


Fall 2001

Fourth Amendment Privacy Interests

William C. Heffernan

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

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

Recommended Citation

William C. Heffernan, Fourth Amendment Privacy Interests, 92 J. Crim. L. & Criminology 1 (2001-2002)

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

CRIMINAL LAW

FOURTH AMENDMENT PRIVACY INTERESTS

WILLIAM C. HEFFERNAN*

I.	INTRODUCTION	2
II.	PRIVACY AND PERSONAL SECURITY: <i>ENTICK</i> TO <i>OLMSTEAD</i> TO <i>KATZ</i> ..	7
	A. The Fourth Amendment's Guarantee of Personal Security	9
	B. The Eighteenth Century Sources	12
	C. Trespass and the Eighteenth Century Heritage: Chief Justice Taft's Opinion for the Court in <i>Olmstead v. United States</i>	15
	D. The Court's Repudiation of the Trespass Standard in <i>Katz v. United States</i>	17
	1. <i>Katz</i> and the Court's Recognition of Privacy as an Independent Fourth Amendment Variable	18
	2. Vindicating the Court's Conclusions in <i>Katz</i>	19
	E. Fourth Amendment Pluralism	24
III.	DEVELOPING THE FORBEARANCE MODEL	31
	A. Post- <i>Katz</i> Privacy Jurisprudence: An Unreasonable Expectation of Eternal Vigilance	32
	1. The Anxious Quest for Privacy	38
	2. The Problem of Exposure to Third Party Facilitators	39
	3. Calculating What a Member of the Public Might Discover	39
	B. The Harlan Test I: From Social Expectations to Legally Enforceable Privacy Interests	40
	C. The Harlan Test II: Methods of Identifying Privacy Interests	45
	D. The Features of a Valid Privacy Claim	48
	1. The Different Types of Privacy: Privacy of the Person and Informational Privacy	52
	2. Interpersonal Privacy: Symmetrical and Asymmetrical Relationships	53
	3. Asymmetry in Surveillance Relationships	56

4. The "What" and "How" of Privacy Analysis: Conventional and Idiosyncratic Sources of Personal Vulnerability.....	57
5. Recapitulation.....	60
E. A Reasonable Expectation of Forbearance on the Part of Others.....	61
F. The Possibility of a Role Discount for the Police: Rejecting an Across-the-Board Discount While Accommodating the Government During Emergencies.....	67
IV. APPLYING THE FORBEARANCE MODEL.....	72
A. Settings Where Privacy Cannot Be at Stake.....	72
B. Observational Surveillance.....	80
1. Private Objects and Information.....	81
2. Privacy Cues.....	87
3. Surveillance of Behavior in Public Places.....	94
4. A Note on Technology and Privacy.....	101
C. Interactive Surveillance.....	106
1. Nonproblematic Settings.....	110
2. Harder Cases.....	118
CONCLUSION.....	126

I. INTRODUCTION

Is it possible to incorporate a serious concern for privacy into Fourth Amendment jurisprudence? Even before the terrorist attacks on America, the question was a pertinent one; in the aftermath, it has become even more so. Fourth Amendment case law is of course grounded in an explicit concern for reasonable expectations of privacy.² But given a long line of decisions rendered prior to the attacks, one could

* Professor of Law, John Jay College of Criminal Justice and the Graduate Center, City University of New York. Marc Bernstein, Janice Dunham, and Steve Wasserman provided helpful suggestions concerning an earlier draft of this article.

¹ The Fourth Amendment 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 particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

² Justice Harlan developed the expectation-of-privacy test in his concurring opinion in *Katz v. United States*, 389 U.S. 347, 361 (1967). Numerous opinions of the Court have since adopted Harlan's test for purposes of Fourth Amendment analysis. See, e.g., *Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990); *California v. Ciraolo*, 476 U.S. 207, 211 (1986).

hardly say that the Supreme Court has shown a *serious* concern for privacy. The Court, for example, has held that individuals do not have any Fourth Amendment privacy interests in their bank records,³ in the phone numbers they dial,⁴ or in freedom from low-flying surveillance of their backyards.⁵ Moreover, by the Court's analysis, even our garbage places us at risk. If someone wraps her garbage carefully in an opaque bag and places the bag on the street, that person, the Court has held, cannot expect the police to refrain from inspecting it to find out what's going on in her home.⁶

Clearly, the Court has parsed the concept of privacy as thinly as possible. It has expressed concern for residential privacy⁷—but has allowed police helicopters to conduct surveillance of backyards.⁸ It has expressed concern for the privacy of phone conversations⁹—but has said people have no privacy interest in the numbers they dial.¹⁰ Whether—or how much—terrorism's arrival in America will influence future privacy jurisprudence is hard to say, but it does at least seem clear that even before its advent the Court did not take privacy seriously as a Fourth Amendment value. My question at the outset, though, was not directly concerned with Supreme Court rulings. Rather, I asked whether it is *possible* to incorporate a serious concern for privacy into Fourth Amendment jurisprudence. In this Article, I argue that it is. But a cogent argument can be advanced to the contrary, an argument that requires special attention given the challenge that police work poses for privacy interests.

³ See *United States v. Miller*, 425 U.S. 435, 443 (1976).

⁴ See *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

⁵ See *Florida v. Riley*, 488 U.S. 445, 449-51 (1988); see also *Ciraolo*, 476 U.S. at 212-14.

⁶ See *California v. Greenwood*, 486 U.S. 35 (1988).

⁷ See *Payton v. New York*, 445 U.S. 573, 589 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of the home."); see also *United States v. Karo*, 468 U.S. 705, 714-15 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of government intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.")

⁸ See *Riley*, 488 U.S. at 449-51; see also *Ciraolo*, 476 U.S. at 212-14.

⁹ See *Katz v. United States*, 389 U.S. 347, 352 (1967) (A person using a telephone "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.")

¹⁰ See *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

The core features of this counterargument are easy to grasp. Privacy norms require people to exercise forbearance in everyday life: they require people *not* to act on their curiosity about their neighbors and officemates, *not* to encourage third-party confidences, *not* to snoop through incoming mail, and so on. But the police, it could be contended, must be exempted from these norms. This exemption is essential for the investigation of what the Court has called “ordinary criminal wrongdoing.”¹¹ It is wholly indispensable, one could continue, for police work on what the Court has called “special governmental needs”¹² (the investigation of terrorism quite clearly comes under this heading). Police officers, it could be conceded, must avoid *egregious* violations of privacy norms. Nothing more than this should be expected of them if they are to perform their function effectively.

Indeed, one could further argue that the Supreme Court’s privacy jurisprudence is admirable precisely because it draws the line here. The central principle of Fourth Amendment case law, it could be maintained, is that the police cannot engage in egregious privacy violations—for example, they must respect the privacy of the home¹³ and personal belongings carried outside the home.¹⁴ On the other hand, the corollary principle implicit in the case law is that the police are otherwise free to gather information about people—and so they can use helicopters to hover over backyards,¹⁵ can sift through people’s garbage,¹⁶ and so on. If undertaken by a layperson, the Court’s defender would say, these activities would be called “snooping.” When undertaken by the police, the defender might continue, the same activities should be endorsed as sound law enforcement practices.

Because it is too early to tell what effect, if any, the investigation of terrorism will have on privacy jurisprudence,¹⁷ I

¹¹ *E.g.*, *City of Indianapolis v. Edmond*, 531 U.S. 32, 38 (2000).

¹² *E.g.*, *Treasury Employees v. Von Raab*, 489 U.S. 656, 665-66 (1989).

¹³ See *supra* note 7 and accompanying text.

¹⁴ See *United States v. Chadwick*, 433 U.S. 1, 7-11 (1977).

¹⁵ *Florida v. Riley*, 488 U.S. 445, 449-51 (1988); *California v. Ciraolo*, 476 U.S. 207, 212-14 (1986).

¹⁶ *California v. Greenwood*, 486 U.S. 35, 39-40 (1988).

¹⁷ In a speech delivered at New York University Law School on September 28, 2001, Justice O’Connor stated that the attack on New York and Washington “has already altered our way of life. And it will cause us to re-examine some of our laws pertaining to criminal surveillance, wiretapping, immigration, and so on.” Linda Greenhouse,

devote the bulk of this Article not to the special problems that will arise in the aftermath of the attacks on New York and Washington, but to an examination of the argument, outlined above, as applied to police investigation of ordinary criminal wrongdoing. In particular, I respond in two ways to the claim that police are entitled to a discount from lay privacy expectations. First, I agree that the argument provides a *descriptively* accurate account of the Court's position on Fourth Amendment privacy protection. The Court, I suggest, has relied on a critical ambiguity in its privacy decisions. When speaking in general terms, it has made privacy protection appear to hinge on lay people's understandings of how they should treat each other—thus the significance of the often invoked reference to the expectations of privacy “that society is prepared to recognize as reasonable.”¹⁸ When resolving specific cases, though, the Court has reasoned in terms of a narrow, occupationally-grounded conception of privacy.¹⁹ The police, the Court has implied, perform a legitimate role as front-line information gatherers about the public.²⁰ They are thus entitled, it has further implied, to a special dispensation from

In a New Climate of Unity, Justices Face Divisive Issues, N.Y. TIMES, Oct. 1, 2001 A16. (Full copy of speech on file with author). It is not clear whether Justice O'Connor, in her use of the word “us” was referring to the American people through their representatives, the nine justices of the Supreme Court, or both. I argue, in any event, that the Court already has the doctrinal tools needed for responding to the threats posed by terrorism.

¹⁸ The original source for this is Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 361 (1967). The phrase appears, in slightly different form, in *Bond v. United States*, 529 U.S. 334, 338 (2000); *Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990); *Greenwood*, 486 U.S. at 39; *Ciraolo*, 476 U.S. at 211 (1986); *Oliver v. United States*, 466 U.S. 170, 179 (1984); *Marshall v. Barlow's Inc.*, 436 U.S. 306, 313 (1978).

¹⁹ The contrast between lay and occupationally-grounded expectations is readily apparent in *Greenwood*, which was concerned with the warrantless inspection of garbage. See *Greenwood*, 486 U.S. at 37-38. When outlining its general standard for assessing the case, the Court appealed to lay expectations, stating that the Fourth Amendment would be implicated if it could be shown that the defendants whose garbage was inspected “manifested a subjective expectation of privacy in [it] that society accepts as objectively reasonable.” *Id.* at 39. A page later, however, the Court justified warrantless police inspection of the defendants' garbage on the ground that scavengers and snoops have been known to sift through people's garbage. *Id.* at 40.

²⁰ The most telling example of this is to be found in the Court's invocation of scavengers and snoops in determining the proper role of the police when sifting through garbage. See *id.* Scavengers and snoops are at the front of the front-line in gathering information about others. In treating them as the baseline for determining the proper police role, the Court must also think of the police as legitimately performing the same function.

everyday privacy norms, one that doesn't extend to egregious violations but that does encompass minor ones.²¹

On the other hand, I argue that as a *normative* matter the distinction between occupationally-grounded and lay conceptions of privacy is constitutionally unacceptable. The Court, I suggest, has reasoned in terms of a vigilance model of privacy, one that requires people to be constantly alert to the way in which others can intrude on their lives.²² The vigilance model, I maintain, is inappropriate even when the investigation of terrorism is concerned; the proper approach there is to recalibrate the Fourth Amendment balancing test by taking into account the special urgency of public security while continuing to accord full weight to lay expectations of privacy. And when we move beyond the special problems occasioned by terrorism, we can see how wholly inappropriate the model is for the investigation of ordinary criminal activity. Vigilance is particularly troubling as an informing principle once one takes into account law enforcement's appetite for information and its capacity to feed it.

The Court, I suggest, has been blind to the points just made; indeed, it has fundamentally misconceived the nature of privacy norms. These norms are grounded not in vigilance but in an expectation of forbearance on the part of others—that is, in an expectation that others will restrain their curiosity with respect to those aspects of life that are essential to defining and maintaining individual identity. The notion of forbearance explains why privacy matters to us: we cherish it because it holds out the prospect of an *unanxious* shelter from the larger world. When the Court has spoken about reasonable expectations of privacy, it has appeared to be concerned with the substantial degree of forbearance that underlies everyday privacy norms though in fact it has reasoned in terms of the norms followed by

²¹ *See id.* The Court's favorable reference to snoops in *Greenwood* and its use of a snoop-baseline for determining the legitimacy of police behavior indicate that it is prepared to tolerate minor deviations by the police from everyday privacy norms. By contrast, its comments on the importance of privacy of the home underscore its unwillingness to tolerate egregious privacy violations. *See infra* note 7 for its comments on residential privacy.

²² For discussion of the vigilance model, *see infra* notes 119-27 and accompanying text.

those whose job is to penetrate privacy.²³ I argue that the Court should honor the premise implicit in its standard.

This Article is divided into three sections. The first examines the development of Fourth Amendment privacy doctrine; the final two provide a framework for improving contemporary doctrine. My aim in the first section is to trace the evolution of Fourth Amendment privacy jurisprudence—to show why eighteenth century courts linked privacy protection to the law of trespass and explain why it was proper for the twentieth century Supreme Court to sever this connection. In the second section, I outline a forbearance approach to privacy protection and contrast it with the Court's vigilance model. Even in settings where terrorism is under investigation, I maintain, privacy expectations, understood in terms of the forbearance model, are entitled to full respect. What distinguishes the policing of terrorism, I contend, is not the weight to be accorded privacy interests, but the extra emphasis entitled government interests in preserving public safety. In the final section, I apply the forbearance approach to specific Court decisions concerning ordinary criminal activity. In the course of this section, I consider not only those settings where police conduct surveillance of suspects but also those in which the police penetrate private life, either by encouraging individuals to betray intimate acquaintances or by seeking a foothold of false intimacy themselves.

II. PRIVACY AND PERSONAL SECURITY: *ENTICK TO OLMSTEAD TO KATZ*

Two issues—one conceptual, one interpretive—must be considered when thinking about Fourth Amendment privacy interests. The conceptual one has to do with the meaning of the term “privacy,” the interpretive with the Fourth Amendment's bearing on privacy. Clearly, the conceptual issue has priority: we need to understand what people mean when they talk about privacy before we can understand how the Fourth Amendment protects it. I thus begin this section with some provisional comments about the concept of privacy, comments I then use to examine changing interpretations of the Amendment. In the next section, I expand on these

²³ See *infra* note 181 for discussion of the analogy between journalists' and police use of helicopters to conduct surveillance of the curtilage of the home.

provisional remarks as I advance an alternative to the Court's account of Fourth Amendment privacy protection.

As a provisional matter, we can say that privacy has two strands. The first has to do with access to one's person, the other with information about key aspects of one's life. These strands can converge: when someone wishes not to reveal something about her person (a scar on her abdomen, a glandular disease, etc.), then limiting access to her person becomes essential to controlling the dissemination of information about herself. But they don't have to converge. Think first about access to one's person. If someone rushes home from a car trip announcing that her bladder is full and that she really needs to go to the bathroom, there is no information she's trying to withhold from others; nonetheless, once she reaches the bathroom, she'll want to be sure no one has access to her person while she's there. Now think about informational privacy. In the modern world, a person is often not in the place where information about her life is located. Indeed, one of the important features of informational privacy is that it allows people to circulate in the larger world while repositories of information about them remain closed to others.

If this is what we mean by "privacy," what justification can be advanced for respecting privacy interests? The general answer to this, which I refine later, is that people feel vulnerable about revealing information bearing on their personal lives and also about allowing unrestricted access to their persons. One can imagine a society in which people have no informational privacy. One can also imagine a society in which there is no privacy of the person; a society in which people dress, copulate, and excrete, among other things, without the benefit of seclusion. The mere mention of these possibilities suggests what it is that legitimates privacy claims: once we agree that people tend to feel vulnerable about granting access to their bodies or revealing facts concerning their intimate lives, we must also agree that they are entitled to avail themselves of the conventions of privacy and so reduce this sense of vulnerability to others.

A. THE FOURTH AMENDMENT'S GUARANTEE OF PERSONAL SECURITY

To provide even a rudimentary analysis of privacy is to establish a conceptual framework that goes beyond eighteenth century reflections on the subject. Although the *Oxford English Dictionary* records instances of the use of the word "privacy" in pre-eighteenth and eighteenth century literature,²⁴ these occasional sightings of the word must be considered in light of its absence from key eighteenth century documents dealing with political life. Perhaps the most important of these documents is the Constitution itself, which contains numerous references to other terms that matter in twentieth century life ("property,"²⁵ "religion,"²⁶ and "speech,"²⁷ for example), but none to privacy. Equally significant is the failure of the authors of *The Federalist Papers* to discuss the concept of privacy: Madison, for example, was deeply concerned about the protection of property rights but had nothing to say about privacy.²⁸ Historians warn us about the risk of interrogating the past in light of a conceptual

²⁴ Two of the sightings from pre-eighteenth century literature are two William Shakespeare plays: TROILUS AND CRESSIDA, act III, sc. iii, 190 (*Achilles*: "Of this my priuacie, I haue strong reasons." *Ulysses*: "But 'gainst your priuicie The reasons are more potent and heroycall.") and THE MERRY WIVES OF WINDSOR, act IV, sc. v, 24 (*Host*: "Let her descend: my Chambers are honourable; Fie, priuacy?"). It will be noted that the term "privacy" is not accorded positive value in either of these passages: it prevents the world from appreciating Achilles's heroic stature; in THE MERRY WIVES, it is a condition associated with secret goings-on. The sightings reported for the eighteenth century are more positive, but they are hardly abundant. 8 OXFORD ENGLISH DICTIONARY 1388 (1933)..

²⁵ "No person shall . . . be deprived of life, liberty, or property, without due process of law . . . nor shall any private property be taken for public use, without just compensation." U.S. CONST. amend. V.

²⁶ "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof . . ." U.S. CONST. amend. I.

²⁷ "Congress shall make no law . . . abridging the freedom of speech . . ." U.S. CONST. amend. I.

²⁸ "This term [property], in its particular application, means 'that dominion which one man claims and exercises over the external things of the world, in exclusion of every other individual.' [quoting Blackstone] In its larger and juster meaning, it embraces everything to which may attach a value and have a right, and which leaves to everyone else the like advantage."

THE MIND OF THE FOUNDER: SOURCES OF THE POLITICAL THOUGHT OF JAMES MADISON 243 (Marvin Meyers ed., 1976) (quoting James Madison, *Property*, NATIONAL GAZETTE, March 29, 1772); see also JENNIFER NEDELSKY, PRIVATE PROPERTY AND THE LIMITS OF AMERICAN CONSTITUTIONALISM: THE MADISONIAN FRAMEWORK AND ITS LEGACY (1990).

framework derived from the present.²⁹ This risk must be borne in mind when thinking about the Fourth Amendment. Privacy is an abiding concern of the present age. As far as the Fourth Amendment is concerned, we must begin by reasoning in terms of one of the abiding concerns of the eighteenth century—that is, we must begin by reasoning in terms of its profound respect for property rights.

“There is nothing,” Blackstone remarks in his *Commentaries*, “which so generally strikes the imagination, and engages the affections of mankind, as the right of property.”³⁰ Important as it was for many branches of the common law, property law and, in particular, the bundle of rules collected under the heading of “trespass” were especially significant in determining the search and seizure liability of government agents. According to eighteenth century common law cases, a necessary condition for establishing such liability was proof that one of the government’s agents had trespassed on someone’s property.³¹ Clearly, this trespass approach to searches and seizures provides substantial protection for privacy interests. Trespass on someone’s person—an arrest can be defined as a trespass in this sense³²—interferes with privacy of the person. Similarly, a trespassory incursion into someone’s home interferes with informational privacy, and, if the owner is home, interferes with privacy of the person as well. On this analysis, however, privacy of person and informational privacy are only *incidentally* protected by the law of search and seizure. Put differently, we can say that if trespass is to function as a necessary condition for search and seizure liability, then certain matters that clearly come under the heading of “privacy” cannot be actionable in

²⁹ “[W]hen we organize our general history by reference to the present we are producing what is really a gigantic optical illusion” HERBERT BUTTERFIELD, *THE WHIG INTERPRETATION OF HISTORY* 29 (1968) “The total result of this method [the method of Whig history] is to impose a certain form upon the whole historical story, and to produce a scheme of general history which is bound to converge beautifully upon the present” *Id.* at 12.

³⁰ 2 WILLIAM BLACKSTONE *COMMENTARIES* *2-3.

³¹ The most prominent case is *Entick v. Carrington*, 19 Howell’s St. Trials 1029 (1765).

³² The term “trespass” is normally employed to refer to possessory interests in real estate. However, the term is relevant to possession of one’s person. As Professor Dobbs has remarked, “The gist of the tort [of trespass] is intentional interference with rights of exclusive possession; no other harm is required.” DAN B. DOBBS, *THE LAW OF TORTS* 95-96 (2001). “Exclusive possession” can of course refer to rights over one’s person as well as rights over real estate.

terms of search and seizure—nontrespassory eavesdropping on conversations, for example, and nontrespassory “peeping” on people in their bedrooms.

Do the Fourth Amendment’s protections hinge on this trespass limitation? The Amendment’s text doesn’t definitively answer this question; indeed, it contains no reference to trespass at all. Rather, the Amendment’s organizing idea is the concept of personal security. The Amendment’s first, and most important, clause states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated”³³ In interpreting this clause, one might reason in terms of a narrow version of personal security, one that treats the trespass standard as implicit in the Amendment and that therefore identifies security with control over physical objects, in particular the objects essential to personal life (persons, houses, papers, and effects). Alternatively, one might argue that because the Amendment contains no reference to trespass, it is grounded in a broader version of personal security. On this account, the Amendment offers protection for the physical environment essential to personal life, but, one could continue, it is also concerned with background factors that can make someone feel vulnerable to others—that is, with nontrespassory surveillance such as constant scrutiny of one’s person or the interception of oral communications with friends. According to the narrow version of personal security, the Amendment offers only incidental privacy protection. According to the broad version, it treats privacy as an independent value, one that matters even when officials do not carry out a physical incursion on someone’s immediate possessions.

In the twentieth century, the Supreme Court has moved from an interpretation of the Amendment based on the narrow version to an interpretation based on the broader one.³⁴ As noted, the Amendment’s text provides no conclusive reason for

³³ U.S. CONST. amend. IV. For a comment on the importance of the concept of personal security in Fourth Amendment jurisprudence, see *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (“For those more extensive intrusions that significantly jeopardize the sense of security which is the paramount concern of Fourth Amendment liberties, I am of the view that more than self-restraint by law enforcement officials is required and at the least warrants should be necessary.”)

³⁴ The contrast is developed through an analysis of *Olmstead v. United States*, 277 U.S. 438 (1928), discussed *infra* in Part I.B, and *Katz v. United States*, 389 U.S. 347 (1967), discussed *infra* in Part I.C.

preferring one to the other. However, it's clear that the Amendment's common law sources are grounded in the narrow version³⁵—and clear as well that the early twentieth century Court, relying on this common law background, read the Amendment as if it constitutionalized the common law.³⁶ Thus anyone who argues, as I do, that the Amendment can properly be interpreted as a provision that protects the broad version of personal security must deal directly with both the Amendment's common law background and with the early twentieth century Court's reliance on that background. I turn to these issues next; then I advance an argument for reading the Amendment in light of the broad version of personal security.

B. THE EIGHTEENTH CENTURY SOURCES

Eighteenth century commentators on search and seizure appear never to have used the word "privacy" when writing about their subject. Their conceptual framework was grounded in a concern for property generally and the law of trespass in particular.³⁷ Thus, if we are to find a concern for privacy in eighteenth century commentaries on search and seizure, we must superimpose the categories mentioned earlier—informational privacy and privacy of the person—on judicial opinions and political oratory informed by a conceptual scheme grounded in property law. As I have already noted, such an undertaking is fraught with danger: the act of translating the past's conceptual scheme into one congenial to the present carries with it many opportunities for intellectual dishonesty. In this case, though, the danger can be avoided, for a strong argument can be advanced for saying that eighteenth century commentators were indeed deeply concerned with each type of privacy I have mentioned even though they did not use the rhetoric of privacy in formulating their claims. Two examples

³⁵ For a discussion of the Amendment's common law sources, see NELSON B. LASSON, *HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE CONSTITUTION OF THE UNITED STATES* 13-50 (1937).

³⁶ See *Olmstead v. United States*, 277 U.S. 438 (1928); see also *Carroll v. United States*, 267 U.S. 132, 149 (1925).

³⁷ See text and note 30 *supra* for an example of the high regard in which the concept of property was held by eighteenth century commentators. For an example of how eighteenth century common law judges analyzed search and seizure in terms of trespass, see *infra* notes 38-43 and accompanying text.

can be cited in support of this argument, one related to informational privacy, the other to privacy of the person.

Consider first a leading eighteenth century case, *Entick v. Carrington*,³⁸ that deals with what I have called informational privacy. *Entick* is one of the many cases that arose out of the Crown's efforts to suppress the anti-government pamphlets John Wilkes and his followers distributed during the early 1760s.. At issue in it was the lawfulness of government officials' seizure of Entick's personal papers.³⁹ At the beginning of their investigation, Lord Halifax's agents conducted a dragnet search, arresting more than twenty people on suspicion.⁴⁰ By the time they turned to Entick, they were able to identify him as a likely participant in Wilkes's efforts but were unable to specify which papers of his should be seized.⁴¹ In bringing an action for trespass, Entick alleged that the officials searching his home "broke open the boxes, chests, drawers, &c. of [all his] private papers," thereby discovering and making public his "secret affairs."⁴² Lord Camden drew on each of these points in finding for Entick, emphasizing in particular the private nature of the papers seized.⁴³

Camden grounded his approach in a Lockean premise about the ends of government, contending that "[t]he great end, for which men entered society was to secure their property."⁴⁴ The law of trespass, Camden continued, serves to protect property interests:

By the laws of England, every invasion of private property, be it ever so remote, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action [in trespass].... If he admits to the [trespass], he is bound to shew by way of justification that some positive law has empowered or excused him.⁴⁵

³⁸ 19 Howell's State Trials 1029 (1765).

³⁹ See LASSON, *supra* note 35, at 43 (describing the investigation of Wilkes and its implication for the development of the law of search and seizure); see also GEORGE RUDE, *WILKES AND LIBERTY* 17-37 (1962).

⁴⁰ TELFORD TAYLOR, *TWO STUDIES IN CONSTITUTIONAL INTERPRETATION* 30 (1969).

⁴¹ See LASSON, *supra* note 35, at 47.

⁴² *Entick*, 19 Howell's State Trials at 1066.

⁴³ See note 47 *infra* and accompanying text.

⁴⁴ *Entick*, 19 Howell's State Trials at 1066.

