evidence obtained against him.[263] The Court dismissed this assertion quickly, even though the provision to which Greenwood referred was contained in his state's constitution:

> We have never intimated . . . that whether or not a search is reasonable within the meaning of the Fourth Amendment depends on the law of the particular State in which the search occurs. We have emphasized instead that the Fourth Amendment analysis must turn on such factors as "our *societal* understanding that certain areas deserve the most scrupulous protection from government invasion." We have already concluded that society as a whole possesses no such understanding with regard to garbage left for collection at the side of a public street. Respondent's argument is no less than a suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment. We do not accept this submission.[264]

The Court was, of course, correct that the state governments assertions of the privacy expectations of their citizens are incapable of binding the federal courts. Such local determinations, however, at the very least, ought to be relevant to a federal court's determination of whether a particular individual enjoyed a reasonable expectation of

---

[261] *See supra* notes 174–188, 199–210, and 218–241 and accompanying text.

[262] I say nothing here of those instances in which a private individual has violated one of these provisions and turns incriminating evidence over to the government. Under current doctrine this evidence simply need not be excluded as there is no government conduct violative of the Fourth Amendment.

[263] 486 U.S. at 43.

[264] *Id.* at 43–44 (citations omitted).

privacy. Although the Supremacy Clause prohibits the states from dictating the bounds of federal law, nothing would prohibit a federal court from considering the fact that a state has protected the defendant against exactly the sort of privacy invasion engaged in by government agents in a given case.

In addition to the misfit between the legality of a search and the determination that the search infringes on the defendant's reasonable expectation of privacy, there is the additional concern that the existence of privacy protection in tort or contract will cause members of the public to become more lackadaisical in protecting their privacy. It would likely have come as a surprise to Ronald Dunn, for example, that federal officers could enter his property to look for drugs notwithstanding the "no trespassing" signs and fences that he constructed on that property.[265] In fact, we can be fairly certain that he would not have manufactured drugs in the way he did had he been aware of this fact. The protections that Dunn was afforded against his neighbors—the opportunity to sue them in trespass or to seek a criminal conviction against them should they enter his property without his permission—were thus worse than useless when it came to protecting him against governmental incursions. It is likely that if Dunn had not been lulled into a sense of security by the trespass laws of his jurisdiction, he either would have put up more and better fences or chosen to manufacture his drugs elsewhere.

Furthermore, the case law makes quite clear that the only way in which privacy statutes can effectively protect individuals from the use of their private information against them in criminal prosecutions is if the statutes explicitly prescribe exclusion as a remedy.[266] The courts have decided in a variety of contexts that the failure of legislatures to provide for exclusion as a remedy is an indication that they wished to make civil remedies exclusive.[267] Unless legislatures become willing to explicitly provide for exclusion—to state that evidence seized in a manner that would violate the statute if obtained by a private party

---

[265] *See* United States v. Dunn, 480 U.S. 294, 305 (1987).

[266] *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000) (finding that there was no need to decide if "the [Cable Communication Policy Act] was violated in the instant action because even if it were, defendant still would not be entitled to suppression of the evidence as a remedy for the violation. As with the ECPA, the CCPA speaks nothing of an exclusionary remedy, only a civil remedy."); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (finding that "[d]espite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the [Electronic Communications Privacy] Act").

[267] *See Kennedy*, 81 F. Supp. 2d at 1111; *Hambrick*, 55 F. Supp. 2d at 507.

may not be admitted in court—the passage of additional privacy provisions is unlikely to prevent the use in criminal proceedings of evidence seized in violation of these statutes.

My point is not that we are better off without trespass laws, without workplace protections, or without medical privacy rules; these rules can significantly increase our privacy, at least with regard to one another. And it is quite possible that increased privacy with regard to private actors may convince some courts that privacy protections against the government ought to be validated as well. Rather, my point is that these protections, alone, are unlikely to be sufficient to protect us from invasions by our government and may, in fact, make us more vulnerable to these invasions. As I argue in the next section, I believe that the only method for reliably achieving privacy from governmental intrusions is to take practical steps to make invasions of privacy by actors, public or private, as difficult as possible.

C. *Taking Practical Steps*

We come, finally, to what I argue is the most effective way to increase the protections we have against government surveillance. Individuals must take actual, practical steps to protect their information from all prying eyes, public and private. For example, Danny Kyllo's indoor marijuana cultivation was detected because he did not take sufficient steps to keep it from being discovered.[268] The facts of the case seem to indicate that the use of additional insulation could have made the heat produced by his grow lamps undetectable from outside his home.[269] Although the Court held that a presumptively invalid search occurred when the thermal imager was used in his case, future cases are unlikely to be resolved in a similar manner.