⁴⁵ *Id.*

Because Camden concluded no such justification was available to the officials who searched Entick's home, he held that they were liable in trespass.⁴⁶ Moreover, he also concluded that because the papers seized were personal ones, extra damages should be assessed against them. Camden remarked:

Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.⁴⁷

To the modern reader, the concept of privacy may seem to be the dominant one here. In fact, though, as close inspection of the passage makes clear, Camden carves out a special domain within property law for the seizure and inspection of those articles that contain a person's intimate thoughts. Although property damages are normally assessed in market terms, the market doesn't provide the baseline for Camden's reasoning as far as private papers are concerned. These are a person's *dearest* property, he remarks: their seizure and illegal inspection call for aggravated damages. With his use of the adjective "dearest," Camden unmistakably focused on the emotional rather than the market value of private papers. What matters, Camden maintained, isn't the price such papers will fetch on an open market but the role such papers play in sustaining personal life. One does no violence to Camden's *Entick* remarks, then, by saying that he evinced a profound respect for informational privacy when writing his opinion for the case. His categories of analysis were those of property law, but property provided an awkward proxy for the values he was actually championing.

Now consider remarks relevant to privacy of the person. A year after *Entick*, as repercussions of the government's investigation of Wilkes continued to be felt, William Pitt outlined his home-as-castle principle to the House of Commons:

The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may

⁴⁶ *Id.* at 1044.

⁴⁷ *Id.*

not enter; all his force dares not cross the threshold of the ruined tenement.⁴⁸

Security in the home, the principle Pitt champions in these remarks, promotes a number of different interests, not only privacy of the person but also informational privacy and control over property. Pitt's eloquent comments thus underscore the fact that eighteenth century commentators didn't view privacy as a separate consideration but instead reasoned in terms of a general interest that, in retrospect, can be said to include a number of specific ones, including privacy of the person. That Pitt expected this general interest to be protected by the law of trespass is made clear by his reference to "cross[ing] the threshold." But we fail to come to terms with the eighteenth century's ambiguous heritage if we focus simply on property rights. Pitt, like Camden, viewed personal property as having a special significance. His remarks, like Camden's in *Entick*, make it clear he was concerned not with the exchange value of property but with the way in which a certain type of property—the property essential to personal life—sustains independent existence. Indeed, Pitt went out of his way to emphasize this concern by focusing attention on the lowest common denominator of seclusion: the "ruined tenement" of the destitute man. This kind of home is significant not because of its commercial value but because it, just as much as a great mansion, offers the possibility of seclusion from the world. The point made about Camden thus also applies to Pitt, for here too property is a somewhat awkward proxy for the values really at stake in Pitt's remark. As the reference to the ruined tenement makes clear, what matters in Pitt's comments is not property's usual function—its exchange value. Instead, what matters is the way in which it offers security against the larger world.

C. TRESPASS AND THE EIGHTEENTH CENTURY HERITAGE: CHIEF JUSTICE TAFT'S OPINION FOR THE COURT IN *OLMSTEAD V. UNITED STATES*

Early twentieth century Supreme Court opinions interpreting the Fourth Amendment focused not on these general considerations but on the stubborn fact that *Entick* and its companion cases used the trespass standard in assessing

⁴⁸ LASSON, *supra* note 35, at 49-50.

search and seizure liability. To the early twentieth century Court, the Fourth Amendment was to be read as containing an implicit trespass condition.⁴⁹ The Court employed the following originalist chain of reasoning: (1) Government officials cannot violate the Fourth Amendment if they engage in neither a search nor a seizure; (2) Given eighteenth century case law, a search can be said to occur only if government officials commit trespass; (3) Therefore, trespass by a government official (or an agent of one) must occur if the Fourth Amendment is to come into play.⁵⁰

Here, then, is a formula that upholds the narrow version of personal security. Under the formula, the Amendment offers protection against the classic method of investigating crime—that is, it offers protection in settings where officials engage in physical incursions on a defendant's person or property. But the formula, of course, offers no protection against modern, nontrespassory methods of investigation. The first case in which the Supreme Court considered nontrespassory surveillance was *Olmstead v. United States*,⁵¹ decided in 1928. At issue in *Olmstead* was the admissibility of evidence secured through wiretaps of the defendants' phone conversations.⁵² During the course of their investigation of the *Olmstead* defendants, who were suspected of running a bootleg liquor ring, government officials placed taps on phone lines going into the defendants' homes and offices, thus avoiding any physical incursion on their property.⁵³ Writing for the Court, Chief Justice Taft treated this point as the critical fact of the case. The Fourth Amendment,

⁴⁹ See note 60 *infra* and accompanying text.

⁵⁰ The first—uncontroversial—premise follows from the text of the Fourth Amendment. The second—controversial and critical—premise is central to Chief Justice Taft's Fourth Amendment originalism. It follows from his remark, quoted *infra* in text at note 57, that the Fourth Amendment is to be interpreted “in light of what was deemed an unreasonable search and seizure at the time it was adopted” and also from the deep respect late nineteenth and early twentieth century members of the Court accorded *Entick v. Carrington*. See, e.g., the comments of Justice Bradley for the Court in *Boyd v. United States*, 116 U.S. 616, 626 (1886) (characterizing Lord Camden's opinion as a “monument of English freedom” and “the true and ultimate expression of constitutional law” on the subject of search and seizure). The third premise, which follows from the first two, is the central doctrine of *Olmstead v. United States*, 277 U.S. 438 (1928), discussed *infra* at notes 51-56 and accompanying text.

⁵¹ 277 U.S. 438 (1928).

⁵² *Id.* at 456-57.

⁵³ *Id.* at 457.

he had stated in an earlier case, “is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted.”⁵⁴ Given this originalist premise, Taft had no difficulty resolving the case. “There was no searching,” he concluded.⁵⁵ “There was no seizure,” he continued, for “[t]he evidence was secured by the use of the sense of hearing and that only.”⁵⁶

No search? Taft’s no-search claim may seem wildly implausible in light of the fact that officials had installed wiretaps as part of their effort to find out about the defendants’ activities. But Taft of course viewed the language of the Fourth Amendment through the prism of trespass law. The Amendment’s text, he pointed out, mentions only material objects: it offers protection, he argued, not for conversations but for *tangible objects that can be subject to physical incursion*—for an individual’s home, her person, papers, and effects.⁵⁷ The wrong it condemns, he maintained, is arbitrary government interference with an individual’s control over certain material objects.⁵⁸ Because no physical incursion on one of the protected objects had occurred in *Olmstead*, Taft concluded that the Fourth Amendment wasn’t implicated in the case.⁵⁹

D. THE COURT’S REPUDIATION OF THE TRESPASS STANDARD IN *KATZ V. UNITED STATES*

What rationale has the contemporary Court advanced for rejecting Taft’s conclusions in *Olmstead*? The answer to this is “none.” In overruling *Olmstead*, *Katz v. United States*,⁶⁰ decided in 1967, unmistakably established privacy as an independent variable in Fourth Amendment analysis. But neither Justice Stewart’s majority opinion for the Court nor any of the other concurring opinions in the case offered a sustained argument as to why Taft was mistaken—as to why, in other words, it is not

⁵⁴ *Carroll v. United States*, 267 U.S. 132, 149 (1925).

⁵⁵ 277 U.S. at 464.

⁵⁶ *Olmstead*, 277 U.S. at 464.

⁵⁷ *Id.* (“The 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 persons or *things* to be seized.”).

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ 389 U.S. 347 (1967).

necessary to interpret the Fourth Amendment as containing an implicit trespass requirement. This is just what I propose to do in the remainder of this section. I first summarize the Court's conclusions in *Katz*. Then I advance a justification, based on the broad conception of personal security, for its rejection of Taft's position.

1. *Katz and the Court's Recognition of Privacy as an Independent Fourth Amendment Variable*

At issue in *Katz* was the legality of an unusual, nontrespassory method of recording telephone conversations. Government agents hung a listening device on top of a phone booth they knew the defendant to use, and in doing so they made sure the device didn't touch the booth's ceiling.⁶¹ Their actions thus satisfied the trespass standard, but the *Katz* Court was not impressed by this point. The "premise that property interests control the right of the Government to search and seize has been discredited," Justice Stewart declared.⁶² The government's electronic surveillance, he stated, "violated the privacy upon which [Katz] justifiably relied."⁶³ As for the trespass standard, Stewart dismissed it in a single sentence: "The fact that the electronic device . . . employed to achieve that end . . . did not happen to penetrate the wall of the [phone] booth," he remarked, "can have no constitutional significance."⁶⁴

Stewart thus held that the Fourth Amendment protects privacy *independently* of its protection of interests in tangible objects. This is *Katz's* core conclusion, a conclusion that can be squared only with the broader version of personal security. This holding did not resolve the case, however, for the government further contended that even if its agents *did* interfere with a protected Fourth Amendment interest they didn't violate the Amendment. At the time its agents installed their listening device, the government maintained, they had probable cause to

⁶¹ *Id.* at 348.

⁶² *Id.* at 353 (quoting *Warden v. Hayden*, 387 U.S. 294, 304 (1967)). In speaking of property interests in *Katz*, Justice Stewart was concerned solely with the question of trespass. The material objects limitation for the Fourth Amendment established in *Olmstead* was not at issue in *Katz* because the Court had already rejected this limitation in *Silverman v. United States*, 365 U.S. 505 (1961). See *infra* note 124 and accompanying text.

⁶³ *Katz*, 389 U.S. at 353.

⁶⁴ *Id.*

believe that Katz was breaking the law, thus making their conduct reasonable (the government asserted) despite the absence of a warrant to overhear his conversations.⁶⁵ Stewart emphatically rejected this argument. Stressing that “searches conducted outside the judicial process . . . are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions,” he held that no further exception to the warrant requirement could be carved out for an electronic surveillance case such as the one at issue in *Katz*.⁶⁶ Stewart thus dealt with the two key issues relevant to Fourth Amendment privacy interests. First, and most importantly, he held that the Fourth Amendment independently protects these interests. And second, he held that when government officials interfere with privacy interests in circumstances such as those at stake in *Katz*, their conduct will be classified as unreasonable unless they have obtained a warrant beforehand.

2. *Vindicating the Court's Conclusions in Katz*

If Justice Stewart can be said to have advanced any justification at all for the *Katz* Court's interpretation of the Fourth Amendment, it is to be found in his remark that a narrower reading of the Constitution would “ignore the vital role that the public telephone has come to play in private communication.”⁶⁷ This statement, however, is at most a first step toward justification. Two options are worth considering in building on it. First, one might justify *Katz* by resorting to an analogy. Telephone conversations are functionally similar to letters, one could maintain, so it is appropriate to expand the Amendment's reach (think of the reference to papers in the Amendment's catalog of protected objects) from written to oral communication. Alternatively, one could contend that there is a general principle implicit in the Fourth Amendment—a principle that enjoins government respect for the environment of personal life—and then argue that *Katz* properly applied this principle to telephone conversations. As will become clear, this latter approach is more promising. The former, however, merits careful attention, in particular because it has informed

⁶⁵ See *id.* at 354.

⁶⁶ *Id.* at 357.

⁶⁷ *Id.* at 352.

Justice Scalia's recent opinions on Fourth Amendment privacy issues.

In resorting to analogy, Justice Scalia has cited the Amendment's catalog of protected objects and asked how far courts can go when applying the catalog to specific fact patterns.⁶⁸ The question is significant for its negative implication—for its implication that anything outside the scope of a reasonable analogy is *not* protected under the Amendment. For example, in construing the term "secure in their . . . houses," Justice Scalia has remarked that the Court was right to hold that a tenant who rents his home is protected.⁶⁹ The Court was also correct when it held that a grandson who lived in his grandmother's home is protected.⁷⁰ And it was even right to protect an overnight guest staying in a host's apartment.⁷¹ But protection of such guests, he has insisted, is the "absolute limit of what text and tradition permit."⁷² In particular, he has argued that the Court would go too far were it to extend the Amendment to a guest who is *not* staying overnight in a home.⁷³

Justification by analogy, it should be clear, requires fine and hardly convincing hair-splitting (overnight guest protected, shorter-term guest unprotected). But this is not its primary flaw. Rather, the major difficulty with this approach is that it casts doubt on the legitimacy of *Katz*. If reasoning by analogy is to be employed, then Taft's point about the material nature of the objects in the Amendment's catalog must be taken into account.⁷⁴ There are, of course, degrees of analogy, but analogy's appeal lies in the discipline it is supposed to impose on courts. Justice Scalia has made just this point in criticizing the Court's later use of *Katz*. In castigating these opinions as "subjective"⁷⁵ and "self-indulgent,"⁷⁶ he has implied that his

⁶⁸ For example, Justice Scalia has remarked that "[w]e [i.e., the Court] went to the absolute limit of what text and tradition permit in *Minnesota v. Olson* when we protected a mere overnight guest against an unreasonable search of his hosts' apartment." *Minnesota v. Carter*, 525 U.S. 83, 96-97 (1998) (Scalia, J., concurring).

⁶⁹ *Id.* at 97 (Scalia, J., concurring) (citing *Chapman v. United States*, 365 U.S. 610 (1961)).

⁷⁰ *See id.* (citing *Bumper v. North Carolina*, 391 U.S. 543 (1968)).

⁷¹ *See id.* at 96-97 (citing *Minnesota v. Olsen*, 495 U.S. 91 (1990)).

⁷² *Id.*

⁷³ *See id.* at 97. This was the issue at hand in *Carter*, 525 U.S. 83.

⁷⁴ *See Olmstead v. United States*, 277 U.S. 438, 464 (1928).

⁷⁵ *Kyllo v. United States*, 533 U.S. 27, 34 (2001). In this instance, Justice Scalia was speaking for the Court.

analogy-based approach places limits on the judiciary.⁷⁷ But if it is discipline Scalia wants, then surely the material-objects point circumscribes the reach of the Amendment—and surely, *Katz* must then be said to have been wrongly decided given the protection it offers oral communication when the Amendment's catalog is limited to material objects.

One could attempt to salvage Scalia's approach by relying on Taft's purer version of it.⁷⁸ But Taft's originalism is also incompatible with *Katz*, and it compounds difficulties by requiring hair-splitting inquiry into when a trespass occurs. The sounder analysis breaks entirely with this approach while still taking the text seriously. On this account, there is a principle implicit in the Fourth Amendment that ensures individuals a secure environment in which to conduct their personal lives. The catalog makes this clear. In speaking of "persons, houses, papers, and effects,"⁷⁹ the Amendment identifies the physical foundations of personhood, the objects an individual must control (including her person) to feel secure in everyday life. But the items are significant not simply as physical objects. The contents of the home and personal papers are, as Camden put it, their owner's *dearest* property.⁸⁰ They matter not because they are material objects but rather as props of personhood and as containers of information about an individual's life. Given this intangible value, it is wholly appropriate for courts to think not only about the physical environment of personhood but about its intangible attributes—and thus appropriate for courts to protect conversations as well as material objects.

This appeal to principle is consistent with the Fourth Amendment's. But is it consistent as well with its common law background—in particular with the common law's insistence on trespass as a prerequisite to search and seizure liability? This

⁷⁶ *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring). In this instance, Justice Scalia was speaking only for himself and Justice Thomas.

⁷⁷ One of the central themes of Justice Scalia's jurisprudence has been that judges must place limits on themselves in construing statutes and the Constitution. See generally Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175 (1989).

⁷⁸ Chief Justice Taft's interpretation of the Amendment limited its scope to material objects and also treated trespass as a prerequisite to liability. See *Olmstead*, 277 U.S. at 464. According to Taft, these limitations are required by an originalist account of the Amendment. *Id.* at 465.

⁷⁹ U.S. CONST. amend. IV.

⁸⁰ *Entick v. Carrington*, 19 Howell's State Trials 1209, 1066 (1765).

question is significant in light of Chief Justice Taft's unbending originalism. Justice Scalia, while also claiming to rely on "the original meaning of the Fourth Amendment,"⁸¹ has in fact diluted originalism by not insisting on either the material-objects limitation or the trespass rule.⁸² Taft's *Olmstead* opinion, on the other hand, relies on both. On Taft's account, the Fourth Amendment gives constitutional standing to *Entick*, thus making trespass and a material-objects limitation essential to Fourth Amendment analysis.⁸³

The best way to answer this *Olmstead*-inspired challenge is to note what is *not* contained in the Fourth Amendment's text. There is no reference in it to trespass, nor does the text contain a reference to the common law. The significance of this omission is underscored by an examination of the text of the Seventh Amendment.⁸⁴ That provision contains an explicit reference to the common law, preserving the right to a civil jury trial in common law suits where the value in controversy exceeds twenty dollars. Given this unequivocal, and detailed, reference, one can discern the different strategies at stake in the drafting of each Amendment. The authors of the Fourth Amendment appealed to a broad principle of personal security, a principle informed by the common law but that also transcends it through use of a term ("unreasonable searches and seizures") not typically employed by common law judges.

⁸¹ *Kyllo*, 553 U.S. at 39.

⁸² Justice Scalia's failure to insist on this is consistent with his general conception of originalism. Although he advocates an originalist interpretation of the Constitution, he has maintained that his approach must be qualified by respect for *stare decisis*. See Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849, 861 (1989). Justice Scalia can be understood to say, then, that he must follow *Katz* given its repudiation of *Olmstead*. But the question to ask of Justice Scalia in this context is what is left of Fourth Amendment originalism, other than a desire to limit the Amendment's protection, once a concession has been made about the material-objects and trespass limitations Chief Justice Taft established in *Olmstead*.

⁸³ See *Olmstead*, 277 U.S. at 464; see also *Carroll v. United States*, 267 U.S. 132, 149 (1925) (Chief Justice Taft remarked that the Fourth Amendment "is to be interpreted in light of what was deemed to be an unreasonable search and seizure when it was adopted.").

⁸⁴ The Seventh Amendment provides:

In suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise reexamined in any Court of the United States, than according to the rules of the common law.

The authors of the Seventh Amendment, on the other hand, referred to the common law and set an exact dollar amount for preserving the common law right to jury trial in civil cases. The Fourth Amendment is thus best read as a provision containing a principle of broad application. Taft's error was to read it as if it were analogous to the Seventh Amendment's mandate to fix forever the dollar amount of the civil trial jury right.

This focus on constitutional principle rather than a narrowly circumscribed common law rule has two advantages as far as interpretation of the Fourth Amendment is concerned. First, it captures the significance of Camden's and Pitt's remarks about the importance of security within personal life. On the account proposed here, the Amendment's catalog is suggestive rather than exhaustive. The catalog underscores the importance of the environment of personal life but doesn't purport to list all items essential to that environment. Although their positions differ in important respects, the Scalia and Taft accounts are similar in treating the catalog as exhaustive—as a list of discrete entities that defines the outer limits of Fourth Amendment privacy protection. Scalia's approach is marred by inconsistency: it casts doubt on *Katz's* legitimacy but avoids the originalist reading of the Amendment that distinguishes Taft's analysis. Taft's framework is internally consistent, but it rests on the problematic assertion that the purpose of the Fourth Amendment is to freeze the common law in its tracks.

Second, the interpretation proposed here makes it possible to consider the continuity between property and privacy interests. It is true of course that these are distinct categories, but it is also true they have some points in common. In particular, both are interests individuals assert for the purpose of *excluding* others—interests that set us off from others, emphasize our individuality, and weaken our ties to larger communities.⁸⁵ Moreover, there is an important sense in which the rhetoric of privacy is derived from that of property—thus the significance of references to *invasions* of privacy and *intrusions* on it, expressions that appeal to boundaries and the

⁸⁵ See, e.g., *Bond v. United States*, 529 U.S. 334, 341 (2000) (Breyer, J., dissenting) (“Privacy itself implies the exclusion of uninvited strangers, not just strangers who work for the Government.”); see also *Rakas v. Illinois*, 439 U.S. 128, 144 n.12 (1978) (“One of the main rights attaching to property is the right to exclude others, . . . and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.”)

language of trespass even though only metaphorical boundaries are at stake. As these points make clear, privacy rights have much in common with property rights because they originated in them and only gradually became distinct from them.⁸⁶ In the less mobile eighteenth century, property rights offered nearly complete protection for privacy interests.⁸⁷ In the twentieth century, as mobility of the person became increasingly important, privacy came to matter on its own—above all, people came to value it as a device for protecting information about themselves while circulating in society.⁸⁸ Had the Fourth Amendment been written in the narrow terms used for the Seventh, courts could not have properly invoked it to offer personal protection for this new, more mobile way of life. Given the Amendment's appeal to principle, though, it was entirely appropriate for the *Katz* Court to apply it to the changing circumstances of life.

E. FOURTH AMENDMENT PLURALISM

Implicit in the justification I have advanced for *Katz* is the claim that there are different ways in which officials can destabilize the environment of personal life—and so different interests protected by the Fourth Amendment. One is to interfere with someone's freedom of movement, to *seize her person*. Another is to interfere with her control over her personal property, to *seize her home, papers, and effects*. Yet another is to subject her to surveillance, to *search her person*,

⁸⁶ Indeed, the property framework continues to be employed when talking about informational privacy. For example, in *My Data, Mine to Keep Private*, N.Y. TIMES, Oct. 23, 2000, at A25, Linda Monk denounces efforts by members of Congress to discover information obtained by census workers on the basis of promises of confidentiality. Clearly, information provided to the census is the property of the United States government, not the property of the person who provided it. But when the information is provided on the basis of a pledge of confidentiality, one feels a strong sense of empathy with those who resort even to property-based arguments for limiting dissemination of their disclosures.

⁸⁷ As Justice Black noted, even in the eighteenth century the trespass doctrine did not provide complete privacy protection, because eavesdropping—that is, listening or observing without trespassing—remained possible. See *Katz v. United States*, 389 U.S. 347, 366 (1967) (Black, J., dissenting).

⁸⁸ Seminal cases such as *Olmstead* and *Katz* can be understood in light of this remark. Each raises questions about the Fourth Amendment's protection of informational privacy. The same value was of course at stake in *Entick* and in Fourth Amendment cases decided in the late nineteenth and early twentieth centuries, but it was not until *Olmstead* that the value of informational privacy was considered independently of other considerations.

home, papers, and effects. Each of the intrusions just mentioned interferes with a different interest in personal security—with a liberty interest (in freedom of movement), with a property interest (in exercising control over personal property), or with a privacy interest (in avoiding surveillance of one's person and of the sources of information about one's personal life). These three interests are of course complementary. But they are also analytically distinct—that is, each can be infringed without the others being affected. It is because this is so that one can speak of “Fourth Amendment pluralism.”

Standing in contrast with this is Fourth Amendment monism, a doctrine that views the Amendment as protecting directly only one interest. Taft, it is clear, was a proponent of Fourth Amendment monism. When he argued in *Olmstead* that the Fourth Amendment is triggered only by trespass, he maintained that the Amendment is concerned exclusively with the control people exercise over physical objects, whether those objects are their person or personal property.⁸⁹ Another kind of monism is possible, however. One can read *Katz* as having turned *Olmstead* on its head, as having interpreted the Fourth Amendment as a provision that offers direct protection only for privacy. This is surely as mistaken an approach to the Amendment as the one Taft employed in *Olmstead*, yet the post-*Katz* Court appeared at one time to be prepared to endorse it.⁹⁰ To understand the significance of privacy in Fourth Amendment jurisprudence, it is essential to see how the Court came close to endorsing privacy as the only value directly protected by the Fourth Amendment—and how it turned away from this, as it should have from the outset, by adopting a pluralistic interpretation of the Amendment.

The case that comes closest to *Olmstead* inversion is *Oliver v. United States*.⁹¹ At stake in *Oliver* was a claim that government agents violated a defendant's Fourth Amendment rights when they trespassed on his open fields, located far from his home, to seize marijuana he was growing.⁹² Writing for the Court, Justice Powell offered two rationales for holding that the Fourth Amendment wasn't implicated in the case. One was drawn from

⁸⁹ See 277 U.S. at 464.

⁹⁰ See *Oliver v. United States*, 466 U.S. 170 (1984).

⁹¹ *Id.*

⁹² *Id.* at 173.

its language. Open fields, Powell noted, aren't mentioned in the Amendment's catalog; therefore, he concluded, the Amendment offers no protection for government intrusion on them.⁹³

This first rationale stands as a primitive version of the Taft-Scalia reading of the Amendment's text. The account advanced by these justices does not limit protection to those objects *specifically* mentioned in the catalog;⁹⁴ rather, their accounts allow for the possibility of reasoning by analogy from the enumeration to other candidates for protection. But although Powell's specific enumeration analysis is wholly unpromising, the principle just outlined of protecting the environment of personal life provides a ready justification for *Oliver*. On this analysis, the Amendment's catalog provides a starting point, rather than an exhaustive list, of what matters in personal life. In treating it as a starting point, one can see that there certainly are objects besides those mentioned in the text that offer important support for the conduct of personal life. Absent special circumstances, though, one cannot argue that open fields provide a context for such conduct. Open fields are not like hotel rooms, which can temporarily become the focus of one's most intimate activities. Rather, they are more like factory workshops or open-air markets in that they are places where people work but do nothing essential to personal life.

It is possible, then, to produce a convincing rationale for the Court's conclusions in *Oliver*, one that Powell himself could have provided had he read the Amendment's inventory as suggestive in form rather than as an exhaustive list of specifically protected objects. Unfortunately, Powell not only failed to employ this interpretive strategy, he compounded his difficulties by advancing another justificatory argument, one that strongly implies that the Amendment's protection does not extend beyond privacy interests. "Since *Katz*," Powell remarked, "the touchstone of [Fourth] Amendment analysis has been the question whether a person has a 'constitutionally protected reasonable expectation of privacy.'"⁹⁵ Continuing, Powell stated

⁹³ See *id.* at 176-77.

⁹⁴ Chief Justice Taft, for instance, wrote the opinion for the Court in which provided that limited Fourth Amendment protection was provided moving vehicles. See *Carroll v. United States*, 267 U.S. 132, 155-56 (1925).

⁹⁵ *Oliver*, 466 U.S. at 177.

that the question posed in all Fourth Amendment cases is whether “a search infringes upon individual privacy.”⁹⁶

Here, then, is an example of Fourth Amendment monism almost as narrow as the monism espoused in *Olmstead*, although Taft’s monism relied on property and Powell’s on privacy.⁹⁷ Given Powell’s approach in *Oliver*, it is of course *property* interests that are incidentally protected under the Amendment.⁹⁸ According to *Oliver*, if government officials seize someone’s wallet or purse, the person suffering the seizure can speak of a cognizable Fourth Amendment interest only if officials violate a privacy interest associated with the object—by, say, opening the wallet or purse. Thus, if officials were merely to dispossess someone of, say, her purse and not inspect its contents, that person could not claim she had suffered an infringement of interests protected by the Amendment.

Oliver, however, did not establish the course the Court has ultimately followed in interpreting the Amendment. Fifteen days prior to *Oliver*, in *United States v. Jacobsen*,⁹⁹ the Court took its first step toward Fourth Amendment pluralism—its first step, in other words, towards an interpretive approach that emphasizes multiple, analytically distinct Fourth Amendment values. In reading the Fourth Amendment, Justice Stevens declared in his opinion for the Court in *Jacobsen*, it is essential to distinguish between two different kinds of government intrusions: searches and seizures. “A ‘search,’” Stevens wrote, “occurs when an expectation of privacy that society is prepared to consider as reasonable is infringed.”¹⁰⁰ A “‘seizure’ of property,” he continued, “occurs when there is some meaningful interference with an individual’s possessory interests in that property.”¹⁰¹ Finally, he remarked, a “‘seizure’ of a person” occurs when there is “meaningful interference, however brief, with an individual’s freedom of movement.”¹⁰²

In retrospect, it seems clear that other members of the *Jacobsen* majority did not grasp the significance of Justice

⁹⁶ *Id.* at 177-79.

⁹⁷ Contrast *Olmstead*, 277 U.S. at 464 with *Oliver*, 466 U.S. at 177.

⁹⁸ Thus, on Justice Powell’s account in *Oliver*, the Fourth Amendment offers no protection against trespass on open fields.

⁹⁹ 466 U.S. 109 (1984).

¹⁰⁰ *Id.* at 113.

¹⁰¹ *Id.*

¹⁰² *Id.* at 113 n.5.

Stevens's triadic division of the Fourth Amendment. When *Oliver* was decided fifteen days later, the majority and dissent groupings on the Court were the same, with one exception. The exception, of course, was Stevens, who moved from the majority in *Jacobsen* to the dissent in *Oliver*. In time, though, Stevens's insistence on pluralism came to dominate the Court's interpretation of the Amendment. The best evidence of this is to be found in the Court's conclusions in the 1992 case of *Soldal v. Cook County*.¹⁰³

At issue in *Soldal* was the Fourth Amendment's relevance to an eviction carried out in the presence of deputies of the Cook County Sheriff's Office.¹⁰⁴ Knowing that the management of a trailer park had initiated an eviction proceeding against the Soldals but that no order of eviction had been obtained, sheriff's deputies nonetheless assisted management employees as they disconnected the sewer and water pipes to the Soldals' trailer home, pulled the home free of its moorings, and towed it to the street.¹⁰⁵ The Soldals subsequently brought suit for money damages against the deputies, alleging that they had violated the Fourth Amendment.¹⁰⁶ The trial court granted summary judgment against them, and Judge Posner, speaking for the Seventh Circuit, upheld this ruling.¹⁰⁷ To Posner, the Court's treatment of the Fourth Amendment as a provision primarily concerned with privacy was the critical point.¹⁰⁸ No one had entered the Soldals' trailer, so their privacy hadn't been invaded, Posner stated.¹⁰⁹ Dispossession of one's home, he continued, affects only property interests, and these interests, he held, are protected under the Fourth Amendment only when government officials interfere with privacy interests.¹¹⁰

¹⁰³ 506 U.S. 56 (1992). See also, William C. Heffernan, *Property, Privacy, and the Fourth Amendment*, 60 BROOK. L. REV. 633 (1995) (for further analysis of *Soldal's* significance).

¹⁰⁴ 506 U.S. at 58.

¹⁰⁵ *Id.* at 58-59.

¹⁰⁶ *Id.* at 59.

¹⁰⁷ See 942 F.2d 1073 (7th Cir. 1990).

¹⁰⁸ Although recognizing that the Soldals' trailer had been seized, see *id.* at 1078 ("not every interference with exclusive dominion and control is a seizure in the relevant sense because not every such interference compromises privacy"). Posner held that the Soldals did not have a cognizable Fourth Amendment claim because their privacy had not been affected by the seizure. *Id.* at 1080 ("no interest protected by the Fourth Amendment is involved" in the case) (emphasis in original).

¹⁰⁹ *Id.* at 1077.

¹¹⁰ *Id.*

Reversing, Justice White, writing for a unanimous Supreme Court, treated Stevens's *Jacobsen* dicta as controlling and so took a pluralist approach to the Fourth Amendment.¹¹¹ *Katz*, White stated, had not "snuffed out the previously recognized protection for property under the Fourth Amendment."¹¹² Indeed, in drawing on both *Katz* and *Jacobsen*, White intimated that there is a general theme running throughout all Fourth Amendment cases—vindication of security expectations in everyday life against arbitrary action by government officials.¹¹³

Accepting Stevens's *Jacobsen* framework,¹¹⁴ White suggested that personal security is grounded in a set of analytically distinct but complementary expectations about government behavior.¹¹⁵ One of these expectations is that government officials will not arbitrarily interfere with one's privacy—thus *Katz*'s significance. Another is that officials will not arbitrarily interfere with one's personal property—thus *Soldal*. And yet another is that they will not arbitrarily interfere with one's personal mobility—thus the many Fourth Amendment cases dealing with freedom of movement. Taken together, these expectations point to a more general one: an expectation of security—of stability and relative invulnerability to destabilizing intrusions—into one's personal life. Table 1 provides an overview of the three interests, Justice Stevens's definition of each in *Jacobsen*, and the Supreme Court cases that treat them as analytically distinct.

Two features of this table require comment. First, it must be emphasized that the table is concerned with *interests*, not *rights*. Because the Amendment prohibits only *unreasonable* searches and seizures, many government operations that interfere with interests protected by the Amendment do so reasonably and so do not violate the right established by it. Given the interest/right distinction, courts can be said to follow

¹¹¹ See the lengthy citation to *Jacobsen* in *Soldal*, 506 U.S. at 62-63.

¹¹² *Id.* at 64.

¹¹³ See *id.* at 69 ("What matters is the intrusion on the people's security from governmental interference [I]t would be 'anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.'" (quoting *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 530 (1967))).

¹¹⁴ See *id.* at 63.

¹¹⁵ *Id.* White noted here that Posner's framework would undermine not only the Court's conclusion in *Jacobsen*, but also its holding in *United States v. Place*, 462 U.S. 696 (1983).

TABLE 1.
FOURTH AMENDMENT PLURALISM

Interests protected by the Amendment	Liberty	Property	Privacy
Jacobsen definitions at 466 U.S. 109, 113 (1984)	A "seizure" of a person [occurs] within the meaning of the Fourth Amendment [when there is] meaningful interference, however brief, with an individual's freedom of movement."	"A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."	"A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."
Scope of the interests	(a) freedom of movement (b) bodily integrity	(a) personalty (b) real estate used as personal dwelling	(a) privacy of the person (b) informational privacy
Supreme Court decisions establishing the independent status of the interest	<i>Tennessee v. Garner</i> , 471 U.S. 1 (1985) (police use of deadly force against fleeing felon analyzed as 'seizure of the person' within the meaning of the Fourth Amendment)	<i>Soldal v. Cook County</i> , 506 U.S. 56 (1992) (dispossession from trailer home with approval of sheriff but without court order of eviction analyzed in light of amendment's prohibition of unreasonable seizures of houses)	<i>Katz v. United States</i> , 389 U.S. 347 (1967) (warrantless electronic surveillance of conversation in telephone booth analyzed under Fourth Amendment)

a two-step inquiry when considering Fourth Amendment privacy claims. First, a court asks whether one or more of the interests it protects was infringed by a government operation. Only if the answer to this is positive does a court move to the second stage of inquiry—whether the government's operation was reasonable under the Amendment, with reasonableness determined in light of the level of suspicion that preceded the operation and the appropriateness of a warrant under the circumstances. The

concept of an interest is thus critical to determining whether the Fourth Amendment is *implicated at all* in a given operation. The concept of a right is critical to the *second* question that must be asked about an operation: whether the government's interference with an interest was reasonable.

The other feature of Table 1 that merits comment has to do with Justice Stevens's distinction between searches and seizures. Under Fourth Amendment monism, either the term "search" or the term "seizure" becomes dominant for judicial interpretation: "seizure" for *Olmstead*-type monism, "search" for its *Oliver* counterpart. Under pluralism, by contrast, each noun is given independent weight, with the Amendment's protection triggered even when only one type of intervention occurs (that is, under pluralism, there can be a search without a seizure, and a seizure without a search). Pluralism is superior to monism because it requires courts to recognize that a government operation can affect one kind of personal security without affecting others. Under Fourth Amendment pluralism, one can, when the facts so require, distinguish between pure privacy, pure property, and pure liberty wrongs. (The three cases mentioned in Table 1—*Katz*, *Soldal*, and *Garner*—provide an example of each.) On other occasions, one can build from this base and analyze government encounters with individuals in terms of the *interplay* of these interests—one can think, for example, about the interplay of liberty and privacy interests in stop and frisk or about the interplay of property and privacy interests when government officials enter a home. This flexible approach isolates the basic elements of personal security while allowing for the possibility that they will intersect in many settings.¹¹⁶ Our primary concern in the remainder of the article will be with privacy interests as they stand alone. However, we shall occasionally consider privacy interests in tandem with property and liberty interests.

III. DEVELOPING THE FORBEARANCE MODEL

To say that the Fourth Amendment offers independent protection for privacy interests is not, of course, to say what the

¹¹⁶ For a justification of the Fourth Amendment exclusionary rule through an analysis of the different interests that the Amendment protects, see William C. Heffernan, *Foreword: The Fourth Amendment Exclusionary Rule as a Constitutional Remedy*, 88 GEO. L. J. 799, 832-40 (2000).

term “privacy” means. Curiously, the modern Court has not addressed this question. It has commented frequently on what privacy is *not*.¹¹⁷ However, it has provided no definition of what privacy *is*. Nor has it given serious consideration to alternatives to a formal definition. For example, although post-*Katz* opinions have often invoked Harlan’s reasonable expectations test,¹¹⁸ none has systematically addressed the question of how to identify the expectations that make a privacy claim valid. The cost of this omission has been substantial, for the Court’s failure to reflect carefully on the nature of privacy has opened the way for the vigilance model that now dominates Fourth Amendment jurisprudence. In the first part of this Section, I outline the key features of the vigilance model. I then turn to its alternative, the forbearance model. In doing so, I offer an answer to the question neglected in *Katz* and subsequent cases—the question of what someone must demonstrate to establish a valid privacy claim under the Fourth Amendment.

A. POST-KATZ PRIVACY JURISPRUDENCE: AN UNREASONABLE EXPECTATION OF ETERNAL VIGILANCE

Three years before *Katz* was decided, Justice Stewart famously remarked, in *Jacobellis v. Ohio*,¹¹⁹ that he was unable to define pornography but that he knew it when he saw it.¹²⁰ Stewart’s approach to privacy was strikingly similar. As he had in *Jacobellis*, Stewart avoided a positive definition of the subject at hand when writing for the Court in *Katz*. But Stewart did at least comment on what privacy is not. The defendant/petitioner in *Katz v. United States* advanced a place-based definition of privacy; both parties disagreed not on whether places are critical to the identification of privacy interests but on whether a phone booth can be a private place.¹²¹ Stewart rejected their dispute as irrelevant. “What a person

¹¹⁷ See *infra* notes 122-23 and accompanying text. The Court has invoked this statement of what privacy is not in *California v. Greenwood*, 486 U.S. 35, 41 (1988); *California v. Ciraolo*, 476 U.S. 207, 213 (1986); and *United States v. Miller*, 425 U.S. 435, 442 (1976).

¹¹⁸ See *supra* note 2.

¹¹⁹ 378 U.S. 184 (1964).

¹²⁰ *Id.* at 197 (Stewart, J. concurring) (“I shall not today attempt further to define the kinds of material [at stake in obscenity cases]; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.”)

¹²¹ See 389 U.S. 347, 349-50 (1967).

knowingly exposes to the public," he stated, "even in his own home or office, is not a subject of Fourth Amendment protection."¹²² By contrast, he stated, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."¹²³

Stewart's juxtaposition of modal verbs reveals just how reluctant he was to provide positive guidance as to privacy claims. He commented forcefully on what is *not* protected under the Fourth Amendment ("what a person knowingly exposes to the public"). But he made no commitment as to what *is* protected, using the cautious locution "may be protected" when talking about what someone seeks to preserve as private. On Stewart's account, exposure is critical to understanding *non*privacy—critical, in other words, to identifying why a privacy claim must fail. But of course this sets the stage for questions about how to identify a valid claim. The most important of these turns Stewart's assertion inside out: is *non*exposure, one must ask, an identifying criterion of privacy? Other questions are closely related. For example, if nonexposure is critical, is this a necessary, or perhaps even a sufficient, condition for a valid claim? And what, in any event, is the relationship between nonexposure and concealment? The latter term suggests an affirmative effort to withhold something from others. The former, by contrast, suggests *either* an effort to withhold *or* acquiescence in a pre-existing condition of nonaccessibility. In speaking of exposure rather than concealment, Stewart appeared to endorse a broad conception of privacy, one that includes affirmative efforts to withhold but but extends beyond them (though Stewart's comments about privacy were, it must be emphasized, so casual one can hardly be certain about his intentions).

It is because Stewart and his colleagues in the *Katz* majority were conscious of the fact that they were inaugurating a new line of Fourth Amendment inquiry—they had, after all, had years of experience in applying *Olmstead*¹²⁴—that one would

¹²² *Id.* at 351.

¹²³ *Id.* at 351-52.

¹²⁴ Indeed, Stewart was the author of the Court's Solomonian opinion in *Silverman v. United States*, 365 U.S. 505 (1961), which overruled *sub silentio* one portion of *Olmstead* by holding that conversations are subject to Fourth Amendment protection. *Olmstead*, it will be recalled, held that that conversations lie outside the ambit of the Amendment because the Amendment's text is concerned solely with material objects.

have expected the Court's opinion in the case to address issues such as the ones just mentioned. As his comment on obscenity made clear, though, Stewart was perhaps the Warren Court justice least likely to be interested in offering positive guidance as to the meaning of a contested concept. It is possible, of course, that Stewart was opposed in principle to formal definition—possible, in other words, that he believed an attempt at formal definition is likely to have a worse effect on future decisions than no definition at all.

This is certainly a plausible point. The legal realist suspicion of formal definition¹²⁵ has a good deal of merit, and Stewart may well have been worried about harming the development of privacy law by advancing a definition of the term. There is, however, a middle ground between formalism and intuition, one that avoids abstract definition but does at least provide identifying criteria. What is missing from Stewart's *Katz* opinion is just this kind of mid-range analysis. Stewart, it should be noted, didn't even comment directly on what is obvious about all privacy claims: that an assessment of someone's claim about privacy must be assessed in light of what was known in the *ex ante*—it must be based, in other words, on what government officials know *prior to* an intrusion.¹²⁶

Olmstead v. United States, 277 U.S. 438 (1928). Stewart's *Silverman* opinion maintained that the case could be resolved without determining whether *Olmstead* should be overruled. See *Silverman*, 365 U.S. at 508-09. As noted, though, *Silverman* in fact did just that, a point Justice Black belatedly discovered in the electronic surveillance cases decided in the late 1960s. "I would not have agreed with the Court's opinion in *Silverman*," he remarked in dissent, "had I thought that the result depended on finding a violation of the Fourth Amendment or had I any inkling that the Court's general statements about the scope of the Amendment were intended to negate the clear holding in *Olmstead* . . ." *Berger v. New York*, 388 U.S. 41, 78-80 (1967). Extraordinarily careful reasoning had thus become necessary under the *Olmstead* regime, reasoning so finely developed its implications even escaped Justice Black, if only for awhile.

¹²⁵ "[I]f I am right, finding out what the judges *say* is but the beginning of your task. You will have to take what they say and compare it with what they *do*. You will have to see whether what they say matches with what they do. You will have to be distrustful of whether they themselves know (any better than other men) the ways of their own doing, and of whether they describe it accurately, even if they know it."

KARL LLEWELLYN, *THE BRAMBLE BUSH: ON OUR LAW AND ITS STUDY* 5 (7th prtg. 1981) (1930).

¹²⁶ Needless to say, the Court has commented on this on other occasions. See, e.g., its remarks in *Smith v. Ohio*, 494 U.S. 541, 543 (1990) (citations omitted):

Post-*Katz* opinions have tried to fill the gaps created by Stewart's opinion by drawing on Harlan's concurrence concerning privacy expectations.¹²⁷ In one sense, this move has been successful. By emphasizing the importance of society's understandings, the Harlan test undercuts any attempt at abstract definition and so requires justices to consider practices that prevail in everyday life. But there is another, more important sense in which this move has failed. To say that society's expectations matter when trying to identify privacy interests is simply to change the terms of discussion. An abstract definition won't do under Harlan's test; but some kind of identifying criterion is nonetheless needed to understand when society's understandings implicate privacy and when they do not. Moreover, the Harlan formula adds another factor to the equation, for it requires courts to explain when, and why, an expectation turns into a constitutionally valid interest. Like Stewart, Harlan didn't consider foundational issues such as these. His test is far from self-executing, yet the Court has drawn on it as if it resolves the problem of guidance left open in Stewart's opinion.

The results, as numerous commentators have agreed,¹²⁸ have been deplorable—a kind of Khadi¹²⁹-style justice for Fourth Amendment privacy interests rather than a reasoned analysis of them. We can best understand how things have gone wrong by examining the Court's use of Harlan's test in post-*Katz* cases. This test has subjective and objective prongs. First, Harlan

"[U]stify[ing] the arrest by the search and at the same time . . . the search by the arrest," just "will not do." As we have had occasion in the past to observe, "[i]t is axiomatic that an incident search may not precede an arrest and serve as part of its justification."

For comments on the implications of this point for the Fourth Amendment exclusionary rule, see Heffernan, *supra* note 116, at 838-40.

¹²⁷ See *supra* note 2.

¹²⁸ See, e.g., Laurence A. Benner, *Diminishing Expectations of Privacy in the Rehnquist Court*, 22 J. MARSHALL L. REV. 825, 826 (1989); Brian Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 594 (1989); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1087-88 (1987).

¹²⁹ For Weber's discussion of Khadi justice, see MAX WEBER, *ON LAW AND ECONOMY AND SOCIETY*, 213 (Edward Shils trans., Max Rheinstein ed. 1954). Professor Rheinstein helpfully notes that Weber uses the term "Khadi justice" "to describe the administration of justice which is oriented not at fixed rules of a formally rational law but at the ethical, religious, political, or otherwise expediential postulates of a substantively rational law." *Id.* at 213 n.48.

remarked, a person must “have exhibited an actual (subjective) expectation of privacy”;¹³⁰ second, he continued, the expectation must “be one that society is prepared to recognize as ‘reasonable.’”¹³¹ Most post-*Katz* opinions treat *each* condition as necessary for establishing a valid privacy claim, though at least one majority opinion has conceded that in some instances the first, subjective prong provides “an inadequate index of Fourth Amendment protection.”¹³² This point is surely valid. If the government were to announce that henceforth all homes will be subject to warrantless inspection (to use the Court’s example¹³³), then, assuming the first prong remains essential, Fourth Amendment privacy protection would be reduced to the extent that the government, through its own efforts, was able to reduce subjective expectations. It is perhaps for this reason that the Court has not treated the first prong as a key element of its post-*Katz* jurisprudence.¹³⁴ Indeed, the first prong of the expectations test is of such marginal importance in post-*Katz* decisions that I shall return to it on only a few occasions in the remainder of the Article.

Rather, it is the second, objective-expectations prong of the Harlan test that has guided modern privacy jurisprudence. As noted, Harlan viewed an expectation of privacy as objectively valid only if it is one “society is prepared to recognize as

¹³⁰ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

¹³¹ *Id.* Morgan Cloud has criticized this first prong as “perhaps the most nonsensical premise in Fourth Amendment law.” Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 250 (1993). This seems far-fetched. Privacy can properly be classified as a claim-right—that is, as a right to something that someone must secure for herself. Given its status as a claim-right, it is surely plausible to say that a person must take a step to secure the condition of privacy for herself. The further question to ask, of course, is whether a demanding standard is established for asserting the claim.

¹³² *See Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979).

¹³³ *See id.*

¹³⁴ In practice, the Court has settled for relatively modest steps as a way of establishing a subjective expectation of privacy. *See, e.g., Bond v. United States*, 529 U.S. 334, 338 (2000) (Passenger on bus exhibited a subjective expectation of privacy “by using an opaque bag and placing that bag directly above his seat.”). Even in cases where the Court has held that someone lacked an objectively reasonable expectation of privacy, it has been willing to concede that relatively modest efforts may establish a subjective expectation. *See, e.g., California v. Greenwood*, 486 U.S. 35, 39 (1988) (Use of opaque bags for garbage may well indicate that someone does “not expect that the contents of their garbage bags would become known to the police or other members of the public.”).

'reasonable.'"¹³⁵ Harlan's approach thus requires courts to examine society's practices—and so to look beyond the Constitution's text—in trying to discern privacy norms. *Olmstead*-based inquiry had also required inquiry beyond the Constitution. Under *Olmstead*, however, the Court had considered common law property rules when determining the Fourth Amendment's scope. Harlan's reasonable expectations test made social norms the focus of attention. In doing so, it quite properly changed the terms of discussion from arcane rules of property law to generally held assumptions about the prerequisites of personal security.

But how are courts to identify privacy norms? It is here that the Court has failed to provide guidance. Harlan's test contains only a suggestion for reorienting Fourth Amendment jurisprudence; it does not, however, contain a criterion for singling out privacy norms. Unfortunately, no post-*Katz* opinion has taken up the challenge. Instead, modern privacy jurisprudence has employed the following, grim chain of reasoning: (1) Only objectively reasonable privacy expectations are protected under the Fourth Amendment;¹³⁶ (2) There is no need to provide a criterion for identifying these expectations because it is clear that whenever someone knowingly exposes an object or information to the public, that person cannot claim to have an objectively reasonable privacy expectation;¹³⁷ and (3) The terms "knowingly," "exposed," and "public" should be interpreted as broadly as possible. Whenever there is uncertainty about whether exposure was knowing or inadvertent, it should be classified as "knowing."¹³⁸ Even a fleeting opportunity to view an object should be interpreted as "exposure."¹³⁹ Finally, the term "public" should be defined

¹³⁵ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

¹³⁶ As Harlan stated, these are expectations "that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361.

¹³⁷ See *Katz v. United States*, 389 U.S. 347, 351 (1967). When a person exposes something to the public, the Court reasons, he *cannot* have an objective reasonable privacy expectation in it. See *id.*

¹³⁸ See, e.g., *California v. Ciraolo*, 476 U.S. 207 (1986). In *Ciraolo*, the defendant had constructed a six-foot outer fence and ten-foot inner one to shield his backyard from observation by passersby. *Id.* at 209. The *Ciraolo* Court, citing *Katz's* knowing exposure standard, concluded that the defendant had knowingly exposed his yard to the public. *Id.* at 213.

¹³⁹ See, e.g., *Florida v. Riley*, 488 U.S. 445 (1989). In *Riley*, the defendant had enclosed placed thick shrubbery around his greenhouse and covered it with corrugated roofing panels, some translucent, some opaque. *Id.* at 448. To examine

expansively to include not simply randomly encountered strangers but also providers of services indispensable to life in modern society.¹⁴⁰ It is by considering the significance of these latter, highly controversial claims that one grasps the significance of the vigilance model. Later in this section, I propose a corrective solution to the Court's approach. At present, however, it is important to concentrate on what the vigilance model has meant in practice.

1. The Anxious Quest for Privacy

On the Court's account, even the slightest exposure of an item to the public can defeat a privacy claim. *California v. Greenwood*, the case concerned with the possibility of privacy interests in garbage, provides a chilling illustration of this point.¹⁴¹ Placing garbage in an opaque bag and leaving it on the street on collection day would appear to meet the requirement of making sure it is not exposed to the public. In holding otherwise, the Court noted that "scavengers and snoops" often rummage through garbage before it is picked up.¹⁴² Using the behavior of "snoops" as its baseline for thinking about privacy, the Court concluded that the *Greenwood* defendants had indeed exposed their garbage to the public and could therefore not claim any privacy interest in that garbage.¹⁴³ How can someone ensure privacy in his garbage, then? Will shredding followed by random distribution of the shredded pieces to several dumps suffice? In applying *Katz's* exposure-to-the-public standard, a lower court held that even these steps were inadequate.¹⁴⁴ Perhaps only an incinerator system—for which permits are hard to obtain—will do.

the contents of the greenhouse, the pilot of a police helicopter had to circle it twice from a height of 400 feet. *Id.* Although the opportunity to look into the greenhouse was, of necessity, a fleeting one from airspace, five members of the Court nonetheless concluded that the defendant did not have a privacy interest in its contents. *Id.*

¹⁴⁰ See *Miller v. United States*, 425 U.S. 435 (1976) (no privacy interest in financial records despite the fact that the only members of the public to whom they have been exposed are bank employees); see also *Smith v. Maryland*, 442 U.S. 735 (1979) (no privacy interest in telephone numbers dialed from the home).

¹⁴¹ 486 U.S. 35 (1988).

¹⁴² See *id.* at 40 n.4.

¹⁴³ *Id.* at 41.

¹⁴⁴ See *United States v. Scott*, 975 F.2d 927 (1st Cir. 1992) (Acting without a warrant, IRS agents seized Scott's garbage, combed through it, and pieced together 5/32-inch shredded strips. They used the information provided by these strips to obtain a warrant to secure additional evidence against Scott.).

2. *The Problem of Exposure to Third Party Facilitators*

What if the only member of the public to whom an object has been exposed is a third party facilitator? Settings involving this kind of limited, special-purpose revelation abound in everyday life. For example, people who take steps to ensure that the public does not have access to their financial records nonetheless routinely rely on bank officials to process their checks and deposits. Similarly, even when people take steps to make sure strangers are unaware of the pattern of phone numbers they dial, they are not troubled by the fact that these patterns are discoverable through a search of the phone company's computers. For the Court, these facilitators are members of the public to whom people have voluntarily exposed information about their personal lives.¹⁴⁵

3. *Calculating What a Member of the Public Might Discover*

What if it is clear that an effort has been made to avoid an object's exposure and the only person who discovers the object is a government official who has expended great effort to make the discovery? The Court's sole concern on such occasions is with what a member of the public who is acting lawfully *might have* discovered. Thus in the Court's most recent aerial surveillance case, it did not matter that the only evidence about what was in a person's backyard came from a government helicopter pilot specifically assigned to use his craft to find out about the contents of that very yard.¹⁴⁶ The Court was not swayed by the presence of a "DO NOT ENTER" sign on the perimeter of the backyard. Nor did it matter that trees and shrubs made the backyard invisible from the street and that corrugated roofing made it difficult to inspect the yard's contents from the air.¹⁴⁷ What did matter to the Court was that a member of the public hovering over the backyard in a helicopter *could have* peered through an open section where roofing had not been installed.¹⁴⁸ On this account, it is the

¹⁴⁵ See *Miller* 425 U.S. 435 (bank records); see also *Smith*, 442 U.S. 735 (telephone numbers).