What is required is not for the public to become technophiles, to engage in a privacy arms race against government.[270] Rather, many of the steps that individuals can take to protect themselves from private snooping and from government searches are relatively straightforward. For example, inexpensive shredders make the reading of private correspondence, the obtaining of financial information, or the

---

[268] *See* Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

[269] *See id.*

[270] In fact, such an arms race might be very much against the public's interest. The goal is not to make discovery of information by the government impossible. Such a goal would be both unwise and largely unattainable. Rather, the goal is to make discovery of information by private citizens more difficult and thus to further guarantee the protection of that information vis-à-vis the government.

perusing of medical records impossible, even when those records are tossed into the common trash. In this sense, a twenty-five dollar device may be much more protective of privacy than a statute imposing civil or criminal penalties for those looking through disposed trash. Similarly, basic encryption software, available from any number of for-profit and not-for-profit purveyors, can do the work that the EPCA and the Wiretap Act simply cannot.[271] Because these techniques can make e-mail, web traffic, instant messaging, and the like almost impossible for a busy-body or snoop to read,[272] they significantly reduce the likelihood that a court will find that a defendant has abandoned a reasonable expectation of privacy in that conduct.[273] Even under the current assumption-of-risk reading of the Fourth Amendment, an individual who has made his e-mail unreadable by anyone except its intended recipient cannot reasonably be found to have waived a privacy interest in that information.

Clearly, asking individuals to take personal, practical steps to protect their privacy is no panacea. For example, it is virtually impossible to live in the modern era without sharing information with others. Although it may once have been possible to do without banks, without credit cards, and without leaving electronic footprints that could be retraced, that era has long since passed. Thus, the goal is to make people aware of the information they send into the world, to alert them to the nefarious uses to which that information can be put—not only by private actors but by the government as well—and to encourage them to minimize their exposure where they can.

There is no doubt that advocating vigilance against one's neighbors is a defeatist view of privacy today. Unfortunately, I believe that any other view of the current state of privacy law in the United States

---

[271] *See, e.g.*, ELEC. PRIVACY INFO. CTR., EPIC ONLINE GUIDE TO PRIVACY RESOURCES, *at* http://www.epic.org/privacy/privacy_resources_faq.html (last updated May 6, 2002) (listing some of the array of products available to make online life more private).

[272] *See, e.g.*, Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH. L. & POL'Y 135, 154 (2003) (explaining that "strong encryption makes e-mail practically impossible to decrypt and virtually pointless to intercept").

[273] Privacy groups generally recommend such practical steps as well. *See, e.g.*, ELEC. PRIVACY INFO. CTR., *What You Can Do to Avoid Profiling: Engage in Privacy Self Defense*, *at* http://www.epic.org/privacy/profiling/#selfdefense (last updated Oct. 13, 2004) (suggesting that "[w]herever possible, minimize the amount of personal data given to commercial or government entities. Do not release contact information where it is unnecessary. . . . Read privacy policies."); HEALTH PRIVACY PROJECT, WHAT YOU CAN DO TO PROTECT YOUR PRIVACY (2002) (encouraging members to read privacy policies and to closely guard those to whom they give their private data), *available at* http://www.healthprivacy.org/usr_doc/Checklist.pdf (last updated Oct. 22, 2002).

is simply unrealistic.[274] Until elected officials are willing to take up the cause of expanding protections against government, however, self-defense is the only course that remains available.

Conclusion

At the outset I described the Bush administration's now-abandoned plans for the formation of a Total Information Awareness program.[275] This plan set off alarm bells as civil libertarians on both the right[276] and the left[277] expressed concern that the agency, which would combine information from both governmental and private sources into an über-database, would signal the death of privacy in the United States.[278] As a result of this outcry, the agency has been abandoned and its mission has been scaled back.

The linkage between information gleaned by private sources and information gleaned by government sources, however, has already been made and will continue to exist regardless of the future of Total

---

[274] In fact, my view of the state of privacy in the United States today is considerably less pessimistic than the views of others. *See, e.g.*, *supra* notes 172, 190 and accompanying text (describing works authored by Jeffrey L. Seglin and John Markoff, respectively).

[275] *See supra* notes 5–7 and accompanying text.

[276] *See, e.g.*, William Safire, *Privacy Invasion Curtailed*, N.Y. Times, Feb. 13, 2003, at A41. William Safire argues the following:

> In the name of combating terrorism, [TIA] would scoop up your lifetime paper trail—bank records, medical files, credit card purchases, academic records, etc.—and marry them to every nosy neighbor's gossip to the FBI about you. [I have described] [t]he combination of intrusive commercial 'data mining' and new law enforcement tapping into the private lives of innocent Americans . . . as a supersnoop's dream.

Id. Similarly, Gene Healy argues the following:

> Some have suggested that [proposed TIA Director Adm. John] Poindexter's record as a former Iran-Contra defendant convicted of five felony counts of lying to Congress disqualify him from his position. But the question isn't whether Poindexter's the right man for the job; it's whether that job should exist in the first place.

Gene Healy, Cato Inst., *Beware of Total Information Awareness*, Daily Comment., *at* http://www.cato.org/dailys/01-20-03.html (Jan. 20, 2003).

[277] *See, e.g.*, Jay Stanley, *Is the Threat from "Total Information Awareness" Overblown?*, *at* http://www.aclu.org/privacy/Privacy.cfm?ID=11501&c=130 (Dec. 18, 2002) (arguing that "a close examination of existing public material on TIA makes several other points clear: the goal is to collect information about everyone, not just specific targets; privacy protections promised by Pentagon officials cannot be relied upon; and existing legal protections for privacy cannot be relied upon").

[278] *See, e.g.*, Solove, *supra* note 203, at 1084 (decrying the flow of information from private to public information collectors).

Information Awareness. Because courts have been instructed to look to private conduct when determining the permissible bounds of official conduct, the link between private invasions of privacy and government intrusion already exists, and it exists in a manner that is in many ways more insidious than the defunct Orwellian agency.