¹⁴⁶ See *Florida v. Riley*, 488 U.S. 445, 448 (1989).

¹⁴⁷ For the existence of the "DO NOT ENTER" sign, see *id.*

¹⁴⁸ *Id.* at 451 ("Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer [who piloted the helicopter in the case] did no more.")

“snoop”, a term the Court favorably invoked in *California v. Greenwood*,¹⁴⁹ who defines privacy expectations.¹⁵⁰ To be more precise, it is the snoop aided by the human and mechanical resources of modern police departments.¹⁵¹

Anyone encountering these summaries of post-*Katz* opinions would say that the Court has turned privacy on its head. Society’s expectation of privacy isn’t eternal vigilance against outsiders, it’s the reverse—an expectation that outsiders will exercise forbearance with respect to personal matters, thereby creating a context of security for the conduct of everyday life.¹⁵² That the Court has gone awry in its post-*Katz* opinions seems clear enough. But it is not enough to charge the Court with error; one must also explain *why* it is mistaken. To do so, two steps must be taken. First, we must reconsider the Harlan test from the ground up. We must think about the relationship between expectations and interests and so come to terms with the social basis of the test. Second, in working from this foundation, we must examine the different methods courts can employ to identify privacy interests. With these tasks accomplished, we will be able to see why the Harlan test, properly understood, requires adoption of the forbearance model of privacy protection.

B. THE HARLAN TEST I: FROM SOCIAL EXPECTATIONS TO LEGALLY ENFORCEABLE PRIVACY INTERESTS

One must question terminology when subjecting the Harlan test to careful scrutiny. Why, one wants to know, did Harlan employ the term “expectations” rather than “interests” when talking about privacy?¹⁵³ Had Harlan spoken directly about privacy *interests*, his reference would have been unmistakably normative, for in speaking of an interest, one suggests that an individual has a good reason (though not necessarily a decisive one) to engage in a certain kind of activity. The term “expectation,” on the other hand, has a more ambiguous meaning. First, it can be used in an exclusively predictive sense,

¹⁴⁹ 486 U.S. 35 (1988).

¹⁵⁰ See *supra* notes 20-21.

¹⁵¹ *Id.*

¹⁵² See *infra* Part II.D for further development of this point.

¹⁵³ Harlan’s *Katz* concurrence is framed exclusively in terms of “expectations.” See 389 U.S. 347, 360-62 (1967).

as in “I expect the Yankees to win today.” In this version of “expectation,” there is no suggestion of an obligation; if, for example, the Yankees fail to win on the day in question, one wouldn’t say that they disregarded an obligation to do so.

But second, there is another version of “expectation,” one whose meaning is simultaneously predictive and normative. Think, for example, about the word’s use in the sentence “I expect people arriving later at the movie theater to line up behind me in the queue.” Here, the word has a predictive quality—in uttering the sentence, a person indicates she considers it likely that people arriving later for the movie will honor queuing conventions. But the term also has a normative meaning: in this instance, it indicates a belief that individuals arriving later *ought to* accept a less advantageous position in the queue. The fact that people occasionally flout queuing conventions (thus upsetting predictive expectations) would not disturb someone’s normative judgment that these conventions ought to be honored. A person, when confronted with another’s violation of queuing rules, would defend them as being fundamentally sound. These conventions fairly allocate spaces for public events and so should be honored.

Harlan, it seems reasonable to suppose, had this more complex version of “expectation” in mind when he spoke of privacy.¹⁵⁴ Because the system of privacy operates through conventions, the notion of a privacy expectation necessarily involves a prediction about how people will behave. But because people believe others *ought to* honor their privacy expectations, there is an inescapably normative element to Harlan’s use of the term.¹⁵⁵ Harlan did, of course, distinguish between subjective and objective privacy expectations—between expectations people believe to be valid (the subjective “ought”) and those “expectations of privacy society is prepared to recognize as reasonable” (the objective “ought”).¹⁵⁶ The former

¹⁵⁴ For example, Harlan’s statement that “a man’s home is, for most purposes, a place where he expects privacy,” suggests not simply an empirically valid belief that people will respect residential seclusion but also a normative commitment to the value of such seclusion. See 389 U.S. at 361.

¹⁵⁵ It is for this reason that Harlan endorsed Stewart’s remark in the majority opinion by saying that “[t]he critical fact in this case is that ‘[o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume’ that his conversation is not being intercepted.” *Id.* (emphasis added).

¹⁵⁶ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

category has to do with someone's conviction, which may or may not be justified, that she has a good reason to be accorded something she desires. The latter category has to do with interests—that is, with valid claims on others, claims not necessarily entitled to absolute weight (they might, after all, be trumped by other interests), but claims that merit respect from others. The challenge in interpreting Harlan's test is to identify the circumstances in which certain, though not all, subjective privacy expectations are transmuted into interests entitled to legal protection.

The obvious and correct answer is that under Harlan's test, society's privacy conventions provide the identifying criterion for the interests entitled to legal protection. But while correct, this simply reminds us of the premise underlying Harlan's test.¹⁵⁷ It does not tell us why this premise should be adopted. In particular, it does not tell us why courts ought to honor social conventions when considering privacy interests. To tackle this more difficult issue, we must examine the nature of privacy conventions and consider how they can generate interests entitled to constitutional protection. In speaking of privacy, we are concerned with a special kind of convention. Some conventions originate in, or at least are deeply dependent on, government sponsorship (think, for example, about patriotism). Others, however, have origins that can be traced neither to government sponsorship nor to formal agreement among laypersons. These conventions, we can say, are spontaneously generated.¹⁵⁸

The system of privacy is an instance of this, though hardly the only such instance. For another case in point, consider queuing conventions, which have already been discussed. No government directive established queuing as a formula for allocating spaces at public events. Nor does there seem to have been a point in time when people deliberated about space-

¹⁵⁷ This is not to say, of course, that it is easy to identify privacy conventions. For an example of an ad hoc, unpromising way to identify them, see *infra* note 165.

¹⁵⁸ Friedrich Hayek is the leading theorist of spontaneous order within society. In commenting on modern society, he has remarked: "It is because it was not dependent on organization but grew up as a spontaneous order that the structure of modern society has attained the degree of complexity which it possesses and which far exceeds any that could have been achieved by deliberate organization." FRIEDRICH HAYEK, *LAW, LEGISLATION AND LIBERTY: RULES AND ORDER* 50 (1973). Hayek can properly be faulted for having overgeneralized on this point, but his argument is certainly helpful in thinking about the development of privacy conventions.

allocation issues and decided it would be best to allocate them through queuing. The term "spontaneously generated," while perhaps not wholly satisfactory as a label, does at least remind us that queuing conventions, like those of privacy, have emerged through a process of social ordering that has received tacit consent without having been the product of deliberate decision-making. "Spontaneously generated" is thus certainly to be preferred to "socially constructed." The latter term suggests deliberate planning, but what characterizes privacy and other social conventions is the *absence* of such planning. Privacy conventions emerged through social processes that did not involve careful reflection but that nonetheless won the consent of the great majority of the population.¹⁵⁹

If we continue to focus on queuing for a moment, we can begin to understand how an interest that merits legal protection can emerge from spontaneously generated social norms. As we have seen, the statement "I expect the people arriving after me at the movie theater to line up behind me in the queue" expresses a prediction *and* a statement of normative belief. Does the subjective belief become legitimate—is it transmuted from a putative to a valid interest—merely because the predictive statement is likely to be true? The answer to this is clearly no—otherwise, any statement about the conventions people are likely to honor would also become a statement about those they ought to honor.

Rather, what is needed is the concept of a legitimate reliance interest—the notion, in other words, that someone's reliance on a convention is in fact justified. In the case of queuing, one would say that the convention of allocating places is sufficiently ingrained in current social relations and sufficiently fair that people are entitled to rely on it in settings where it is currently followed. The concept of legitimate reliance thus provides the bridge to move from expectations to (justified) interests. One cannot derive the statement that it is legitimate to expect people to honor queuing conventions simply from the fact that people tend to do so. At the same time, though, it is clear that queuing conventions provide one of the conditions necessary for the proposition that subjective queuing expectations merit respect, for it is only when

¹⁵⁹ For a discussion of privacy in colonial America, see DAVID H. FLAHERTY, *PRIVACY IN COLONIAL NEW ENGLAND* (1972).

conventions are widely followed that people can properly claim to rely on them in their behavior.

There are two reasons why the concept of a legitimate reliance interest is also critical to the analysis of privacy. First, it seems reasonable to suppose that Harlan's *Katz* concurrence was prompted by Stewart's statement in his opinion for the Court that the government's eavesdropping "violated the privacy upon which [Katz] justifiably relied while using the telephone booth"¹⁶⁰ Second, and more generally, we can say that Harlan's appeal to expectations provides a way to understand how social practices whose provenance lies outside government directives can give rise to interests meriting judicial protection.¹⁶¹ The system of privacy hinges on a series of

¹⁶⁰ *Katz v. United States*, 389 U.S. 351, 353 (1967).

¹⁶¹ *See id.* The *Katz* concurrence is adoptionist in nature: it treats privacy norms as developing independently of, and as properly adopted by, the law. Justice Harlan later came to doubt the wisdom of his expectations test. *See United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). In particular, he doubted that expectations of privacy emerge primarily from social processes that develop independently of legal norms. *See id.* "Our expectations, and the risks we assume," he suggested, "are in large part reflections of laws that translate into rules the customs and values of the past and present." *Id.* In contrast to Harlan's adoptionist approach in *Katz*, his account in *White* emphasizes the interaction of law and privacy norms. *See id.* Harlan's interactionist approach in *White* is certainly plausible for some kinds of social norms; norms about property, for example, have been shaped by statutory and common law rules, and these rules in turn can be said to have been formulated in light of widely held attitudes about property. For a discussion of the subtle interaction in early English property law between social norms and formal pronouncements of authorities, see 2 William Holdsworth, *A History of English Law* 54-87 (4th ed. 1936).] But privacy is different.

Legal rules about property are as old as the common law itself (and are also found in the legal systems of ancient societies). *See id.* Rules protecting privacy, on the other hand, developed only in the nineteenth century—and at first were placed under headings such as implied contract and implied trust. *See Samuel D. Warren and Louis D. Brandeis, The Right to Privacy*, 4 HARV. L. REV. 193, 209-10 (1890). Indeed, it was the celebrated Warren-Brandeis article that stimulated judges invoke privacy as a common law tort category. According to Harry Kalven, what Warren and Brandeis wrote was perhaps "the most influential law review article of all." Harry Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?* 31 LAW & CONTEMP. PROBS. 326, 327 (1966). In the case of privacy, then, Harlan's adoptionist approach in *Katz* is more sound. The privacy conventions judges attempt to discover under the expectations approach actually did develop in large measure without the influence of legal rules.

Indeed, the alternative Harlan proposed in his *White* dissent to that which he proposed in *Katz* illustrates the difficulty of trying to dispense with adoptionism when thinking about legal norms of privacy. *See White*, 401 U.S. at 786 (Harlan, J., dissenting). Harlan remarked: "Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them on society." *Id.*

convention-based expectations as to how people will behave: expectations about how they will respond to closed doors, sealed envelopes, markings that something is confidential, and so on. These are *reasonable* expectations in that they constitute a widely-acknowledged basis for social interaction. Moreover, given the Fourth Amendment's text, they are also *legitimate* expectations, for failure to honor them undermines a person's sense of security in everyday life. Thus courts must seek to understand the conventions underlying the system of privacy and seek to uphold these conventions in order to protect Fourth Amendment interests.

C. THE HARLAN TEST II: METHODS OF IDENTIFYING PRIVACY INTERESTS

Here, then, is the first step that needs to be taken in correcting the Court's vigilance model. Privacy conventions contribute to each person's sense of security in the conduct of their everyday life. They assuage anxiety rather than exacerbate it. The Court has indeed turned privacy upside down through its emphasis on vigilance, for when privacy is at stake, people expect (in both a normative and empirical sense) others to exercise restraint; they do not expect them to act as snoops. These general points are insufficient by themselves, however, to help courts answer the intensely practical question of how to identify privacy interests.

One way to approach this question—perhaps the one Stewart would have followed given his “I know it when I see it” approach to the definition of pornography¹⁶²—is to follow the common law's case-by-case method of analysis.¹⁶³ Such analysis

Continuing, he stated that judges should “assess[] the nature of a particular practice and the likely extent of its impact on the individual's sense of security [by] balanc[ing the practice] against the utility of the conduct as a technique of law enforcement.” *Id.* Apart from the difficulties that accompany any attempt to balance incommensurable goods, this test is flawed because it necessarily appeals to privacy conventions—to “objectively reasonable expectations”—through its invocation of the term “sense of security.” See *White*, 401 U.S. at 786. For what is it that creates a sense of security with respect to one kind of practice but not another if not social conventions? Judges can avoid arbitrariness in their assessment of personal security only by considering social conventions as regarding what generates security and what does not. On close inspection, it turns out that Harlan's theory in *White* actually hinges on the judicial assessment of social convention he advocated in *Katz*.

¹⁶² See *supra* notes 119-20 and accompanying text.

¹⁶³ See KARL N. LLEWELLYN, *THE COMMON LAW TRADITION: DECIDING APPEALS* (1960).

considers privacy claims *seriatim* (accepting some, rejecting others), and eventually generalizing on the claims held to be valid.¹⁶⁴ This common law method is not without its merits. To understand how privacy conventions operate, one could argue, it is essential to be sensitive to the subtle nuances of specific settings—to think in terms of thick bundles of facts rather than thin analytic principles. In developing this argument, one could contend that the key to privacy analysis is to be found in the factually rich details of a given situation—in whether someone closed a door all the way, in whether someone spoke in a loud or soft voice, and so on.

Because no one on the Court has even discussed the problem of how to identify privacy conventions, one can't say that its members have actually *chosen* this situation-specific approach. At most, one can say that the justices have fallen into the habit of reasoning in this way.¹⁶⁵ In stepping back from it, though, one can see that its weaknesses are greater than its strengths. Consider first the problem of technological change. When a technological innovation is at issue, it simply doesn't make sense to reason from a situation-specific premise about how society's expectations are likely to be aware of the innovation; fewer still are likely to have reached a conclusion about its implications for privacy. Courts thus have to search for patterns in current practices: they have to develop concepts that

¹⁶⁴ For a general discussion of this method, see *id.* at 121–57.

¹⁶⁵ See argument in *Bond v. United States*, 529 U.S. 334 (2000), which provides a good example of the ad hoc form of inquiry that now prevails in privacy cases. At stake in *Bond* was the lawfulness of a drug agent's handling of soft luggage by squeezing it as he walked down the aisle of a bus loaded with passengers. *Id.* at 335. Rather than reason from a general principle relevant to the case, the Court's members argued on the basis of their own experiences about expectations of privacy concerning luggage-squeezing. Linda Greenhouse, *Police Under a Microscope in 2 Supreme Court Cases*, N.Y. TIMES, Mar. 1, 2000, at A17. Justice Breyer stated that when he traveled by plane, people often shoved around his carry-on luggage after he had placed in an overhead bin. *Id.* Responding to Breyer's point, other justices insisted on a distinction between pushing around luggage and squeezing it to determine its contents. *Id.* Justice Ginsburg remarked, "people don't take it [i.e., a piece of soft luggage placed in an overhead storage bin] and feel it." *Id.* Justice Kennedy agreed, stating that he didn't think a fellow passenger would be entitled "to start squeezing my luggage to see what's in it." *Id.* For further discussion of *Bond*, see Linda Greenhouse, *Police Under a Microscope in 2 Supreme Court Cases*, N.Y. TIMES, Mar. 1, 2000, at A17. Oral argument in *Bond* thus began to seem like a dormitory bull-session, with the justices drawing on personal experience to develop what Justice Breyer, in a sarcastic dissent to the Court's opinion in the case, called "a constitutional jurisprudence of 'squeezes.'" *Bond*, 529 U.S. at 342.

capture the significance of these patterns and then apply these concepts to the innovation at issue.

Moreover, even when an innovation is not at issue, it is best to begin by considering general patterns. Situation-specific decision-making tends to produce biased results. If a court makes no effort to discern the patterns underlying privacy conventions, then that court will have little difficulty slanting its conclusions to fit a preconceived ideological position. This point is clearly relevant to a diagnosis of the problems with post-*Katz* jurisprudence, for the Supreme Court's favorable view of the "war on drugs" appears to have overwhelmed it in its search for society's privacy expectations.¹⁶⁶ Needless to say, there is a danger lurking in the opposite approach. To begin by identifying thin patterns underlying society's privacy expectations and to give them ever-increasing thickness as one comes to terms with the facts of a specific situation is to run a different risk: it is to risk missing the judgments of degree that inform conclusions about privacy claims. This risk is worth taking, however, given the even greater risk associated with the alternative. In what follows, I thus analyze the general structure of privacy conventions. In particular, I concentrate on privacy's function in protecting personal vulnerability.

¹⁶⁶ See, e.g., *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 636 (1989) (Marshall, J., dissenting) ("The [Court's] acceptance of dragnet blood and urine testing ensures that the first, and worst, casualty of the war on drugs will be the precious liberties of our citizens.") Even if the Court were not predisposed to favor the war on drugs over the Fourth Amendment, serious difficulties might arise with an inductive, case-by-case approach to the identification of privacy expectations. Such an approach could well produce an incoherent, patchwork privacy doctrine, one that reflects contemporary attitudes but that lacks underlying unity. This is just the danger that would emerge if courts were to give normative significance to polling data about privacy expectations. See Christopher Slobogin & Joseph 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). In surveying members of the public, Slobogin and Schumacher asked subjects to rank 50 different kinds of interventions in terms of their intrusiveness on privacy. *Id.* at 738-39. Topping their list (as most intrusive) were body cavity searches; at the bottom were searches of foliage in public parks. *Id.* But interesting as these results are, they do not hold out the promise of a coherent body of privacy doctrine. In particular, they hold out no promise of guidance for technological innovations yet to be produced. By contrast, the coherence method advocated here, which starts with a unifying theme in privacy conventions (concern about personal vulnerability), and considers how that theme is manifested in specific settings, does hold out the prospect of a unified body of legal doctrine.

D. THE FEATURES OF A VALID PRIVACY CLAIM

When we think about privacy, we are concerned with an exclusionary practice—that is, we are concerned with a practice that distinguishes between insiders and outsiders and accords an advantaged position to the former vis-à-vis the latter. Privacy is, of course, only one of many exclusionary practices.¹⁶⁷ There are two ways in which privacy is different for other exclusionary practices: (1) The way in which privacy is achieved; and (2) The social function of privacy. Privacy is achieved by nonexposure—that is, by an insider denying outsiders sensory access to what she withholds from them. “Nonexposure” is an awkward word, yet it is essential because it captures an important feature of privacy. The term “privacy” is *not* the converse of the term “publicity.” There is a middle ground between active efforts to achieve privacy and active efforts to publicize, and that middle ground is a domain in which someone *cannot* validly claim privacy.

Think, for example, about the placement of a relatively unimportant object in a setting where members of the public are likely to notice it in the course of their routine activities. If someone leaves her sunglasses in the back seat of a car she has parked on a city street, one would not say that she has made an effort to publicize the sunglasses. On the other hand, one would not say that she has made an effort to ensure the privacy of the sunglasses. Because the sunglasses are exposed to members of the public using the sidewalk, one would have to conclude that their owner does not have a privacy interest in them.¹⁶⁸

¹⁶⁷ See, for example, Blackstone's characterization of property as “that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe.” 2 WILLIAM BLACKSTONE, COMMENTARIES *2.

¹⁶⁸ The Supreme Court's first Amendment jurisprudence concerning public and private figures provides a helpful contrast here. As a general rule, the Court has stated, “public figures . . . thrust themselves to the forefront of particular public controversies in order to influence the resolution of the issues involved.” *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 345 (1974). The Court has recognized exceptions to this, noting that it is “possible for someone to become a public figure through no purposeful action of his own.” *Id.* It has emphasized, however, that “instances of truly involuntary public figures must be exceedingly rare.” *Id.* The contrast with privacy is quite clear, then. Privacy must be sought; if someone fails to take the precautionary steps that ensure nonexposure, that failure can result in public consciousness of an object or information and consequently in loss of privacy. On the other hand, in

What about the reverse, then? Can it be said that someone achieves—or at least takes an important step toward achieving—privacy by ensuring that an object is not exposed to people as they go about their daily activities? This is the question Justice Stewart avoided in *Katz v. United States*.¹⁶⁹ He could, and should, have addressed it, however, for it is clear that someone partially fulfills the conditions of a valid privacy claim by taking steps to ensure that an object or information he wishes to withhold from others is substantially not exposed to them. The word “substantially” is essential here. That privacy claims do not require *full* nonexposure is made clear by everyday experience.

Consider, for example, the arrangement of door stalls in public restrooms. In the typical restroom, closing the door to a toilet stall does not wholly limit exposure of the person to those outside. Someone standing outside a stall can still peer through the slit that remains between the closed door and the beam to which it can be bolted. Does this mean that privacy conventions do not protect the person inside? Certainly not. In closing the door to a bathroom stall, the person using it achieves substantial nonexposure. A person standing outside is expected to grasp the significance of the closed door. While that person may still be motivated to look inside, she would not be able to do so.¹⁷⁰ Stated more generally, the nonexposure condition holds that the first identifying element of a privacy claim is met whenever it is clear an outsider would be unlikely to happen upon an object or information while present in a place members of the public are entitled to occupy.¹⁷¹

Substantial nonexposure is insufficient, however, to establish a valid claim. If it were sufficient, an individual could claim a privacy interest in anything she takes steps to avoid

most instances someone becomes a public figure only by seeking to become one. Only in the rare case will publicity be thrust upon someone.

¹⁶⁹ 389 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.”) (emphasis added). Stewart thus never commented on what *is* constitutionally protected given his nonexposure criterion. *See id.*

¹⁷⁰ *See Lorenzano v. Superior Court*, 9 Cal. 3d 626, 636 (1973) (“There is no requirement that a person ‘enclose himself in a light-tight, air proof box.’”); *see also* ERVING GOFFMAN, *BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS* 151-52 (1963) (distinguishing “conventional situational closure” from actual physical closure).

¹⁷¹ *See Katz*, 389 U.S. at 352.

exposing to others. Social conventions clearly do not support so broad a conception of privacy. Two contrasting scenarios help to underscore the importance of this point. Consider first a scenario in which someone receives a letter while visiting friends. The recipient of the letter opens the envelope, reads the letter, reacts with astonishment to its contents, carefully replaces it in its envelope, and then slips the envelope back in his pocket, saying nothing to those around him about its contents. Now consider a different scenario. While playing a game of poker, someone picks up the cards dealt her, inspects them, and holds them close to her chest, saying nothing to those in the room about the contents of the cards. Each scenario has important points in common. Each involves an insider/outsider relationship. Furthermore, people take on the status of outsiders in each instance by virtue of a person's effort to avoid exposing something to them.

But of course there is an important difference as well. For a poker player, efforts to exclude outsiders further only a strategic interest. By contrast, the exclusionary strategy followed in the letter-scenario involves a more substantial interest, one that is characteristic of privacy claims. At stake in such a setting is an individual's sense of personal vulnerability to others. At stake, in other words, are the embarrassment, anxiety, and distress people experience on having key features of their lives involuntarily revealed to outsiders.¹⁷² Clearly, the letter-writing scenario involves a privacy interest; equally clearly, the poker-game scenario does not.

Given the contrast between the two scenarios, it is reasonable to conclude that the special power associated with the word "privacy" is based on the term's connection to the protection of matters involving personal vulnerability. One would abuse the word were one to say that a poker player has a *privacy* interest in the contents of her cards. By contrast, one would use it properly were one to say that a person reading a letter has a privacy interest in its contents. There's no reason, of course, why "privacy," one of the many terms concerned with nonexposure strategies, should be connected with the

¹⁷² A college applicant has captured this sense of vulnerability in speaking of the embarrassment she felt if people examined even the return address envelopes of the colleges sending her letters of admission and rejection. See Johanna Winant, *Me and My Mailbox*, N.Y. TIMES, Mar. 27, 2000, at A21 ("Waiting for the college letters is easier in privacy.").

protection of personal vulnerability. But *some* term must have this connection—that is, some term is needed to emphasize the high seriousness associated with shielding people from unwanted revelations of personal matters to others.

It is because of privacy's connection to personal vulnerability that outsiders are expected to exercise forbearance when encountering it. Put differently, we can say that privacy conventions define the circumstances in which outsiders are expected to exercise restraint in order to spare insiders the embarrassment that comes with the involuntary revelation of matters related to personal life. The Court's fundamental error in its post-*Katz* jurisprudence is traceable to its failure to grasp privacy's social function. Vigilance expectations do indeed prevail in certain settings; they simply do not prevail in settings where personal vulnerability might be affected. When something less important is at stake—for example, when all that matters is winning or losing a card game—then vigilance is the norm. A similar point can be made about corporate trade secrets. An expectation of vigilance prevails for such secrets because the vulnerability at stake is commercial, not personal.¹⁷³ It is only because personal vulnerability involves interests of a higher order that the more stringent standard of forbearance defines social conduct.

The forbearance expectation does not, of course, mean that privacy can never be invaded. One must make allowance for the fact that people sometimes employ nonexposure strategies in order to make it seem as if personal vulnerability is at stake when it is not. Indeed, Fourth Amendment case law is rife with examples of people who have invoked the trappings of privacy to carry out schemes harmful to others.¹⁷⁴ But while the

¹⁷³ A similar point can be made about vigilance expectations in sports: "Orlando Hernandez and the new Yankee Roger Clemens are sharing secret information about pitching that Hernandez cannot relate. This is like war, Hernandez explains through an interpreter, and of course you cannot share war secrets." Buster Olney, *A Habit Yanks Can't Seem to Shake*, N.Y. TIMES, Mar. 5, 1999, at D2.

¹⁷⁴ Modern case law, for example, has often been concerned with settings in which people turn their homes—while invoking the trappings of residential privacy—into business centers for assembling and selling narcotics. See, e.g., *Minnesota v. Carter*, 525 U.S. 83 (1998); *United States v. Leon*, 468 U.S. 897 (1984); *United States v. Lewis*, 385 U.S. 206, 211 (1966) ("[W]hen, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than it if were carried on in a store, a garage, a car, or on the street.").

forbearance model doesn't require absolute protection for privacy, it does require that an outsider grant insiders considerable leeway in settings where privacy might be at stake. It requires, at a minimum, that people avoid prying and snooping in such settings. Summarizing the points just made, we can say that someone in the *ex ante*—an outsider not privy to the conduct of an insider—is expected to exercise forbearance in a setting where a substantial degree of nonexposure can reasonably be supposed to signal an interest in protecting personal vulnerability.

These remarks provide a general framework for thinking about privacy. Let us now expand on the framework by considering key issues related to it: the different types of privacy, the possibility of interpersonal privacy, and the signals people use to communicate an interest in privacy.

1. *The Different Types of Privacy: Privacy of the Person and Informational Privacy*

The paradigmatic privacy claim has to do with the body, in particular with limiting access to one's sexual organs.¹⁷⁵ Why people invest this issue with such importance is not entirely clear. The likeliest explanation is that cultural taboos have developed about sex, although it is possible something instinctive is at stake.¹⁷⁶ But the source of this sense of vulnerability is not critical here. What matters for purposes of privacy analysis is that most people in our culture experience feelings of embarrassment, distress, and anxiety about the involuntary revelation of their sexual organs.¹⁷⁷

¹⁷⁵ Thomas Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 266 (1977) (“[Wh]atever the sources of its normative commitments, must take the body as its first and most basic reference.”) Elsewhere, Gerety states that privacy should be defined as “an autonomy or control over the intimacies of personal identity.” *Id.* at 236.

¹⁷⁶ See NORBERT ELIAS, *THE CIVILIZING PROCESS: THE HISTORY OF MANNERS* 134 (1978). Elias has argued that during the sixteenth and seventeenth centuries, many acts that were once viewed as public—wiping one's nose, defecation, and lovemaking, for example—came to be considered private. As he puts it, there was a “notable rise of the shame threshold” during this epoch. *Id.*

¹⁷⁷ In commenting on mores in the Middle Ages, Norbert Elias has remarked on a general “unconcern in showing the naked body” NORBERT ELIAS, *THE CIVILIZING PROCESS: THE HISTORY OF MANNERS* 164 (1978). “This unconcern disappears,” Elias argued, “slowly in the sixteenth and more rapidly in the seventeenth, eighteenth, and nineteenth centuries, first in the upper classes and much more slowly in the lower.” *Id.*

The distinction between privacy of the person and informational privacy is made clear by the fact that someone can feel vulnerable about exposing her body to outsiders even when outsiders have detailed information about it. Think, for example, about a doctor who has just completed an examination of the scars on someone's thighs. If informational privacy were all that mattered to the patient, one would not expect her to dress before conferring with the doctor about remedies for her problem. That most patients decide to dress on such occasions is an indication of the importance people accord privacy of the person when it stands alone as a value.¹⁷⁸

Informational privacy can also stand alone. Indeed, although there are many occasions when informational privacy and privacy of the person converge, informational privacy's special significance is discernible in those settings when it has no connection to privacy of the person. For example, when someone leaves her home, she can still have an interest in limiting access to the material she left behind—an informational interest, in other words, that the traveler can assert independently of her interest in limiting access to her person.

2. *Interpersonal Privacy: Symmetrical and Asymmetrical Relationships*

In thinking about privacy, one tends to focus first on the protection it offers the solitary individual. In the classic setting, an individual is the sole insider, someone who has taken steps to ensure that important objects (perhaps his body, perhaps something else) or information are not exposed to *any* outsider. Familiar examples include closing the door to a room (privacy of the person) or making a diary entry (informational privacy).

¹⁷⁸ A parallel pattern can be found in a newspaper interview conducted with an advocate of public nudity. See Sarah Lyall, *Godiva Outstripped: A Global Call to Peel It Off*, N.Y. TIMES, Mar. 13, 2001, at A4. In trying to promote the cause of public nudity, Vincent Bethell, an artist from Coventry, England, has founded an organization, Freedom to Be Yourself, and even started a website. See *id.* He has also been subjected to numerous arrests and, on at least one occasion, argued, while completely naked, successfully before a jury for his acquittal on charges of being a public nuisance. See *id.* Nonetheless, Bethell wears clothes while granting interviews to newspaper reporters. See *id.* "Mr. Bethell takes his campaign seriously," one reporter remarked, "even if he does not walk around unclothed all the time. He was not naked, for instance, during a recent interview at home in Coventry—which, coincidentally, was the scene of Lady Godiva's ride." *Id.*

Here, then, is the public in its simplest form—the public is everyone except the person who has taken steps to avoid exposing something to all others.

But what if a small group of people—a married couple, for instance, or a circle of friends—seeks privacy from the world? Or what if someone confides information on the basis of a special-purpose relationship with, say, a doctor or a psychotherapist? Settings such as these involve interpersonal privacy, not the privacy of one person vis-à-vis the world. Everyday conventions make allowance for circles of privacy such as these. Indeed, the points already made about privacy of the individual are relevant to small-group bonds as well. In considering interpersonal privacy, we will be able to draw on the distinction already developed between privacy of the person and informational privacy. Moreover, we will find further confirmation of the argument that privacy's social function is to protect personal vulnerability.

Interpersonal privacy is possible in both symmetrical and asymmetrical relationships. Consider first the negotiation process that underlies the creation of small-group ties. Adults establish bonds with one another through a delicate process of exchange, one that can escalate from acquaintanceship to friendship, and from friendship to intimacy. These can be classified as "symmetrical relationships" because the defining feature of each is reciprocal revelation and a corresponding growth of trust. Sexual relationships involve two simultaneous exchanges: an exchange of access to the person and a parallel exchange of confidences. In friendship, there isn't the same kind of access to the other's person, though the exchange of confidences can be just as intense. Trust is established by each side's *not* exposing delicate information to outsiders. Rarely are formal agreements reached about what can be revealed.

Rather, people establish trust over time by not revealing confidences exchanged, thereby laying the foundations for further exchanges. Distinctions between different types of symmetrical relationships are drawn in Table 2. The contrast between symmetrical and asymmetrical relationships is easy to state: the former are marked by reciprocal, the latter by one-sided, revelation. Because people usually feel vulnerable about making one-sided revelations, many asymmetrical relationships—for example, those between doctors and patients,

TABLE 2.
PERSONAL SECURITY AND THE SYMMETRY OF RELATIONSHIPS

<u>Structure of relationship</u>	<u>Specific relationship</u>	<u>Legal status</u>
Asymmetrical relationships	Doctor-patient	Legally protected
	Lawyer-client	
	Police-citizen	Partial legal protection
	Press-citizen	
	Corrections officer-inmate	Legally Unprotected
	Ancient mariner-listener (insider revealing matters to a reluctant outsider)	
	Gossip-subject of gossip (outsider pursuing information from reluctant insider)	
Symmetrical	Husband-wife	Legally protected
	Unmarried lovers	Legally Unprotected
	Friendship	
	Acquaintanceship	

Characteristics of asymmetrical relationships:

Revelation of facts and sometimes of private parts of the body without corresponding revelation by other person.

Power derived from (1) asymmetrical access to body and/or (2) asymmetrical possession of information about the person making revelations.

Characteristics of symmetrical relationships:

Initial acceptance of forbearance: relationship predicated on each party's willingness to make revelations to one another.

Negotiated revelations—of information and body—grounded in principle of exchange, thus allowing for upward spiral of intimacy.

and lawyers and clients—are safeguarded by legal prohibitions against the disclosure of confidences. Many asymmetrical relationships are thus special-purpose in nature. People reveal embarrassing facts about their lives in return for the benefits

they hope to receive from professionals.¹⁷⁹ In this sense, there is a *quid pro quo* arrangement discernible in client-professional relationships. At the same time, one must note that, even when safeguards against revelation to outsiders are in place, the one-sidedness of a client-professional relationship confers substantial power on the latter over the former. A patient exposes his body to a doctor, but the doctor of course does not reciprocate. A patient discusses her life's crises with a psychotherapist, but no reciprocation is provided. The relative standing of the parties is defined by this asymmetry.

3. *Asymmetry in Surveillance Relationships*

When asymmetrical relationships are not protected by legal prohibitions against disclosure, they loom as ominous and frightening to those under observation. Three types of relationships fitting this description are mentioned in Table 2: one having to do with the police, another with the press, and a third with prison officials. Because the police are the subject of this Article, let us turn for a moment to their closest analogue, the press. Like the police, journalists are subject to legal restrictions that require them to respect the privacy of others.¹⁸⁰ One misunderstands the nature of the press, however, if one focuses solely on such formal restrictions, for the press, like the police, are occupationally committed to gaining information through asymmetrical relationships with members of the public. It is the highly atypical member of the public who follows people about in the streets or who hangs around doorsteps in

¹⁷⁹ The most telling example of this in modern life is to be found in the patient-psychotherapist relationship. It is an axiom of psychotherapy that the therapist is not to inject herself into the relationship with a client. A client discusses his anxieties in the absence of reciprocal revelation by the therapist. The Court has upheld a client-psychotherapist privilege through its interpretation of Rule 501 of the Federal Rules of Evidence. *Jaffee v. Redmond*, 518 U.S. 1, 10 (1996) ("Effective psychotherapy . . . depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears.") For a discussion of evidentiary privileges in other asymmetrical relationships, see 8 WIGMORE ON EVIDENCE, Chaps. 82 (Attorney-Client), 86 (Physician-Patient), and 87 (Priest-Penitent) (Walter Reiser ed. 1991).

¹⁸⁰ These rules are sometimes place-based. Consider, for example, the conclusion of the California Supreme Court that the secret placement of television cameras in a workplace not open to the general public is an invasion of privacy. *Sanders v. American Broadcasting Companies.*, 85 Cal. Rptr. 2d 909 (1999). The rules can also incorporate a concern with social roles, in particular, with whether someone has sought a public role for himself. See *Time, Inc. v. Firestone*, 424 U.S. 448 (1976).

the hope of gleaning information about someone who leaves her home. For the press (and the police), on the other hand, this is part of their job. While legally placed in the same position as members of the public in terms of what they can observe, journalists in fact use the resources of their organizations to carry out operations few individual members of the public are able to execute.¹⁸¹

Now consider prison life. The Supreme Court has held that inmates have *no* constitutionally protected privacy interests in the contents of their cells.¹⁸² Assuming for purposes of discussion that this is a correct analysis of the Fourth Amendment, we can say that prison life stands in direct contrast with life outside, a contrast far more dramatic than the one that prevails in relations between the press and the public. The degradations of the prison—strip searches, random inspections of inmates' cells, pervasive telephone surveillance—define the polar opposite of everyday privacy expectations. Within prisons, corrections officers affirm their power over inmates by imposing on them a condition of permanent, asymmetrical exposure.¹⁸³ Given the numerous published accounts of the demeaning side effects of this condition,¹⁸⁴ it is reasonable to conclude that when asymmetry is subject to no legal standards, it confers on the nondisclosing party a debilitating power over those living in the condition of compelled exposure.

4. *The "What" and "How" of Privacy Analysis: Conventional and Idiosyncratic Sources of Personal Vulnerability*

We have concentrated so far on the connection between privacy and different types of interpersonal relationships. Let

¹⁸¹ Indeed, journalists avail themselves of exactly the same surveillance techniques and expensive resources used by the police. Compare the helicopter surveillance by reporters for *THE NATIONAL ENQUIRER* of the backyard of actor Carroll O'Connor (discussed in JEANNETTE WALLS, *DISH: THE INSIDE STORY ON THE WORLD OF GOSSIP* 171 (2000)), with the Court's endorsement of the same technique for police surveillance in *Florida v. Reilly*, 488 U.S. 445 (1989).

¹⁸² See *Hudson v. Palmer*, 468 U.S. 517 (1984).

¹⁸³ See, e.g., GRESHAM SYKES, *THE SOCIETY OF CAPTIVES: A STUDY OF A MAXIMUM SECURITY PRISON* 41 (1958) ("The most striking fact about this bureaucracy of custodians is its unparalleled position of power vis-à-vis the body of men which it rules and from it is supposed to extract compliance.")

¹⁸⁴ See, e.g., JACK HENRY ABBOTT, *IN THE BELLY OF THE BEAST* (1981); PAUL LIBERATORE, *THE ROAD TO HELL: THE TRUE STORY OF GEORGE JACKSON, STEPHEN BINGHAM, AND THE SAN QUENTIN MASSACRE* (1996); STEVEN LINSKOTT, *MAXIMUM SECURITY* (1994); PETER REMICK, *IN CONSTANT FEAR* (1975).

us now consider the “what” and the “how” of privacy: *what* it is that social conventions designate as private; and *how* a person can avail herself of signals that convey an interest in privacy.

The “what” of privacy analysis is easily defined. In a given society, matters are classified as private when their involuntary exposure is likely to engender a sense of vulnerability to others.¹⁸⁵ This conventionalist account is consistent with the analysis, provided earlier, of Harlan’s reasonable expectations test. On this account, nothing is intrinsically private. Indeed, this approach allows for the possibility of changes over time in the sources of personal vulnerability. Less than a hundred years ago, ladies experienced anxiety over the involuntary exposure of their legs.¹⁸⁶ Today, few women do. Even in contemporary society, people experience anxiety over the involuntary exposure of their genitals. Other matters that are strongly private (in that people feel substantial anxiety about their involuntary exposure) include the contents of medical records and of one’s home. Matters that are weakly private (i.e., that generate only a mild feeling of anxiety) include the contents of cars, of the curtilage of homes, of pockets, and so on.¹⁸⁷

¹⁸⁵ Some examples from the press will help illustrate that the category “personal information” (the “what” of privacy, as I have called it) is deeply embedded in everyday speech. Medical records, for instance, are said to contain “intimate information.” *Trifling With Medical Privacy*, N.Y. TIMES, Sept. 11, 1997, at A30. Financial records are viewed as “personal information.” *Privacy in Financial Dealings*, N.Y. TIMES, Nov. 3, 1999, at A24. Love letters are said to be “as private as correspondence can be” Peter Applebome, *Love Letters in the Wind: A Private Affair of the Famously Anonymous Salinger*, N.Y. TIMES, May 12, 1999, at E1. All the above examples have been drawn from one newspaper, however, an example from another underscores the broad consensus that exists in contemporary society as to the “what” of privacy. In speaking of a requirement that an employee take a penile plethysmograph test to find out whether he was attracted to young boys, a reporter for *The Wall Street Journal* characterized the test as a “particularly intimate” one. Stephen J. Adler, *Privacy, Technology Collide in a Dispute over an Intimate Test*, WALL ST. J., Feb. 2, 1993, at A1.

¹⁸⁶ See BERNARD RUDOFSKY, *THE UNFASHIONABLE HUMAN BODY* 47-48 (1974) (“For five generations legs have led a twilight existence. Only outcasts of society who lived on the periphery of proper conduct, such as circus performers, were recognizable as bipeds When female legs came in the open, it was often thought necessary to encase them in heavy stockings, tights, or, better yet, boots Human ingenuity, tempered with hypocrisy, even found ways of measuring modesty in yards and inches. When fashion magazines published charts giving the correct length of little girls’ skirts, the yardstick superseded the etiquette book.”)

¹⁸⁷ See Stanley Benn, *Privacy, Freedom, and Respect for Persons*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY* 224 (Ferdinand Schoeman ed., 1984).

And what about matters whose involuntary exposure generates anxiety in only a few members of society? We can call these “idiosyncratic” sources of vulnerability. Because the possible sources of this kind of vulnerability are infinite, the critical point here is an individual’s resort to widely understood cues that signal to others the individual’s interest in withholding something from others. This is the “how” of privacy expectations. Because understandings of what constitutes a cue can vary, the key to idiosyncratic sources of vulnerability can be found in someone’s invocation of a symbol that those around her can be expected to understand—the closed door, for example, or the sealed envelope (to cite two examples that are unmistakable in our culture).

That someone’s anxiety is prompted by an idiosyncratic source doesn’t mean that that person’s concern is any less worthy of respect than anxiety prompted by conventional sources. On the contrary, *both* sources of vulnerability receive widespread respect, though in different ways. Because the defining feature of conventional vulnerabilities is that many people feel the same way about revealing something, everyday expectations are grounded in a presumption *favoring* privacy on such occasions.¹⁸⁸ Only a modest cue is needed to secure privacy when conventional sources of vulnerability are at stake—closing the door to one’s room, pulling down a shade, sealing an envelope, and so on. By contrast, the opposite presumption prevails for idiosyncratic sources of vulnerability. In our culture, people don’t expect others to feel vulnerable about, say, revealing their legs. A person emits an unmistakable signal that he expects privacy when he does feel vulnerable (think, for example, about someone wearing full length pants held tight by a strong belt during a hot day at the beach).

This account, it should be noted, builds on, while also modifying, Harlan’s two-prong test.¹⁸⁹ It is consistent with the test in treating social conventions as the touchstone of privacy

¹⁸⁸ An affirmative act is thus required to make it clear to outsiders that someone wishes a stranger to consider matters conventionally classified as private. Think, for example, about Samuel Taylor Coleridge’s ancient mariner. “It is an ancient Mariner/and he stoppeth one of three . . .” SAMUEL TAYLOR COLERIDGE, *THE RHYME OF THE ANCIENT MARINER* (1798). In detaining the wedding guest and pouring out his story to him, the mariner makes clear that he doesn’t want to keep private his peculiar tale of sea-faring woe. *See id.*

¹⁸⁹ *See* note 153 *supra* and accompanying text for a discussion of the Harlan test.

analysis.¹⁹⁰ It is also consistent with Harlan's approach in holding that privacy must be *secured*—in holding, in other words, that some affirmative step (a cue, as I have called it) is essential to gaining privacy.¹⁹¹ But it modifies the Harlan test by focusing on two distinct sources of personal vulnerability, conventional and idiosyncratic ones. Harlan made no effort to distinguish between these; indeed, he did not suggest that the occasions for experiencing personal vulnerability are among the identifying criteria of privacy. In this respect, the analysis I have provided serves as a corrective to the Harlan test.

5. *Recapitulation*

A summary of the points just made will provide an overview of the key elements of privacy analysis. When we speak of privacy, we are concerned with an exclusionary practice defined by two features. One has to do with nonexposure—that is, with a condition that makes it unlikely a member of the public will discover an object or information by chance. The other has to do with personal vulnerability, for it must be reasonable to suppose in the *ex ante* that the condition of nonexposure has the function of shielding someone from the distress, embarrassment, or anxiety associated with involuntary revelation of the object or information. Implicit in this framework is the distinction between privacy of the person and informational privacy. Moreover, given the framework, a further distinction can be drawn between conventional and idiosyncratic sources of vulnerability. One can place under the former heading those items whose involuntary disclosure is likely to generate a sense of embarrassment and distress in most members of a given society. The latter heading is concerned with those items most members of a society *do not* consider private but which someone may nonetheless not wish to disclose. Privacy cues—signals that communicate to outsiders an insider's interest in avoiding exposure—are needed for both sources of vulnerability. However, the signals must be stronger when the source of personal vulnerability is idiosyncratic.

¹⁹⁰ See notes 160-61 *supra* and accompanying text for a discussion of the significance of convention.

¹⁹¹ See *Katz*, 389 U.S. 347, 361 (1967), where Harlan, in outlining his criterion for determining whether someone has a subjective privacy expectation, says that a person must "have *exhibited* an actual . . . expectation of privacy. . . ." (emphasis added).

It is because privacy's social function is to protect personal vulnerability that forbearance expectations surround it. The special power of the term "privacy" is understandable in terms of this connection to personal vulnerability. Many exclusionary practices besides privacy employ nonexposure strategies: people in card games exclude their fellow players by means of nonexposure strategies; corporations exclude competitors from trade secrets by means of such strategies; baseball teams keep secret their signs for hitting and base-stealing; and so on. Vigilance is the norm in these settings precisely because personal vulnerability is not at stake. Forbearance expectations prevail in privacy settings because of the importance accorded to what is not exposed.

E. A REASONABLE EXPECTATION OF FORBEARANCE ON THE PART OF OTHERS

How do forbearance expectations operate in practice? In particular, how do they operate given the distinctions just drawn between conventional and idiosyncratic sources of vulnerability? A contrast with vigilance expectations will prove helpful in answering these questions. Under the forbearance model, a person expects others to exercise restraint, once modest efforts have been taken to avoid exposure, concerning matters generally understood to be private. A person similarly expects others to exercise restraint. Under the vigilance model, a person operates under the opposite expectation—that is, a person expects people will want to interfere with efforts to ensure nonexposure. Privacy expectations in everyday life are, of course, grounded in the forbearance model—or, to be more precise, in what I call "qualified forbearance." But the vigilance model, while not describing privacy expectations, does indeed capture expectations that prevail in certain settings (for example, card games) and special-purpose institutions (prisons, for instance). Table 3 provides an overview of the contrast. This table is based on a double distinction: (1) A general distinction between vigilance and forbearance models; and (2) A further distinction between full and qualified versions of each. Under the full vigilance model, *everything* is legitimately subject to surveillance. Full vigilance makes no allowance for privacy cues, nor does it treat anything as a private fact. Prison life provides a helpful example of full vigilance in action.

TABLE 3.
VIGILANCE AND FORBEARANCE MODELS OF PRIVACY EXPECTATIONS

	<u>Full Vigilance</u>	<u>Qualified Vigilance</u>	<u>Qualified Forbearance</u>	<u>Full Forbearance</u>
Typical setting	Prison	Card game	Everyday relations	"Best manners" social settings
General principle defining outsider/insider relationship	Unrelenting surveillance	Surveillance limited by insider's cues	Restraint toward others, with restraint lifted in limited circumstances	Restraint at all times
Cues recognized (the "how" of privacy)	No	Yes	Yes	No
Private facts recognized (the "what" of privacy)	No	No	Yes	Yes

Inmates' bodies, including all body cavities, are subject to routine inspection; given officials' concern with security, even these aspects of human anatomy are not off limits.¹⁹² Moreover, corrections officers accept no cues as to privacy. Indeed, if an inmate were to use a conventional privacy signal (if, for example, an inmate were to seal an envelope and mark it "Personal and Confidential"), this would have the perverse effect of subjecting the inmate's activities to more intense scrutiny than they would otherwise receive.¹⁹³ An inmate can

¹⁹² See, e.g., 28 C.F.R. 541(b) (Corrections officials may conduct a visual search where there is a reasonable belief that contraband is concealed on the person of a prisoner or where a good opportunity for concealment has occurred.); see also *Covino v. Patrissi*, 967 F.2d 73 (2d Cir. 1992) (upholding random visual body cavity searches for prisoners in Vermont's Northwest State Correctional Facility).

¹⁹³ Numerous circuit courts have held that corrections officials do not violate an inmate's constitutional rights by opening sealed envelopes containing nonlegal correspondence between that inmate and outsiders. See, e.g., *Gassler v. Wood*, 14 F.3d

expect privacy, then, only in the sense that she can anticipate that certain kinds of conduct will evade scrutiny.

Qualified vigilance creates important variations to the full vigilance model. With qualified vigilance, one encounters a world in which people are subject to surveillance by others (in this respect, it is similar to full vigilance), but in which they can invoke cues that require restraint on the part of those conducting surveillance (in this respect, it is different). If we return to the example of a card game, we will be able to discern the specific features of this model. The rules of poker presuppose an environment in which the players symmetrically observe each other but are required to exercise restraint when encountering cues that place limits on their quest for information. Thus, if Smith holds her cards close to her chest, Jones can not rip them away from her, nor can she surreptitiously inspect them if Smith places them face down on the table and rises to get a drink of water. But the rules offer no protection beyond this. In particular, if a player fails to hold her cards close enough to her chest, others can legitimately survey her hand. And of course, there is no conception of private facts in a poker game—a player's cards are fair game for inspection if she fails to exercise vigilance in shielding them from others.

Structurally, there is little difference between the world of the gossip and that of the poker player. For a gossip, human relations are the “playing field” in which the “game” of information discovery is conducted. The gossip engages in systematic surveillance of others; in turn, the gossip's subjects must exercise constant vigilance to ward off unwanted attention.¹⁹⁴ The gossip acknowledges the legitimacy of privacy cues—he doesn't open unsealed envelopes or barge through

406 (9th Cir. 1993); *Smith v. Delo*, 995 F.2d 827 (8th Cir. 1993); *United States v. Whalen*, 940 F.2d 1027 (7th Cir. 1990).

¹⁹⁴ See PATRICIA MEYER SPACKS, *GOSSIP* 11 (1985):

Gossip, even when it avoids the sexual, bears about it a faint flavor of the erotic. (Of course, sexual activities and emotions supply the most familiar staple of gossip—as of the Western realistic novel.) The atmosphere of erotic titillation suggests gossip's implicit voyeurism. Surely everyone feels—although some suppress—the same prurient interest in others' privacies, what goes on behind closed doors. Poring over fragments of others people's lives, peeing into their bedrooms when they don't know we're there, we thrill to the glamour and the power of secret knowledge, partly detoxified but also heightened by being shared.

closed doors, for example. But when a person's invocation of a cue indicates that a "juicy" fact is being withheld from others, that cue simply prompts the gossip to look for other means of discovering the withheld information. The gossip looks for that information because he believes it will be about an individual's vulnerability. For the gossip, there are no private facts—no facts that require restraint. Instead, private facts, like privacy cues, are bait for the gossip; they are exactly what the gossip's surveillance is designed to uncover.¹⁹⁵

Clearly, there are many important parallels between this model and the Court's analysis of privacy. The Court acknowledges that in everyday life each person has an interest in shielding matters from others' inspection.¹⁹⁶ But the Court analyzes this interest narrowly, in effect reasoning as if there are small islands of privacy in an otherwise huge sea of surveillance.¹⁹⁷ Its approach to privacy cues follows from this. While recognizing that people can legitimately take steps to ensure that objects and information are not exposed to others, the Court insists, as would a gossip or a card player, on complete nonexposure.¹⁹⁸ Thus, a person's failure to achieve complete nonexposure—for example, his failure to place a piece of corrugated roofing on his otherwise completely enclosed backyard¹⁹⁹—means that the person has no privacy interest in the objects she wishes to conceal. In fact, the Court sanctions police attempts to determine just what it is people have unmistakably signaled they wish to conceal.²⁰⁰ The Court has routinely rejected claims about private facts. It has refused,

¹⁹⁵ See WALLS, *supra* note 181, at 9.

¹⁹⁶ *Katz v. United States*, 389 U.S. 347, 352 (1967) ("One who occupies [a booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.")

¹⁹⁷ This point is particularly clear in the aerial surveillance cases. There can be no certainty that either *Ciraolo* or *Riley* "knowingly exposed" their backyards to the public (the criterion for not securing privacy adopted in *Katz*, 389 U.S. at 351). In each instance, the defendants took steps to make sure passersby at the street level could not inspect the contents of their yards, and *Riley* took the further step of covering most of his greenhouse with corrugated roofing. See *Ciraolo*, 476 U.S. at 209, and *Riley*, 488 U.S. at 448. It seems quite possible, then, that *Ciraolo* and *Riley* inadvertently exposed the contents of their yards to members of the public engaged in aerial surveillance.

¹⁹⁸ See *infra* notes 296-310 and accompanying text.

¹⁹⁹ See *Florida v. Riley*, 488 U.S. 445, 448 (1989).

²⁰⁰ See *infra* notes 296-310 and accompanying text.

for example, to acknowledge that people in our society feel a sense of vulnerability to others when their bank records are involuntarily disclosed to outsiders.²⁰¹

If privacy had no special function—if the protection of personal vulnerability were of no greater urgency than the protection of information in a card game—it would make good sense to say that privacy expectations are grounded in vigilance. It is because privacy does indeed have a unique social function that the more stringent expectations associated with qualified forbearance have developed for the conduct of personal life. The general principle underlying qualified forbearance is one of restraint in one's dealings with others. This principle can be stated in terms of a presumption against the sustained, uninvited interest in the lives of others. Consistent with this presumption are two specific rules of forbearance: (1) The rule to respect the conventional sources of personal vulnerability; and (2) The rule to respect the idiosyncratic sources of personal vulnerability.

Restraint is required when it is reasonably clear to an outsider in the *ex ante* that care has been taken to avoid the exposure of objects or information whose involuntary disclosure generates a feeling of vulnerability to others among most members of a given society. When it appears that conventional sources of vulnerability are at stake, an outsider must ascertain that an insider has affirmatively indicated her willingness to disclose them. Restraint is also required when privacy cues are employed as signals for objects or information that do not normally generate a sense of vulnerability for others. A cue having been used, outsiders must view it as interdicting access to the object or information; they must also honor the cue by not trying to gain access to the item by some other means.

Taken together, the general presumption in favor of restraint and the specific rules of forbearance define the underlying structure of the privacy expectations that prevail in everyday life. They do not offer full protection for privacy. Rather, they strike a balance, one that imposes on privacy-seekers the modest burden of signaling a desire for privacy while imposing on outsiders a burden of restraint once it seems likely a privacy interest is at stake. Two important points are understandable in light of this balancing calculus. First,

²⁰¹ See *United States v. Miller*, 425 U.S. 435, 441-43 (1976).

because privacy conventions place a burden on those seeking it, these conventions make allowance for the possibility of an inadvertent loss of privacy, either through negligence or bad luck. But while inadvertent losses of privacy are possible under everyday conventions, outsiders are expected not to exploit such mishaps through sustained scrutiny of what an insider meant not to expose to others.²⁰² Thus if we think about a misplaced wallet, we can readily agree that that owner of the wallet must accept some loss of privacy concerning the wallet's contents if he carelessly leaves it behind upon leaving a room. However, once an outsider has determined who owns the wallet, the rule enjoining respect for personal facts requires the outsider to stop examining the wallet further and to find a way to return it to its owner.

The second point relevant here has to do with the distinction between the curiosity and systematic scrutiny of others. Neither the general presumption in favor of restraint nor the specific rules of forbearance require people to rein in all curiosity about the world. Rather, they prohibit sustained, uninvited surveillance of others. For example, if Smith, who enjoys observing the world, happens to note as she walks down the street that Jones, who hasn't pulled the blinds for the parlor of her first floor apartment, is sobbing and wailing as she sits on her couch, Smith can properly say to herself that she did not interfere with Jones's privacy by noticing her behavior. At the same time, though, privacy conventions require Smith to hold her curiosity in check. The fact that she happened upon a setting that piqued her interest does not provide her with license to begin sustained surveillance to determine what is going on. Everyday privacy expectations, we can say by way of summary, offer people a chance to appreciate the surface of the human comedy but prohibit them, absent invitation from the players, to penetrate the comedy's details.

²⁰² See Eleena de Lisser, *Hearing and Seeing Business Travel Blab and Laptop Lapses*, WALL ST. J. Nov. 8, 1999, at A1:

Steven Bennett was pecking away on his laptop on a flight from San Francisco when he sensed another pair of eyes intently looking at his computer screen. Mr. Bennett, a media consultant in Cambridge, Mass., has experienced this before. So, he swung into action. With just a few keystrokes, Mr. Bennett opened a file called READTHIS.Doc. Up popped a single sentence: 'If you can read this, you ought to be ashamed of yourself.' The busted traveler next to him stiffened in his seat. 'It works every time,' says Mr. Bennett, 'It's a nice, polite two-by-four between the eyes.'

With full forbearance, by contrast, the possibility of enjoying any part of the human comedy is almost completely precluded. This is because the contrasts just noted disappear—or at least are strongly attenuated—under the full forbearance model. Strenuous efforts are taken by outsiders to ensure that insiders do not inadvertently lose privacy, and outsiders also act on the assumption that there can be no legitimate curiosity in others' activities absent an explicit, affirmative invitation to inquire.²⁰³ In this respect, the full forbearance model takes us into the world of exquisite manners—a world of tact and restraint, a world beyond society's everyday expectations. Privacy cues cease to matter in this context because everything having to do with personal life is presumed private. Correspondingly, the domain of private facts and objects is vastly expanded, and the threshold for discussion is raised through the requirement that people unambiguously demonstrate their willingness to have them discussed. There is often an element of hypocrisy in the world of perfect manners, with people feigning a lack of curiosity in private facts when they actually are immensely interested in what might be discovered. Fine manners should not be scorned, however. Although they do not define the rougher world of everyday privacy conventions, they do remind us that there is a realm of consideration and tact located beyond it.

F. THE POSSIBILITY OF A ROLE DISCOUNT FOR THE POLICE:
REJECTING AN ACROSS-THE-BOARD DISCOUNT WHILE
ACCOMMODATING THE GOVERNMENT DURING EMERGENCIES

A critic of the points just made could agree with the characterization of laypersons' privacy expectations but still maintain that the police should not be held to them. The critic might advance two arguments on this score. First, the critic could argue for an across-the-board discount for the police from lay expectations. Second, the critic might make a more modest claim, contending that a discount is appropriate in emergency settings. The broader claim is without merit, I shall maintain,

²⁰³ See ELIZABETH L. POST, *EMILY POST'S ETIQUETTE* 90 (15th ed. 1992). Consider Emily Post's rules about contact with the handicapped. See *id.* First, "NEVER stare or indicate that you are conscious that the person is different from others in any way." *Id.* Second, "never . . . ask personal questions of one with an obvious disability." *Id.*

while the narrower one can be sustained, though only in substantially modified form.

Consider first the argument for an across-the-board discount. Although the Court has *spoken* in terms of laypersons' privacy expectations, it has *reasoned* in terms of a police discount from these. The results, the critic could suggest, have thus been sound; the only problem is that the Court has failed to argue candidly for its conclusions. In openly declaring its position, the Court would reject the prospect of a full discount from lay expectations. It would, however, provide a partial one—that is, it would openly exempt them from the more stringent expectations of everyday life but would still proscribe egregious conduct. Because this is exactly the line the Court has already been pursuing, all that now needs to be done, the critic could maintain, is to muster the courage to acknowledge its position candidly.

This argument is deeply flawed, both as a matter of prudence and of principle. The consideration of prudence is easy to grasp. As noted earlier, the police stand in an asymmetrical relationship with the public: they scrutinize individuals, but they are not subject to comparable scrutiny in return. Moreover, as also noted, the police devote vast resources—in manpower (stakeouts and tailing, for example) and equipment (infrared devices, eavesdropping paraphernalia)—to the systematic scrutiny of members of the public. Even when the layperson baseline is used, then, the difference between police resources and those of most laypersons means that the police can subject people to far more surveillance than can virtually any other organization in contemporary society (with the press a somewhat distant second). And if the layperson baseline occasions concern given current police resources, deeper disquiet is appropriate if the police receive a discount from this baseline. Indeed, from the standpoint of prudence, an across-the-board discount appears to be the height of folly. Rules that hold the police to the layperson baseline pose danger enough given the special resources available to them. To grant the police a discount in all times and places from this baseline is to court disaster.

This, of course, is simply an argument (though a powerful one) from prudence. There is, however, a quite different argument—one based on principle—that explains why the current, unacknowledged, across-the-board discount should be

rejected. As noted in the first section of this Article, courts follow a two-step process of inquiry in assessing Fourth Amendment claims.²⁰⁴ Courts first ask whether the police have violated an interest the Amendment protects.²⁰⁵ If the answer to this question is negative, no further inquiry is needed.²⁰⁶ If positive, then courts further ask whether the police activity was reasonable (whether, for example, an officer had probable cause to arrest).²⁰⁷ The distinction between the two steps is critical. The first involves a norm of general application, applicable to both government officials and the public.²⁰⁸ The judicial inquiry into privacy interests begins with an examination of the expectations that prevail generally in social life.²⁰⁹ Courts also begin their inquiries into property and liberty interests with an analysis of norms of general application.²¹⁰

It is in the second stage of analysis that the police receive a role discount.²¹¹ Consider electronic surveillance, for example. Laypersons are legally barred from interfering with privacy interests by conducting electronic surveillance of other people's phone conversations.²¹² The police, by contrast, are authorized to do so upon obtaining a court order²¹³—and the police further possess qualified immunity against tort suits when they act pursuant to an order's conditions.²¹⁴ Think also about the discount accorded the police with respect to liberty and property interests. A citizen's arrest for a felony is legally justified if the arrestee actually committed the felony for which he is arrested or if, a felony having occurred, the citizen carrying out the arrest has reasonable grounds to suspect the arrestee actually committed that crime.²¹⁵ By contrast, an officer can justify a felony arrest on the basis of probable cause—and

²⁰⁴ See *supra* pp. 30-31.

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ See the *Jacobsen* passages cited *supra* in Table 1. In each, the Court invokes a norm of general application.

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ That is, they are subjected to a more lenient standard than the one imposed on members of the public.

²¹² See 18 U.S.C. § 2511(1)(a) (2000).

²¹³ See 18 U.S.C. § 2516 (1) (2000).

²¹⁴ See *Malley v. Briggs*, 475 U.S. 335 (1986).

²¹⁵ See RESTATEMENT OF TORTS 2d, § 119(a)-(b).

provided probable cause is present, is immune from civil liability even if it turns out no felony was actually committed.²¹⁶ Thus, the special nature of the police role is *already* taken into account in the second stage of inquiry. To include it in the first as well would introduce a spurious form of double-counting into the Fourth Amendment calculus.

The points just made provide a framework for determining what is, and is not, plausible about an argument for reducing privacy during times of emergency. What courts should not do is discount privacy interests themselves. Indeed, for the reasons just stated, this is wholly unnecessary. Given the reasonableness requirement of the Fourth Amendment, the approach courts should take during times of emergency is not to discount privacy interests but to give greater weight to public security, thereby recalibrating the balance between government and individual interests. This approach avoids the devaluation of privacy interests. While the weight of privacy interests remains constant, those interests are simply eclipsed by the increased urgency of public security. This approach also promotes candor in judicial opinions, requiring courts to focus directly on the factors that justify a recalibration.

Although the Court has tended to discount privacy interests in almost all its opinions, it has, on the specific question of how to respond to pressing emergencies, taken the recalibration approach advocated above. For example, in *Camara v. Municipal Court*, the Court remarked, when considering how to weigh factors on the government side of the reasonableness equation, that "the public interest demands that all dangerous conditions be prevented or abated."²¹⁷ Moreover, in numerous opinions considering the permissibility of government intrusions *not* based on particularized suspicion, the Court has distinguished carefully between settings in which "ordinary criminal wrongdoing" is under investigation (particularized suspicion always required) and settings in which a "special governmental need beyond the normal need for law enforcement" requires immediate action (particularized suspicion not required if dispensing with it is reasonably related

²¹⁶ See *id.* at §121. The common law origins of the special protection of police officers are discussed in Horace Wilgus, *Arrest Without a Warrant*, 22 MICH. L. REV. 673 (1924).

²¹⁷ 387 U.S. 523, 537 (1967).

to solving the problem).²¹⁸ Thus, under the Court's analysis, when there is a substantial, immediate hazard unrelated to ordinary criminal wrongdoing, the reasonableness inquiry is recalculated. This approach makes it necessary for government officials to identify an emergency and to explain why their disregard of particularized suspicion will help to address that emergency.

Inevitably, we must ask what counts as an emergency? The question is by no means an easy one, but certainly a paradigm case of a national emergency is to be found in the terrorist attacks of September 11, 2001. This emergency had the following characteristics: (1) There was no doubt that some people were willing to inflict mass death on innocent American civilians; (2) Particularized suspicion of those willing to carry out terrorist schemes was frequently unavailable; and (3) Confined public spaces essential to modern life—bridges and tunnels, for example, as well as public conveyances—provided particularly inviting targets for terrorists.²¹⁹ Under such circumstances, it was reasonable for the police to dispense with particularized suspicion and to conduct random searches that would ordinarily be impermissible.²²⁰ The Fourth Amendment's reasonableness requirement allows for this kind of flexibility.²²¹ In using it, courts need not discount privacy interests but

²¹⁸ See also *Michigan v. Sitz*, 496 U.S. 444, 449-50 (1990); *U.S. v. Martinez-Fuerte*, 428 U.S. 543, 561-64 (1976). Compare *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-42 (2000) (discussing ordinary criminal wrongdoing), with *Treasury Employees v. Von Raab*, 489 U.S. 656, 665-66 (1989) (discussing special governmental needs beyond the normal need for law enforcement).

²¹⁹ See David Wessel, *A Pivot Point in American Life*, WALL ST. J., Oct. 4, 2001 at A1:

Before Sept. 11, Americans worried about the growing capacity of government and business to use technology to instantly retrieve and share intimate details of our lives. When the Department of Health and Human Services was drafting new privacy rules for medical records last year, it got 52,000 comments. Today, concern about privacy is displaced by concern about security. At Tyler's airport [in Tyler, Texas], the screeners open every carry-on bag and examine every crevice. But no one complains, even silently about exposing dirty underwear in a public place.

Mr. Wessel's comments on the change in public attitudes are perceptive. It seems unlikely that the concern with privacy he notes with respect to medical records and technology in general will simply disappear.

²²⁰ See Justice O'Connor's remarks, cited in note 17 *supra*, for an indication of the way in which current justices may be willing to rethink fourth amendment doctrine in light of the terrorist attacks on the United States.

²²¹ See the Court's analysis of reasonableness in *Camara v. Municipal Court*, 387 U.S. 523, 537 (1967).

instead revalue, as circumstances require, the public's interest in security. In the remainder of this essay, my discussion will assume that an emergency does not justify the overriding of privacy interests. My remarks here serve as a reminder that this justification will not always be the case.

IV. APPLYING THE FORBEARANCE MODEL

If society's core privacy expectation is forbearance with respect to matters of personal vulnerability, then a great deal of post-*Katz* privacy jurisprudence must be reassessed. The reassessment will not, however, invariably require an expanded version of privacy protection. As we shall see, the Court has erred in both directions. In many instances, it has been too stingy about privacy; in others, it has been too generous.²²² I begin by considering the latter possibility—by considering settings where an outsider can discern in the *ex ante* that no privacy interest can possibly be at stake but where the Court has nonetheless spoken of Fourth Amendment privacy protection. I then turn to the reverse possibility by noting the even greater list of settings where the Court has failed either to note the existence of privacy interests or to accord them sufficient weight.

A. SETTINGS WHERE PRIVACY CANNOT BE AT STAKE

Because no Court opinion has tackled the question of what we mean by the term "privacy," numerous cases have proceeded from the premise that an object or information is the subject of Fourth Amendment privacy protection when it is fully shielded from the public-at-large.²²³ We have already seen why this premise involves a conceptual error.²²⁴ Complete nonexposure, as I have noted, is not essential to a valid privacy claim.²²⁵ Rather, two other factors, each of which must be discernible in the *ex ante*, are essential: (1) A substantial degree of

²²² For my argument that it has been too stingy, see *infra* Parts IV.B, IV.C; for my argument that it has sometimes been too generous, see *infra* Part IV.A.

²²³ In the aerial surveillance cases, for example, the Court assumed that the defendants could not claim Fourth Amendment privacy protection because they had failed to shield their backyards completely from surveillance by airplanes and helicopters. *California v. Ciraolo*, 476 U.S. 207 (1986); *Florida v. Riley*, 488 U.S. 445 (1989).

²²⁴ See *supra* notes 172-73 and accompanying text.

²²⁵ *Id.*

nonexposure, enough to signal to an outsider that caution is required before proceeding further; and (2) Some reason to believe that the nonexposure is related to the protection of personal vulnerability. When something has been fully shielded from others, there *may* be a privacy interest at stake. There may not be, however; indeed, on many occasions, it is possible to know in the *ex ante* that a concealment strategy has nothing to do with privacy.

We have already considered this point with respect to poker games.²²⁶ The poker player, we have seen, has a *strategic* interest in making sure his cards are not exposed to other players in a game.²²⁷ This strategic interest is not to be confused with a privacy interest, however.²²⁸ In fact, because personal vulnerability is not and cannot be at stake in a poker game, a poker player operates with an expectation about the vigilance, not the forbearance, of others.²²⁹ We can now apply this point to other settings, in particular to those in which government agents subject corporations to surveillance.

Let us start with what the Court has gotten right in this context—its conclusion that certain *methods* of penetrating concealment don't interfere with privacy interests. The seminal case regarding this issue is *United States v. Place*, where the Court considered the constitutionality of dog-sniffs of luggage.²³⁰ Suspecting that Place had narcotics in his suitcase but not having probable cause to seize and inspect it, police at New York's LaGuardia Airport instead detained the bag for ninety minutes while bringing over a detection dog from nearby Kennedy Airport.²³¹ The dog reacted positively to the luggage, thus providing the probable cause needed to secure a warrant to search the suitcase.²³²

The *Place* Court unanimously held the search to be illegal, reasoning that the ninety-minute wait Place had had to endure was unreasonably long.²³³ However, in dicta endorsed by six of

²²⁶ See *supra* p. 50.

²²⁷ *Id.*

²²⁸ *Id.*

²²⁹ See *supra* p. 51.

²³⁰ 462 U.S. 696 (1983).

²³¹ *Id.* at 698-99.

²³² See *id.* at 699.

²³³ See *id.* at 709-10.

its nine members,²³⁴ the Court also stated that dog sniffs in the absence of even reasonable suspicion do not offend the Fourth Amendment since they do not implicate an individual's reasonable expectation of privacy.²³⁵ The Court assumed that a sniff by a well-trained dog offers a highly accurate way of determining the presence of narcotics in a concealed space.²³⁶ Drawing on this assumption, it stated that a "sniff discloses *only* the presence or absence of narcotics, a contraband item."²³⁷ Because no one can have a privacy interest in contraband and because the Court assumed that sniffs by well-trained dogs accurately detect narcotics and narcotics only, such sniffs were held to have no implications for Fourth Amendment privacy interests.

Provided we accept the Court's premise about the accuracy of dog sniffs, the Court's conclusion is sound. Needless to say, the premise is open to serious challenge given the fact that even trained dogs sometimes do produce false positives.²³⁸ But even if the Court's specific premise is set aside, one can still defend a more abstract principle arising out of *Place*—i.e., that all devices which detect a certain type of contraband *and only that type of contraband* are acceptable under the Fourth Amendment. Even

²³⁴ Three justices—Blackmun, Brennan, and Marshall—declined to join the Court's opinion. In two separate opinions, Justices Blackmun and Brennan noted that it was unnecessary for the Court to consider the constitutionality of dog sniffs under the Fourth Amendment given the holding that the police violated *Place*'s Fourth Amendment rights in holding his luggage for 90 minutes. 462 U.S. at 710-24.. Concurring in the judgment of the *Place* Court, Justice Blackmun faulted the majority for resolving the question of whether a dog sniff implicates a privacy interest. *See id.* at 723.

²³⁵ *Id.* at 707.

²³⁶ *Id.*

²³⁷ *Id.* at 707 (emphasis added).

²³⁸ *See Doe v. Renfrew*, 475 F.Supp. 1012 (N.D. Ind. 1979). Four years prior to *Place*, for example, the Northern District of Indiana considered a case in which a trained dog reacted positively to a teen-age girl while a dog sniff inspection was being conducted in the girl's school. *See id.* at 1017-18. The dog continued to react positively even after the girl emptied the contents of her pockets. *See id.* at 1024. The girl was then required to remove all her clothes and submit to a search by two women. *See id.* The search produced no evidence of contraband, and the court noted the possibility that a dog may be responding not to contraband on a suspect but rather to the odor of contraband on the suspect's clothes. *Id.* Note also the possibility that a trained dog will react positively to luggage that previously carried marijuana but that does not at the time of the sniff. If, for example, A, who has used a piece of luggage to carry marijuana, sells the luggage to B, who packs it and flies on an airplane, a trained dog might react positively to the traces of marijuana despite the fact that none is presently contained in the luggage.

this principle is subject to a collateral criticism, for a foolproof device can have humiliating side effects, a point noted by critics of dog sniffs.²³⁹

Some detection devices have no such side-effects, however—or at least none except those brought about either by wrongdoing or carelessness. Think, for example, about the clasps department stores place on unpurchased merchandise or the computerized signals libraries use for books that have not been checked out. Assuming these do not produce false positives, no one can claim a privacy interest is violated when such a device sounds an alarm. A somewhat more complicated calculus is needed for gun detectors because people licensed to carry concealed weapons have a legitimate privacy interest in not revealing them. But provided a detector can be devised that identifies only those concealed weapons people have *not* been licensed to carry, this too would not implicate Fourth Amendment privacy interests.²⁴⁰

Place, of course, deals only with *methods* of intrusion.²⁴¹ What about the larger question of whether one can tell in advance, *regardless of the method* of intrusion to be followed, that no privacy interest will be affected by interference with an arrangement designed to avoid exposure to the public? The Court has sedulously avoided this question, yet it is inescapable once one understands that concealment is an over-inclusive category as far as privacy is concerned. Card games have served as our initial guide on this point. It is easy to provide other examples, though; indeed, corporations and governments routinely rely on concealment strategies for matters that have nothing to do with personal vulnerability. I shall concentrate in a moment on corporations, but it would also be helpful to consider government efforts to ensure concealment.

²³⁹ See *United States v. Place* 462 U.S. 696, 721-22 (1983) (Brennan, J., concurring) (“A dog adds a new and previously unobtainable dimension to human perception. The use of dogs . . . represents a greater intrusion into an individual’s privacy” than does an electronic detection device.).

²⁴⁰ See Arnold Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 U. MICH. L. REV. 1229, 1248 (1983) (“[I]f a device could be invented that accurately detected weapons and did not disrupt the normal movement of people, there could be no Fourth Amendment objection to its use.”) For the reasons advanced in the text, this standard is too weak. The device would have to distinguish between concealed weapons people are licensed to carry and those they are not licensed to carry. See *id.*

²⁴¹ That is, *Place* is concerned with the legality of dog sniffs.

Governments, of course, have national security interests in concealment. The very term "national security," however, reminds us that one would make a conceptual error if one were to speak of a government as having a privacy interest in, say, its military capabilities or its diplomatic initiatives. These are matters wholly unrelated to personal vulnerability. The terms applied to them include "Top Secret," "Secret," and "Confidential"—but not "private."²⁴² And of course, national security is an area in which expectations of vigilance rather than forbearance prevail. Governments must exercise extreme care to make sure their national security secrets remain well-concealed.

Similar points can be made about corporations. While the term "privacy" is simply not used in everyday corporate speech, corporate terminology does include the phrases "trade secrets," "proprietary information," and "strategic planning." Ignoring these road signs from everyday language, the Court, on the other hand, has consistently reasoned in terms of corporate and commercial *privacy*.²⁴³ Moreover, it has done so while reviewing settings in which it was clear *prior* to the inspections carried out by government agents that those agents would look over commercial and manufacturing operations but wouldn't encounter anything remotely related to personal vulnerability.²⁴⁴ For example, in *Dow Chemical v. United States*, the Court was concerned with the aerial surveillance of a chemical plant, an activity with implications for corporate and financial, but not for personal, vulnerability.²⁴⁵ Chief Justice Burger, however, stated in his opinion for the Court that "Dow plainly [had] a reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings."²⁴⁶ Furthermore, in an embarrassing appropriation of the rhetoric of personal relationships, Burger even went on to discuss the possibility that government surveillance of Dow's plant would reveal "intimate details" of Dow's plant.²⁴⁷ In *Marshall v. Barlow's Inc.*, where a

²⁴² See Executive Order No. 12356, 47 F.R. 14874, 15557 (April 2, 1982) (reprinted in supplement to 50 U.S.C. Sect. 401) (setting out classifications for national security information "Top Secret," "Secret," and "Confidential").

²⁴³ See *infra* notes 245-54 and accompanying text.

²⁴⁴ *Id.*

²⁴⁵ See 476 U.S. 227, 229-30 (1986).

²⁴⁶ *Id.* at 236.

²⁴⁷ See *id.* at 238.

company had challenged an on-site factory inspection, the Court reasoned in terms of an owner's expectation of privacy in business premises regularly used by employees but not open to the public.²⁴⁸ And in *United States v. Biswell*, a 1972 case, the Court even spoke of a gun dealer's "justifiable expectations of privacy" in the contents of his shop.²⁴⁹

What accounts for this strange pairing of privacy and corporations, and how can Fourth Amendment doctrine be set straight? The answer to the first question is to be found in the influence of *Katz v. United States* on Fourth Amendment jurisprudence. Long before *Katz* was decided, the Court had held that, although the Fifth Amendment's self-incrimination clause applies only to individuals, the Fourth Amendment applies to corporations as well as persons.²⁵⁰ *Katz* of course should have occasioned a judicial reappraisal of possible beneficiaries of the Fourth Amendment.²⁵¹ But since the Court has failed to acknowledge privacy's role in the protection of personhood, it has also, not surprisingly, failed to note the inappropriateness of its invocation of privacy in cases involving corporate concealment. We can call this a one-size-fits-all approach to constitutional decision-making. Once the Court established privacy as a critical concept in Fourth Amendment jurisprudence, it mechanically applied the term to corporations seeking the Amendment's protection.²⁵²

How, then, should Fourth Amendment doctrine be set straight? The first step, of course, is to recognize the inappropriateness of references to privacy in this context. Not every concealment strategy has a connection to privacy. Because an outsider (an EPA inspector, for example) will be in a position to determine in advance that no privacy interest is

²⁴⁸ See 436 U.S. 307, 315 (1978).

²⁴⁹ 406 U.S. 311, 316 (1972).

²⁵⁰ See *Hale v. Henkel*, 201 U.S. 43, 75-77 (1906).

²⁵¹ See *Katz*, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.") As noted earlier, however, the Stewart opinion avoided systematic analysis of privacy issues; it certainly did not investigate the connection between privacy and personhood. See *supra* notes 173-74 and accompanying text.

²⁵² The first post-*Katz* case in which the Court applied privacy analysis to a corporation is *Marshall v. Barlow's Inc.*, 436 U.S. 307 (1978). Subsequent cases include *Donovan v. Dewey*, 453 U.S. 594 (1981) and *United States v. Dow Chemical*, 476 U.S. 227 (1986). There appears to have been no occasion in which any member of the Court has questioned the appropriateness of applying the concept of privacy to corporations.

likely to be implicated by his activity, references to the oxymoronic phrase "corporate privacy" should disappear from the judicial lexicon. The second step must be to ask about Fourth Amendment property protection for corporate concealment strategies. In some settings, even property protection is irrelevant; in others, it remains so. Let us pursue this property-based inquiry at greater length.

If government officials never enter corporate property but simply subject it to surveillance from the outsider, then the Fourth Amendment offers no protection at all to the corporation subject to scrutiny. In this limited respect, it is appropriate to reason in terms of a variation on the *Olmstead* rule—that is, to hold in settings *where privacy cannot be at stake* that interfering with property interests by trespassing is a prerequisite to Fourth Amendment liability.²⁵³ Under this analysis, the proper resolution of *Dow Chemical* would have been for the Court to reject Dow's claims completely. The only surveillance the company complained of in the case involved an overhead flight of its Midland, Michigan plant by EPA officials trying to discover violations of the agency's standards. This was a quest for information of course, but not a quest for information with any bearing on personal vulnerability. Moreover, while Dow could properly complain on common law and statutory grounds about rival corporations trying to discover its trade secrets, it could not advance such a complaint about EPA overflight inspections since EPA officials do not engage in such inspections as part of a government effort to compete with corporations.²⁵⁴

Thus, no argument Dow might advance could secure Fourth Amendment protection. First, as a corporation, Dow could have no privacy interest in the contents of its plant. Second, although Dow could properly claim that it had a proprietary interest in information about its manufacturing procedures, it could not claim that the government was interfering with this interest in conducting overflights of its plants since the government was not trying to appropriate the information for its own use. And third, since no government

²⁵³ See *Olmstead v. United States*, 277 U.S. 438 (1928).

²⁵⁴ See *Dow Chemical*, 476 U.S. 227, 231-32 (1986) ("Governments do not generally seek to appropriate trade secrets of the private sector, and the right to be free of appropriation of trade secrets is protected by law.")

official actually entered Dow's plant, Dow could not complain about government interference with its property interest in exercising control over its real estate and equipment.

By contrast, when government inspectors actually enter a corporation's premises, the corporation can properly point to "meaningful [government] interference with a possessory interest."²⁵⁵ Thus, in *Marshall v. Barlow's Inc.*, where OSHA inspectors sought access to the corporation's work area, the corporation was clearly able to complain about interference with the use it wished to make of its facilities.²⁵⁶ Similarly, in *Donovan v. Dewey*,²⁵⁷ when federal inspectors sought entry to the Waukesha Lime and Stone Company's mines,²⁵⁸ the company could, under the theory advanced here, have sought judicial protection against government interference with its property interests. Corporations are property holders, after all, so courts must consider their property interests when assessing the permissibility of inspections of their premises.

But what about family shops and stores, where living quarters can shade imperceptibly into commercial premises? And what about closely held corporations in which all shareholders and employees are members of the same family? Boundary problems of this kind are inevitable once we agree that not every concealment strategy has implications for privacy. The best approach in gray area settings, I suggest, is to err on the side of caution. If there is even some reason for an outsider to believe that a concealment arrangement might protect personal matters from unwanted exposure, then an outsider should proceed on the assumption that a privacy interest is at stake. Thus, if it seems possible, when standing on the threshold of the back room of a family-run shop where the

²⁵⁵ See *Jacobsen v. United States*, 466 U.S. 109, 113 (1984).

²⁵⁶ See 436 U.S. 307, 314 (1978) ("The critical fact in this case is that entry [into the premises of Barlow's Inc.] over Mr. Barlow's objection is being sought by a Government agent.")

²⁵⁷ See 452 U.S. 594 (1981). Whether it could have sought protection against warrantless inspection of its premises is another matter. *Barlow's* and *Dewey* hinge on the question of whether warrants are required for inspection of regulated industries. *Id.* at 604-05. The Court treats the extent to which a type of business activity is subject to public regulation as the decisive factor in determining whether a warrant is required prior to entering the premises of a corporation. *Id.* As the *Dewey* Court noted, even when a warrant is not required prior to entry, a corporation still enjoys Fourth Amendment rights. *Id.*

²⁵⁸ *Id.* at 597.

room contains items of personal use as well as the store's inventory and records, a government inspector should exercise the restraint appropriate in settings where personal vulnerability might be at stake and so, absent exigent circumstances, seek a warrant prior to searching.²⁵⁹ The points just made about corporations are simply the converse of this: they apply in settings where an outsider can tell, without penetrating concealment arrangements, that privacy is *highly unlikely* to be at stake.

B. OBSERVATIONAL SURVEILLANCE

Now let us turn to the longer list of settings in which the Court has spurned legitimate privacy claims. For purposes of analysis, we should distinguish between two kinds of surveillance—observational and interactive—that can interfere with privacy. When engaged in observational surveillance, government agents passively scrutinize the behavior of others—they report on what is occurring but try not to affect the conduct they are observing.²⁶⁰ By contrast, when engaged in interactive surveillance, agents actually intervene in human relationships: on some occasions, they operate undercover; on others, they reveal their identity and try to persuade an insider to betray another.²⁶¹ I begin by considering settings involving observational surveillance. Later, I turn to interactive surveillance.

²⁵⁹ This is perhaps best characterized as a prophylactic rule for privacy. The constitutional status of prophylactic rules for police interrogation has been the subject of considerable debate. Compare, e.g., Joseph Grano, *Prophylactic Rules in Criminal Procedure: A Question of Article III Legitimacy*, 80 NW. U. L. REV. 100 (1985), with David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190 (1988). There is no need, however, to engage in a similar debate about Fourth Amendment prophylaxis. Everyday expectations of privacy are grounded in a prophylactic framework—that is, forbearance is required in settings where personal vulnerability *might be* at stake. See *supra* notes 172-73 and accompanying text. Thus if there is a possibility that privacy might be at stake when conducting an inspection of, say, the back room of a family store, then everyday expectations require government agents to exercise the restraint appropriate for privacy when carrying out their inspection.

²⁶⁰ See RICHARD H. WARD, INTRODUCTION TO CRIMINAL INVESTIGATION 207 (1975) (“Surveillance is the observation of a person, place, or thing, usually surreptitiously.”).

²⁶¹ *Id.* at 205 (“[A]n undercover operative is a law enforcement agent who attempts to develop the confidence of an individual or to infiltrate a group or operation for the purpose of developing information concerning criminal activity.”).

1. *Private Objects and Information*

When conducting observational surveillance, government officials engage in sustained scrutiny of one or more individuals.²⁶² In doing so, agents attempt to avoid influencing the behavior of those they are scrutinizing.²⁶³ Indeed, a central aim of people conducting observational surveillance is to become part of the background—to stand outside the subject and compile information about his activities without making him aware of the surveillance.²⁶⁴ It is arguable that sustained scrutiny of this kind almost invariably interferes with privacy interests. At the very least, though, it is clear that observational surveillance interferes with privacy when the focus of an individual's attention is a private object or information.

The term “peeping Tom” provides a helpful way to illustrate this point. To classify someone as a “peeping Tom” is to say that the person has engaged in sustained, nonconsensual scrutiny of something viewed as intrinsically private. It doesn't matter that a peeping Tom stands in a place he is lawfully entitled to occupy. Someone isn't any less subject to condemnation if, for example, he stands in the public area of a restroom and stares through the slits of closed stalls. Rather, what is critical to such settings is that the person doing the observing has not respected what we may call the “principle of ancillary privacy.” This principle holds that given conventional understandings that certain objects are private—the naked body, for example, or the contents of bedrooms—then sustained, nonconsensual scrutiny of those objects even from a public place amounts to an interference with privacy interests. Needless to say, it is drawn-out scrutiny that is condemned on such occasions. No one is called a “peeping Tom” if, by chance, he notices—but then turns away from—a private object.²⁶⁵

²⁶² *Id.* at 208.

²⁶³ *Id.* at 207.

²⁶⁴ *Id.*

²⁶⁵ See 7 OXFORD ENGLISH DICTIONARY 615 (1933). Citing an 1837 publication concerning Lady Godiva, the Dictionary reports: “The story [of Godiva] is embellished with the incident of Peeping Tom, a prying inquisitive tailor who was struck blind for popping out his head as the lady passed.” *Id.* The tailor, it should be noted, was staring at someone who was traveling through a public thoroughfare. *Id.* His transgression was not that he was in a place he was not supposed to occupy; rather, it was that he subjected private facts—Godiva's naked body—to sustained scrutiny. *Id.*

The principle of ancillary privacy can be applied in settings beyond the lurid ones at stake in peeping Tom cases. For example, if (as the *Katz* Court held) a telephone call is a private activity, then outsiders can reasonably be expected to exercise restraint not simply about the contents of phone conversations but also about their incidental features, such as the pattern of someone's calls. Similarly, given the respect due the contents of first-class mail, privacy interests are also implicated if someone scrutinizes another person's pattern of correspondence by examining the addresses and return addresses on his envelopes. And given the respect due the home, privacy is certainly implicated if someone tries to peer through open windows to see what's going on. Needless to say, the expectations associated with ancillary privacy are more relaxed than those associated with full privacy. As was made clear in the peeping Tom example, it is systematic scrutiny that is unacceptable, not the inadvertent, passing glance. People occasionally notice addresses on envelopes or the contents of a room when a window has been left open. This can readily be distinguished, however, from a full-blown, deliberate inspection.

The Court, as one would expect, has consistently rejected the principle of ancillary privacy. On the Court's analysis, private objects have no penumbra, no outer area in which a modest degree of restraint is needed in order to support the object's function in securing privacy. The conclusions reached in *Smith v. Maryland* provide a chilling illustration of this point.²⁶⁶ At issue in *Smith* was the ability of the police to use a pen register, a device that provides information about the pattern of calls from a given telephone.²⁶⁷ The pen register had been installed at police request on a phone in Smith's home, with no warrant having been obtained prior to installation.²⁶⁸ Because *Katz* had recognized the telephone's role in protecting personal communication,²⁶⁹ the *Smith* Court had a particularly strong reason to consider a caller's ancillary privacy interest in the pattern of calls he makes.²⁷⁰ Instead, Justice Blackmun, writing for the Court, held that pen registers don't implicate

²⁶⁶ 442 U.S. 735 (1979).

²⁶⁷ *Id.* at 737.

²⁶⁸ *Id.*

²⁶⁹ See 389 U.S. 347, 351-53 (1967).

²⁷⁰ Indeed, Justice Blackmun's opinion in *Smith* defined the issue in light of *Katz*. See 442 U.S. at 739-42.

objectively reasonable privacy expectations because phone company customers "assume the risk" that the company will reveal their pattern of calls to the police.²⁷¹ Blackmun, it should be noted, could not claim that customers assume the risk that the company will reveal their pattern of calls to the public-at-large. This claim would clearly be false. Rather, essential to Blackmun's argument was the proposition that a customer's reliance on a third-party facilitator—even on one who would not be willing to divulge information to the public-at-large—robs that customer of any expectation of privacy with respect to the police.²⁷²

So stated, the *Smith* Court's conclusions seem particularly questionable. Members of the public can sometimes act as snoops when checking on the pattern of someone's incoming and outgoing mail and can always act as snoops by looking from sidewalks into the open windows of other people's homes. However, they can never gain access to the pattern of someone's phone calls from her home because phone companies would flatly refuse to reveal such information.²⁷³ But this of course isn't all that's wrong with *Smith*. The general principle at stake in the case is respect for ancillary privacy, and this principle extends far beyond pen registers.

The proper way to approach ancillary privacy issues is to say that they raise less serious questions about forbearance than do the private objects with which they're concerned. A standard lower than probable cause (reasonable suspicion, for example) can justify interference with ancillary privacy. Ironically, the government could, in all likelihood, have satisfied this standard in *Smith*. At the time it requested the pen register, the Baltimore Police Department had already accumulated a good deal of information indicating that the defendant was making threatening phone calls to the victim.²⁷⁴ That the Court failed to remand the case with instructions to employ the reasonable suspicion (a remand that would almost certainly have still made it possible for the government to prevail) shows just how deeply committed it is to the vigilance model.

²⁷¹ *Id.* at 744.

²⁷² *Id.* at 744-46.

²⁷³ A telephone call to Verizon Communications on Apr. 5, 2002 confirmed this point.

²⁷⁴ *See* 442 U.S. at 737.

Questions about ancillary privacy arise in settings where the Court has recognized the private status of an object or information. But what if the Court has simply refused to accord an object its proper status? Two examples—one involving judicial refusal to treat a (mobile) home as a home, the other a refusal to recognize the private status of bank records—illustrate how stingy the Court has been in classifying objects as private. The first shows the Court working at the margins, making a concerted, and implausible, effort to lessen the protection available for one type of residence.²⁷⁵ The second shows the Court denying the obvious—denying that bank records are conventionally treated as private.²⁷⁶

Consider first the Court's approach to mobile homes. By the time it reached the issue of mobile motor homes in *California v. Carney*,²⁷⁷ the Court had already concluded that people have a modest privacy interest in cars—an interest that requires probable cause in order to justify a full-scale search but an interest insufficiently strong as to require a warrant prior to commencement of the search.²⁷⁸ Also, in case law prior to *Carney*, the Court had consistently accorded substantial privacy protection to homes, requiring a warrant for searches of a home unless exigent circumstances justify dispensing with one.²⁷⁹ The issue in *Carney* was thus one of classification—whether to think about searches of mobile motor homes in light of the warrant requirement that prevails for stationary homes or to think about them in light of the more relaxed requirement that prevails for cars.²⁸⁰

That the Court opted for the latter alternative should hardly occasion surprise given its record on privacy issues. The critical

²⁷⁵ See *California v. Carney*, 471 U.S. 386 (1985).

²⁷⁶ See *United States v. Miller*, 425 U.S. 435 (1976).

²⁷⁷ 471 U.S. 386 (1985).

²⁷⁸ See *Carroll v. United States*, 267 U.S. 132 (1925); see also *United States v. Ross*, 456 U.S. 798 (1982).

²⁷⁹ See *Payton v. New York*, 445 U.S. 573, 589 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of the home."); see also *United States v. Karo*, 468 U.S. 705, 714-15 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of government intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.")

²⁸⁰ 471 U.S. at 393-94.

question, of course, is whether one can provide an argument that improves on its Khadi-style methodology for pronouncing on society's privacy expectations. The answer is that one surely can by relying on the Court's own conclusions in other cases. The question posed by *Carney* has to do with the privacy expectations associated with temporary "homes."²⁸¹ Prior to *Carney*, the Court had addressed this issue in *Stoner v. California*, where it held that a warrant is required to search a hotel room.²⁸² Five years after *Carney*, it considered a related question when it held in *Minnesota v. Olson* that overnight guests in someone else's home have an expectation of privacy in the premises they occupy, thus making it essential that government officials obtain a warrant before searching those premises.²⁸³

Viewed in light of the Court's holdings in *Stoner* and *Olson*, *Carney*'s conclusion is anomalous, then. The Court has recognized substantial privacy expectations for home-substitutes such as hotel rooms and spare rooms for overnight guests.²⁸⁴ The Court's denial of a similar level of seriousness for mobile motor homes is particularly troubling since such a home sometimes functions not simply as a home-substitute on the road but as a full-time home.²⁸⁵ A careful examination of the Court's opinion in *Olson* reveals why it overlooked this analogy. In *Olson*, Justice White, writing for the Court, repeatedly referred to what "we" feel as overnight guests in other people's homes. "We stay in others' homes when *we* travel for business or pleasure," White stated, "when *we* visit our parents, children, or relatives out of town, when *we* are in between jobs or homes, or when *we* house-sit for a friend."²⁸⁶ In one of the rare references to personal vulnerability in a Supreme Court privacy opinion, White remarked: "We are at our most vulnerable when *we* are asleep" in someone else's home.²⁸⁷

By contrast, one finds no references to "we" in *Carney*'s opinion about mobile motor homes. This is a temporary residence arrangement wholly unfamiliar to Supreme Court

²⁸¹ *Id.* at 387.

²⁸² 376 U.S. 483, 490 (1964).

²⁸³ 495 U.S. 91, 100 (1990).

²⁸⁴ See notes 183-84 *supra* and accompanying text.

²⁸⁵ This point is made in Justice Stevens's *Carney* dissent. See 471 U.S. at 399 and n.9.

²⁸⁶ *Olson*, 495 U.S. at 98 (emphasis added).

²⁸⁷ *Id.* at 99 (emphasis added).

justices.²⁸⁸ It is an arrangement used primarily by economically and socially marginal members of society, by people who also “travel for business or pleasure” but do so under circumstances constrained by financial need.²⁸⁹ It is hardly surprising, then, that the analogy to other types of homes was not advanced in *Carney*. The Court’s method of discerning privacy expectations begins, and ends, with the experience of the affluent.²⁹⁰

Finally, let us consider an absolute devaluation of privacy—a claim that certain objects are not conventionally deemed private at all. In *United States v. Miller*, decided in 1976, the Court concluded that bank customers have no expectation of privacy in the papers, such as deposit slips, they fill out when conducting transactions with their banks.²⁹¹ Relying on assumption of risk analysis, the *Miller* Court concluded that in undertaking transactions with third parties, people assume the risk that the information they provide will ultimately be “conveyed . . . to Government authorities.”²⁹² In *Miller*, information about the defendant’s banking transactions wasn’t, of course, *voluntarily* conveyed to the government. Rather, the defendant’s bank was served with a subpoena *duces tecum* concerning the transactions.²⁹³ The *Miller* Court sidestepped this point. Because the possibility existed that the defendant’s deposit slips might be (involuntarily) conveyed to the government by the bank, the defendant, the Court held, could not claim an expectation of privacy in them.²⁹⁴

²⁸⁸ Justice Douglas retired from the Court more than a decade before *Carney* was decided. He proudly recounted his use of an early twentieth century analogue to the trailer home in his memoir when he told how he had ridden a freight car from Yakima, Washington to New York City to enroll at Columbia Law School. WILLIAM O. DOUGLAS, *GO EAST YOUNG MAN* 127-33 (1974).

²⁸⁹ *Id.*

²⁹⁰ Once Douglas had become (moderately) affluent following his appointment to the Supreme Court, he told Chief Justice Harlan Fiske Stone, who had been a Dean of the Columbia Law School, about how he had arrived in New York. Stone asked whose railroad freight cars Douglas had used. When Douglas replied that he had slept mostly in Great Northern cars, Stone replied, “Then you should always ride the Great Northern, paying first class fares. Come to think of it, why not send them a check for your Law School transportation?” *Id.* at 135.

²⁹¹ See 425 U.S. 435 (1976).

²⁹² *Id.* at 443.

²⁹³ *Id.* at 437-38.

²⁹⁴ *Id.* at 443 (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”).

The difficulty with this account is that it fails to take note of the complex set of reliance interests underlying banking transactions. Banks are physically arranged so as to make it possible for customers to avoid broadcasting to the public-at-large the nature of their transactions. Tellers' cages are constructed so that a customer can turn her back to the queue and carry out her business. Automatic teller machines envelop a customer, creating barriers to snoops in the rear who might want to find out about the customer's transactions. And, most important, banks do not provide members of the public-at-large with information about their customers; indeed, no bank could stay in business if it did so. Customers thus *rely on* their banks to keep financial information private.

On the *Miller* Court's account, this consistent pattern of confidentiality vis-à-vis that public-at-large counts for nothing in the calculation of privacy interests given the government's subpoena power over banks. But this approach wholly undercuts the reasonable expectations test. The test's central premise is that the government must operate according to the expectations that prevail among the public-at-large.²⁹⁵ There can be no doubt, given the precautionary measures undertaken by banks, that each person's finances are deemed private. *Miller* rejects this obvious conclusion by focusing on ways in which the government exercises special power unavailable to members of the lay public.

2. *Privacy Cues*

When social conventions do not treat an object as private, privacy cues become particularly important as a way of indicating an interest in privacy. The Court has examined numerous settings in which cues have been critical. In each instance, however, the Court has mentioned the cues employed only to disregard their significance in reaching its conclusions. I begin by considering settings in which people signaled an interest in the privacy of their backyards. Later, I turn to police inspection of garbage.

²⁹⁵ See *Marshall v. Barlow's Inc.*, 436 U.S. 307, 315 (1978): "Without a warrant, [a government official] stands in no better position than a member of the public. What is observable by the public is observable, without a warrant, by the Government inspector as well." See also *California v. Ciraolo*, 476 U.S. 207, 213-14 (1986).

Two post-*Katz* cases consider warrantless aerial surveillance of backyards. In *California v. Ciraolo*, decided in 1986, the Court held such surveillance constitutional when conducted from an airplane one thousand feet in the air.²⁹⁶ *Florida v. Riley*, decided three years later, produced only a judgment of the Court, one that upheld warrantless surveillance conducted from a helicopter hovering four hundred feet above a yard.²⁹⁷ Although the difference in the height of the surveilling aircraft is significant, it is the similarity in the owners' use of privacy cues that is particularly striking. Ciraolo enclosed the backyard of his suburban home with high double fences.²⁹⁸ In looking at the property from the street, passersby first encountered a six-foot outer fence and then saw a ten-foot inner one, the effect being to close off the property completely from street-level view.²⁹⁹ Riley was even more thorough. He posted a "DO NOT ENTER" sign on his backyard and had enclosed two sides of a greenhouse located in his backyard.³⁰⁰ Trees and shrubs surrounded the other two sides of the greenhouse and thereby cut off the view of the back yard from the street.³⁰¹ Riley also placed corrugated roofing over most of the top of the greenhouse, with only two panels missing at the time the police carried out their surveillance.³⁰² Given the narrowness of the greenhouse's rooftop opening, a helicopter was needed to hover at a low altitude in order to peer into it.³⁰³

By the time *Ciraolo* was decided, the Court had declared that the curtilage surrounding the home must be "considered part of the home itself for Fourth Amendment purposes."³⁰⁴ Because there is no doubt that Ciraolo's backyard and Riley's greenhouse lay within the curtilage of their homes, each case could be classified as one of ancillary privacy in which there were *also* unmistakable cues indicating an interest in privacy.³⁰⁵ This analysis, which is clearly sound, makes the *Ciraolo* and *Riley*

²⁹⁶ See 476 U.S. 207, 215 (1986).

²⁹⁷ See 488 U.S. 445, 450-52 (1989).

²⁹⁸ See *Ciraolo*, 476 U.S. at 209.

²⁹⁹ *Id.* at 211.

³⁰⁰ See *Riley*, 488 U.S. at 448.

³⁰¹ *Id.*

³⁰² *Id.*

³⁰³ *Id.*

³⁰⁴ *Oliver v. United States*, 466 U.S. 170, 180 (1984).

³⁰⁵ For discussion of the concept of ancillary privacy, see notes 266-66 *supra* and accompanying text.

conclusions—that neither defendant had an objectively reasonable privacy interest in the contents of his backyard—patently untenable. There is no point, however, in considering the cases from this perspective, for it is clear that no member of either the *Ciraolo* or *Riley* majorities accorded any special significance to the private status of the curtilage.³⁰⁶ Rather, the *Ciraolo* majority and *Riley* plurality reasoned in terms of the plain view doctrine.³⁰⁷ Because the officers in each case were in a position they were lawfully entitled to occupy and because they observed matters that were in plain view once they had taken their positions, their surveillance, the justices reasoned, interfered with no privacy interests whatsoever. In each case, the Court concluded that the Plain View Doctrine settled the matter—there is no privacy protection for what can be seen from a public place.

So much, then, for the special status of the curtilage. But even if considerations about the curtilage are set aside, one still must ask about the respect due privacy cues. This question is particularly relevant to *Ciraolo* and *Riley*, for a majority of the justices in both cases conceded that in each case the officers were aware of the privacy cues *before* undertaking aerial surveillance.³⁰⁸ The Court deemed this point irrelevant, however. The cues indicated that each defendant had a *subjective* expectation of privacy, the justices reasoned, but they did not establish the further point that the defendants'

³⁰⁶ Thus the significance of the following remark in *Ciraolo*: "That the area [observed] is within the curtilage does not itself bar all police observation." 476 U.S. at 213.

³⁰⁷ See *Ciraolo*: "Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed." *Id.* at 213-14; *Riley*: "Because the sides and roof of his [Riley's] greenhouse were left partially open, . . . what was growing in the greenhouse was subject to viewing from the air" by those within navigable airspace. 488 U.S. at 450 (White, J., plurality opinion).

³⁰⁸ See *Ciraolo*, 476 U.S. at 209 ("Police were unable to observe the contents of respondent's yard from ground level because of a 6-foot outer fence and a 10-foot inner fence completely enclosing the yard. Later that day, Officer Shutz, who was assigned to investigate secured a private plane and flew over respondent's house at an altitude of 1000 feet, within navigable airspace; he was accompanied by Officer Rodriguez."); see also *Florida v. Riley*, 488 U.S. 445, 448 (1989) (White, J., plurality opinion) ("When an investigating officer discovered that he could not see the contents of the greenhouse from the road [because of the protective measures Riley had taken to shield it from the glances of passersby on the ground], he circled twice over respondent's property in a helicopter at a height of 400 feet."); *Riley*, 488 U.S. at 452 (O'Connor, J., concurring) (accepting the factual outline provided in Justice White's plurality opinion).

expectations were objectively reasonable.³⁰⁹ On the contrary, the justices concluded in each case that the defendants' privacy cues did nothing to establish an objectively reasonable privacy expectation.³¹⁰ Under *Ciraolo* and *Riley*, a person acts consistently with everyday understandings of privacy if he disregards unmistakable signs that someone wants privacy for his backyard, hires an aircraft to fly over the yard, and then takes pictures of the yard to provide a detailed inventory of its contents.

If the source of this proposition were not the Supreme Court, one might simply laugh at it as a "snoop's" version (a *very rich* "snoop") of privacy. Given the source, however, one must take it seriously. In assessing the Court's position, think first about what would happen to the system of privacy if cues were systematically disregarded—if, for example, the markings "Personal and Confidential" were taken as an invitation to hold an envelope up to the light to inspect its contents, or if the fact that someone closed a door before beginning a conference were taken as an incitement to outsiders to cup their ears against the door. These circumvention techniques meet the criteria established in *Ciraolo* and *Riley*. They involve nothing more than an effort, undertaken by people in places they are lawfully entitled to occupy, to sidestep unmistakable signals indicating an interest in privacy.

But these are, of course, the techniques of the snoop. Courts must reject such techniques if privacy conventions are to serve as the basis of the law. Once someone has signaled an interest in privacy by cutting off the straightforward ways in which people are likely to come upon an object, the burden shifts to outsiders to honor these signals by *not* looking for techniques of circumvention. Police officers having discovered

³⁰⁹ See *Ciraolo*, 476 U.S. at 211 ("Clearly—and understandably—respondent has met the test of manifesting his own subjective intent an desire to maintain his privacy"; see also *Riley*, 488 U.S. at 450 (White, J., plurality opinion); *Riley*, 488 at 454 (O'Connor, J., concurring) ("Individuals who see privacy can take precautions, tailored to the location of the road, to avoid disclosing private activities to those who pass by.").

³¹⁰ *Ciraolo* recognized that the defendant had, through his construction of double fences for his backyard, manifested a subjective expectation. 476 U.S. at 211. But it held that *Ciraolo* had no objective expectation of privacy vis a vis aerial surveillance from 1000 feet. *Id.* at 215. The *Riley* plurality also recognized that the defendant in the case had demonstrated a subjective privacy expectation. 488 U.S. at 450. But it too held that the defendant did not have an objective expectation. *Id.* at 451-52.

that *Ciraolo* and *Riley* had signaled an interest in privacy bore the burden of securing by other means the requisite level of suspicion about the backyards. Any other ruling is incompatible with everyday understandings of privacy.³¹¹

The same line of reasoning should be followed when considering settings in which the police scrutinize activities in the home from street vantage points. Home-dwellers often use blinds, shades, or curtains to prevent scrutiny by outsiders. But what if there is a gap in, say, someone's window blinds that makes it possible for an outsider to peer into the person's home provided he positions himself in just the right way outside the window? Given privacy conventions, the answer to this is straightforward: blinds function as a cue, one that outsiders are expected to honor rather than circumvent. Not surprisingly, the Court has ignored this convention—or, at least, it has done so with respect to *guests* in a home. In *Minnesota v. Carter*, the Court concluded that short-term guests cannot claim a privacy interest from outsider surveillance of their behavior within a home.³¹² Indeed, given *Carter's* facts, the conclusion was more stark: that short-term guests have no privacy interest in being free of surveillance when a police officer climbs over bushes partially obscuring a ground-floor window, places his face twelve to eighteen inches from the window, and peers for fifteen

³¹¹ But what if the police are unaware of the privacy cues? For example, what if a police officer on routine aerial patrol were simply to notice the contents of someone's backyard without having encountered any street-level cues signaling an interest in privacy for that yard? The answer to this is that the officer's discovery cannot be said to have violated a privacy interest. Privacy conventions allow for a distinction between casual glances and systematic scrutiny. Police officers on foot patrol sometimes happen upon objects that provide probable cause for further investigation—and the same is possible when officers conduct aerial patrol of, say, a city's highways. But this, of course, is a principle that depends on happenstance and chronology. In enforcing it, courts must guard against pretextual searches by insisting that officers demonstrate their discoveries were made in the course of routine patrols. The Court, it should be noted, has blurred the distinction between casually noticing objects and seeking them out. In *Ciraolo*, for example, it even went so far as to state that "[T]he Fourth Amendment protection of the home has never been extended to require law enforcement to shield their eyes when passing by a home on public thoroughfares." 476 U.S. 207, 213 (1986). But this statement was disingenuous given the facts of the case. It's true, of course, that an officer on aerial patrol *might have* noticed the contents of *Ciraolo's* yard. In fact, though, the officer expended great effort to find out about its contents. In the gap between these two extremes lies the difference between everyday privacy conventions and the Court's distortion of them.

³¹² 525 U.S. 83, 91 (1998).

minutes through a small gap in the blinds drawn over the window.³¹³

Had there been anything in the record to indicate that the officer in *Carter* knew he was observing short-term guests, the Court's conclusion might have met a minimum—though still contestable—standard of plausibility. However, because there is no reason to believe that the officer was able to distinguish between guests and homedwellers, *Carter* stands for the proposition that even the privacy interests of the latter can be legitimately undermined for the sake of monitoring the activities of the former. As Justice Ginsburg observed in her dissent, given *Carter's* conclusion, "people are not genuinely 'secure in their . . . houses . . . against unreasonable searches and seizures' if their invitations to others increase the risk of unwarranted governmental peering and prying into their dwelling places."³¹⁴ How should *Carter* have been resolved, then? The question is difficult given the problematic status of the short-term guest. But even if we agree with the Court's claim that social conventions deny such guests any privacy interest, it seems clear that the proper resolution of *Carter* would have been to hold that police officers may ignore a home-dweller's privacy cues only if they are aware *ex ante*—that is, at the time they engage in surveillance—that the people they are observing are short-term guests.

These comments about privacy cues for homes provide a context in which to understand the Court's conclusions about police inspection of garbage. The way in which people usually signal an interest in privacy for their garbage is to wrap it in opaque bags tied at the top. This is exactly how the defendants in *California v. Greenwood* dealt with their garbage: after placing their trash in dark bags, the defendants deposited it at the curb in anticipation of its collection.³¹⁵ The *Greenwood* Court conceded that the defendants may have had a *subjective* expectation of privacy.³¹⁶ But it yielded no further ground. No one can have an *objectively valid* privacy expectation in trash placed on the curb outside the home, the Court stated, since "scavengers, snoops, and other members of the public" can go

³¹³ See *id.* at 103 (Breyer, J., concurring).

³¹⁴ *Id.* at 108 (Ginsburg, J., dissenting).

³¹⁵ 486 U.S. 35, 39 (1988).

³¹⁶ *Id.* at 39.

through such garbage if they wish.³¹⁷ The police, the Court concluded, did not infringe on the Greenwoods' privacy when they systematically went through their garbage without obtaining a warrant since the police were simply doing what snoops already do.

Greenwood will always be memorable for this point, for here the Court openly acknowledged that it considers the behavior of snoops relevant to the definition of objectively reasonable privacy interests. Expanding on its reference to snoops, the *Greenwood* Court even inserted a footnote in which it explained, with no indication of disapproval, how a tabloid reporter had gone through garbage left outside Henry Kissinger's home.³¹⁸ Presumably, the Court meant that because Kissinger had been preyed on by reporters, everyone else should consider the possibility of snooping in seeking privacy for themselves. But this turns matters upside down. The snoop *threatens* privacy. The term "snoop" is instructive because it reminds us of the precautions we must take *beyond* those normally needed to insure privacy. So, for example, if I'm worried that a snoop might cup his ear to the door of the room in which I'm talking to someone else, I'll then have to speak in a whisper rather than my normal tone of voice. But a whisper, of course, goes beyond the normal precautions associated with privacy. Speaking in a whisper, even when the door has been closed, indicates that someone is insecure even when in a setting normally associated with privacy. *Greenwood*, we can thus say, errs in its unwillingness to treat the normal precautions people take to ensure privacy as sufficient to create an objectively reasonable interest in it.

Must the police always obtain a warrant to search garbage, then? Of course not. Garbage is not a private object, so if a police officer happens to come upon garbage strewn on the sidewalk, the officer cannot be said to have interfered with a privacy interest on inspecting it. The *Greenwood* Court actually endorsed a formula of this kind when it remarked that "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity"³¹⁹ Given the facts in

³¹⁷ *Id.* at 40.

³¹⁸ *Id.* at 40 n.4 ("Even the refuse of prominent Americans has not been invulnerable," the Court remarked. "In 1975, for example, a reporter for a weekly tabloid seized five bags of garbage from the sidewalk outside the home of Secretary of State Henry Kissinger.") .

³¹⁹ *Id.* at 41.

Greenwood, this remark was as disingenuous as was a similar one in *Ciraolo*.³²⁰ But the remark does at least underscore the importance of the distinction between serendipitous discovery and devious snooping. We can thus readily agree that no privacy interest is at stake if the police stumble upon garbage strewn on the sidewalk. But we can also agree that the police can't disregard the signal provided by a closed, opaque bag; they open the bag, inspect its contents—and *then* say they shouldn't have to "avert their eyes from evidence of criminal activity."³²¹

3. *Surveillance of Behavior in Public Places*

What if conventional understandings don't classify an object as private and no signals are sent indicating an interest in keeping it that way? At first glance, it would seem that the answer to this is easy: no privacy interest, one might argue, can ever be claimed under these circumstances. To use Erving Goffman's phrase, people "present themselves" to others in public places.³²² When they do, it could be said, there is nothing they can claim as private. It may be rude to engage in prolonged staring at others in public places, but rudeness, it could be claimed, must be distinguished from an actual invasion of privacy. The system of privacy is not to be confused with the rules of exquisite manners.

There is a great deal to be said for this line of reasoning. In presenting ourselves to others, we make allowance for the occasional stare as we sit on subway trains or walk along on sidewalks. And if the occasional stare is acceptable from the layperson, then it is acceptable as well from a police officer. An officer on foot patrol or riding in a car surveys the world before her, letting her eyes run over a great many objects and pausing to stare more carefully at a few. But does this point establish the further one that there can *never* be an objectively reasonable privacy expectation for behavior in public places? Does it show that privacy interests are not implicated when technology is substituted for a police gaze—when, for example, a television

³²⁰ See *Ciraolo* ("The Fourth Amendment protection of the home has never been extended to require officers to shield their eyes when passing by a home on public thoroughfares." 476 U.S. at 213.

³²¹ *Id.*

³²² ERVING GOFFMAN, *THE PRESENTATION OF SELF IN EVERYDAY LIFE* (1959).

camera is used to survey a street scene? And does it show that privacy interests are not implicated when, either by means of technological innovation or regular use of police manpower, someone is followed as he moves about through public places? These are the questions addressed in the following pages. I concede that privacy interests are modest indeed for behavior in public places. However, I challenge the Court's conclusion that they are nonexistent.

Consider first the issue of "shadowing"—the question of whether someone has a privacy interest in not being followed around in public places. Given modern technology, police can track someone's movements without having to keep that person within eyesight at all times. A beeper, for example, can be attached to a device someone has purchased; when properly monitored, the beeper can often provide the police with information about the buyer's movements.³²³ In *United States v. Knotts*³²⁴ and *United States v. Karo*,³²⁵ the Court upheld beeper surveillance of conduct within public places. Each case involved surveillance of prolonged travel. In *Knotts*, for example, the beeper was used to monitor the defendants' movements as they drove more than a hundred miles from Minneapolis to the Minnesota/Wisconsin state line and, ultimately, to a cabin located in northern Wisconsin.³²⁶ The *Knotts* Court unequivocally rejected the defendants' claim that beeper surveillance of their car ride interfered with a protected privacy interest. "When Petschen [one of the *Knotts* defendants] traveled over the public streets," the Court stated, "he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."³²⁷

³²³ In *Knotts*, for example, the Court remarked that "[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver. In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants." 460 U.S. 276, 277 (1983).

³²⁴ 460 U.S. 276.

³²⁵ 468 U.S. 705 (1984).

³²⁶ *Knotts*, 460 U.S. at 278-79.

³²⁷ *Id.* at 281-82.

There is a surface plausibility to this conclusion, given the fact that movement in public places isn't considered a private activity. However, the Court's reference to "anyone who wanted to look" should alert us to the disingenuousness in this context similar to its disingenuousness in *California v. Ciraolo*. In that case, it will be recalled, the Court stated that police shouldn't have to "shield their eyes" to avoid examining the contents of Ciraolo's backyard—a point it made only after noting that the police had disregarded signals indicating an interest in privacy for the yard, hired a plane, and taken pictures of the yard from an altitude of one thousand feet.³²⁸ The term "shielding their eyes" correctly appeals to privacy conventions, then, but it does so in a context where the police have already flouted them.

Exactly the same point can be made here. Anyone "wanting to look" at Petschen as he traveled through the streets of Minneapolis would have noticed him for a fleeting moment. A further look, however, would have required instant access to a car with a full tank of gas and a detective's ability to follow another car for hours on end. "Wanting to look" thus captures an important convention—the legitimacy of the brief glance at someone in a public place. It doesn't capture what's at stake in prolonged surveillance of a lengthy trip over a public road.

In developing this point, we can identify two reasons why shadowing someone's public movements runs afoul of everyday privacy understandings. The first has to do with the symmetry of encounters in public places. The fleeting glance in a public place is often returned by another person's fleeting glance. As already noted, privacy conventions depend on this kind of symmetry.³²⁹ Shadowing someone, by contrast, breaks the symmetry, for the shadower subjects the person under surveillance to sustained scrutiny with nothing comparable being returned. Of course, more than privacy is at stake in such settings. There is something ominous about being shadowed. At its most extreme, shadowing can amount to stalking, with the person being followed feeling terror about her physical safety.³³⁰ But even when this is eliminated—even when we subtract this

³²⁸ *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

³²⁹ See *supra* p. 54.

³³⁰ Some states have made stalking a crime. In 1999, for example, New York criminalized stalking and distinguished between four different degrees of it. See NEW YORK PENAL LAW §§ 120.45-120.60 (McKinney (2002)).

fear—there is still a privacy concern that arises out of the asymmetry of the relationship.

The second reason why privacy is implicated in shadowing has to do with the resolution of uncertainty. On the Court's account, uncertainty is only an incidental element of privacy.³³¹ What matters, as far as the Court is concerned, is full concealment from other people of what one wishes to keep private.³³² We have seen time and again, though, how deeply this approach departs from everyday understandings of privacy.³³³ The everyday concept of privacy allows for partial *nonconcealment*. It requires only that an insider take meaningful steps to generate uncertainty among outsiders as to what is being withheld, with the burden then placed on outsiders not to resolve this uncertainty by a scheme of circumvention. In shadowing someone, a person rejects the uncertainty about others that characterizes symmetrical encounters in public places. The still picture each party takes away from a brief encounter in a public place is replaced by a one-sided moving picture of a person's movements throughout the public world.

In this respect, shadowing someone is not unlike examining a person's pattern of phone calls. There is rarely much significance to be found in the isolated call. The accumulation of information about calls made can, however, help to identify the patterns of someone's life. Chance encounters at the supermarket or on the street also reveal little about a person. In shadowing someone for days or weeks, though, one can often discover a good deal. The concept of privacy is relevant in this context precisely because people are likely to feel vulnerable about an outsider's discovery of such information.

To speak of a privacy interest in public places is not, of course, to suggest that the interest is a strong one. The vulnerability at stake here is far weaker than that associated with the involuntary revelation of the contents of, say, one's home or

³³¹ That is, if an insider has taken sufficient steps to signal an interest in privacy by creating uncertainty as to what he wishes to withhold from outsiders but has failed to conceal completely an object or information, then outsiders, on the Court's account, are under no obligation to refrain from trying to discover what the insider was seeking to withhold. This point is analyzed in the discussion of privacy cues. See Part IV.B.2 *supra*.

³³² *Id.*

³³³ *Id.*

finances. However, one also can't say, as the Court has, that shadowing someone's movements has no implications for that person's privacy.³³⁴ How, then, should courts address shadowing? The proper approach, I suggest, is to treat shadowing as implicating a modest privacy interest and so to require *Terry*-type reasonable suspicion as a prerequisite for undertaking it. In *Terry v. Ohio*, the Court held that reasonable suspicion, rather than probable cause, is required for brief interference with someone's liberty interests.³³⁵ Shadowing offers a privacy analogue to the liberty interests at stake in *Terry*: it is sufficiently important to warrant judicial oversight but not so weighty as to require probable cause. The soundness of this conclusion is underscored by considering the facts in *United States v. Knotts*. At the time the police began shadowing the *Knotts* defendants, they knew that officials of the 3M Company suspected one of the defendants, Armstrong, of stealing chemicals needed to manufacture drugs.³³⁶ The police also knew that Armstrong had been buying the same kind of chemicals from a retailer in Minneapolis.³³⁷ The Court thus could have remanded the case on the basis of a reasonable suspicion rationale, with instructions to the lower courts to determine whether government shadowing of Armstrong would have led to the discovery of the other defendants. That it failed to do so—that it instead held shadowing to be wholly unconnected to privacy—reveals how aggressive it has been in building the vigilance model.

The points just made apply to beeper-enhanced shadowing as well as person-to-person surveillance, so if a police officer can be said to interfere with privacy by following someone through the streets, the same objection can be made to shadowing someone by beeper. There is, however, a further difficulty with beepers, one that may well make them wholly unacceptable under the Fourth Amendment. This difficulty has to do with their installation—with their attachment to objects prior to conducting surveillance. In *Knotts*, the retailer of chemicals had attached a beeper to a container of chloroform, a fact that of course was not conveyed to the *Knotts* defendant who

³³⁴ For the Court's position, see *Karo*, 468 U.S. at 713-14.

³³⁵ 392 U.S. 1, 16-30 (1968).

³³⁶ See *United States v. Knotts*, 460 U.S. 276, 278 (1983).

³³⁷ *Id.* at 277-79.

subsequently purchased the container.³³⁸ No *Knotts* defendant challenged the constitutionality of this installation, however, so the installation issue was not addressed in that case.³³⁹ A year later, in *United States v. Karo*, the Court did take up this issue, considering a fact-pattern pertaining to installation similar to the one in *Knotts*.³⁴⁰ *Karo* argued that the warrantless installation of a beeper on an object followed by a sale of the object (without a warning to the buyer of the beeper's presence) constitutes an unreasonable search and an unreasonable seizure.³⁴¹ The *Karo* Court rejected both contentions.³⁴² No privacy interest is implicated before a beeper is turned on, the Court held, because police officers begin beeper monitoring only after a sale has been completed.³⁴³ Furthermore, one cannot claim that beeper installation implicates a privacy interest.³⁴⁴ No property interest is implicated, the Court concluded, because beeper installation amounts only to a technical trespass.³⁴⁵ "Although the can [purchased by *Karo*] may have contained an unknown and unwanted foreign object" at the time of sale, the Court remarked, "it cannot be said that anyone's possessory interest was interfered with in a meaningful way."³⁴⁶

Karo's conclusion about privacy is arguably sound: no threat to privacy can be said to exist until a beeper begins transmission. Its conclusion about property interests, on the other hand, is palpably wrong. The *Jacobsen* Court, it will be recalled, established the criterion for determining when government officials interfere with property interests under the Fourth Amendment. According to *Jacobsen*, a seizure of property occurs when "there is some meaningful interference with an individual's possessory interests in that property."³⁴⁷ As Justice Stevens aptly noted in his *Karo* dissent, "[w]hen the

³³⁸ *Id.* at 278.

³³⁹ Justice White noted this at the beginning of his opinion of the Court in *Karo*. 468 U.S. 705, 707 (1984).

³⁴⁰ 468 U.S. 705.

³⁴¹ *Id.* at 710.

³⁴² *Id.* at 712-13.

³⁴³ *Id.* at 712.

³⁴⁴ *Id.*

³⁴⁵ *Id.*

³⁴⁶ *Id.*

³⁴⁷ *Jacobsen v. United States*, 466 U.S. 109, 113 (1984).

Government attaches an electronic monitoring device to [someone's] property, . . . it convert[s] the property to its own use."³⁴⁸ Moreover, this conversion-of-property phenomenon is inescapable as far as involuntary beeper monitoring is concerned. In attaching a beeper to a person's clothing, car, or bicycle, government officials meaningfully interfere with that person's possessory interests. Only voluntary beeper monitoring—that is, monitoring conducted by someone who has agreed to have a beeper attached to his person or possessions—will be constitutionally acceptable. Involuntary attachment of a beeper will invariably interfere with an individual's possessory interests.

If beepers fail on possessory grounds and if shadowing in the absence of reasonable suspicion is, in any event, unacceptable because of its interference with privacy interests, what conclusion should be reached about television surveillance of behavior in public places? It is here that the analogy with a police officer's wandering gaze proves to be well-founded. In surveying a public place, a television camera captures exactly what an officer could capture on scrutinizing the place. Because no privacy interest is implicated when an officer surveys a public place (just as none is implicated when a private citizen does so), one would have to say that television surveillance of conduct in public places doesn't affect privacy. It is true, of course, that television cameras vastly enhance the efficiency of police surveillance; a single police officer, for example, can monitor five or six screens, thus surveying far more than she could were she actually out and about in a public place. But efficiency arguments have no weight here. The fact that a television camera outperforms an officer walking a beat doesn't mean that television cameras must be rejected as a surveillance device.

What if television surveillance of a public place is videotaped, with the tapes retained indefinitely by the police? The analogy with an officer's surveying eye is, of course, weakened once this extra factor is added. Few individuals have (though many claim to have) a "photographic" memory; retained videotapes, by contrast, *are* photographic memories. But it is hard to see why retention of a videotape should alter our conclusions about privacy in such a setting. Once it is

³⁴⁸ *Karo*, 468 U.S. at 729.

agreed that individuals don't have a privacy interest in being free from chance "spottings" in public places, one must also agree that devices facilitating permanent retention of these spottings also don't interfere with privacy.

4. *A Note on Technology and Privacy*

Lurking in the background of this—and, indeed, any—discussion of surveillance is a concern about the threat to privacy posed by technological innovation. If technology invariably undermined privacy interests, it would be possible to reject aerial overflight (in *Ciraolo* and *Riley*) and beeper surveillance (in *Knotts* and *Karo*) on that ground alone. But in doing so, one would offer a simplistic, Luddite solution to what in fact is a complex problem. People welcome technological innovation for the efficiencies it offers in everyday life. Furthermore, technology only sometimes subverts privacy; it can also serve as a shield for it.³⁴⁹ One thus can't take a given year—say, 1967, the year in which *Katz* was decided³⁵⁰—and declare that all innovation occurring since then is incompatible with privacy. Rather, one must consider carefully the ways in which technology impinges on the sources of personal vulnerability. On this analysis, *Katz* was properly decided because it prevented technology from interfering with each person's interest in intimate conversation. But *Dow Chemical* also was properly decided given the fact that the government's technology was being used to examine objects with no connection to personal relationships.

Unfortunately, the contemporary Court has not employed this framework when examining technology's implications for privacy. Indeed, its approach has had the effect of undermining *Katz* while leaving the scope of permissible technological

³⁴⁹ See, e.g., Lawrence Lessig, *Technology Will Solve Web Privacy Problems*, WALL ST. J., May 31, 2000, at A26 (arguing that encryption codes will help to ensure privacy on the internet).

³⁵⁰ *Katz*, it should be noted, was decided at a moment in the development of telecommunications technology that was uniquely favorable to privacy claims. Operators, though still needed to place long distance calls, were no longer required for local ones; had they still been needed for local calls, operators could of course have noted where calls were made and listened to them. Also, telephone booths were full enclosures. It was only in the seventies that banks of public telephones, with only modest plexiglass partitions, came to separate one another. An appeal to principle—to the importance of phone calls in sustaining personal communication—makes it unnecessary to consider changes such as these.

infringement on privacy far from clear. The leading case is *Kyllo v. United States*, which considered the use of a thermal imaging device to detect heat waves emanating from inside a home.³⁵¹ A thermal imager detects infrared radiation.³⁵² By converting radiation into images reflecting warmth, it provides information about the amount of heat emanating from a home.³⁵³ Suspecting that Kyllo was using high-intensity lamps to grow marijuana in his home, police officers stood outside it at three o'clock on a January morning and used a thermal imager to detect heat emanating from it.³⁵⁴ The scan established that the roof over the garage was hot by comparison with the rest of Kyllo's home and the homes nearby.³⁵⁵ Relying on this finding as well as tips from informants and utility bills, the police obtained a search warrant.³⁵⁶ On executing it, they found an indoor drug operation that included more than one hundred marijuana plants.³⁵⁷

Writing for the *Kyllo* Court, Justice Scalia announced that "[t]he question we confront today is what limits there are upon th[e] power of technology to shrink the realm of guaranteed privacy."³⁵⁸ His expression of concern was reassuring, and at first sight, the rule he announced appears reassuring as well. "[O]btaining by sense-enhancing technology," Scalia wrote, "any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search, at least where (as here) the technology in question is not in general public use."³⁵⁹ This final caveat—about general public use—makes the scope of the rule uncertain. On Scalia's approach, market forces have the potential to subvert any privacy arrangement, for once the manufacturer of a device such as the thermal imager succeeds in generating substantial

³⁵¹ *Kyllo v. United States*, 533 U.S. 27 (2001).

³⁵² *Id.* at 29 ("Thermal imagers detect infrared radiation, which virtually all objects emit but which is invisible to the naked eye.").

³⁵³ *Id.* at 29-30.

³⁵⁴ *Id.* at 29.

³⁵⁵ *Id.* at 30.

³⁵⁶ *Id.*

³⁵⁷ *See id.*

³⁵⁸ *Id.* at 34.

³⁵⁹ *Id.* (citing *Silverman v. United States*, 365 U.S. 505, 512 (1961)).

sales for its product, individuals will no longer be protected against it.

This, however, is only one of the difficulties posed by *Kyllo*. A more important problem is doctrinal, for *Kyllo* intimates an approach to privacy fundamentally at odds with the *Katz* reasonable expectations test. Concurring in *Minnesota v. Carter*, a case decided three years before *Kyllo*, Justice Scalia denounced the test as “notoriously unhelpful” and “self-indulgent.”³⁶⁰ He went on to state that the Fourth Amendment protects privacy through its enumeration of specific objects (“persons, houses, papers, and effects”) and so leaves “expansion [of privacy protection] to the good judgment, not of this Court, but of the people through their representatives in the legislature.”³⁶¹ In *Kyllo*, Scalia revived this criticism of *Katz*. He did not, however, reject Justice Harlan’s reasonable expectations test. On the contrary, after expressing his dissatisfaction with the test, he invoked it, stating that the no-technological-enhancement rule protects “the minimal expectation of privacy that *exists*, and is acknowledged to be *reasonable*,” for homes.³⁶²

The almost certain explanation for this peculiar about-face (criticizing a framework and then employing it) is that Scalia did not have the votes to reject outright the reasonable-expectations test. The result, however, is a muddle. Perhaps the best interpretation of *Kyllo* is that houses now enjoy a specially privileged position under the expectations test. Any item in which there is an objective expectation of privacy will enjoy *some* protection, but houses, one might say, are *fully* protected—or at least they are fully protected against technology not in general use.³⁶³ But if this is so, does

³⁶⁰ *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

³⁶¹ *Id.* at 97-98.

³⁶² *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

³⁶³ Indeed, it is far from clear that even this qualification is sufficient. Justice Scalia’s *Kyllo* opinion contains the sweeping dictum that “[in] the home, as our cases show, *all* details are intimate details because the entire home is held safe from prying government eyes.” *Id.* at 37. The Court’s cases hardly do establish this. In *Carter*, a decision that Justice Scalia joined, the Court held it permissible for government officials to peer through a hole in living room blinds to inspect the activities of people the officials did not know to be temporary guests. See *Carter*, 525 U.S. at 98. Similarly, in *Lewis v. United States*, 385 U.S. 206, 211 (1966), the Court declared that when “the home is converted into a commercial center to which outsiders are invited to transact unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street.” It seems unlikely that

enumeration in the Amendment's catalog ensure superior protection for *all* objects mentioned there—for persons, papers, and effects as well as houses? Or is the privileged status of the house not dependent on the fact of enumeration? Could it be that Justice Scalia, despite his criticism of Harlan's reasonable expectations test, was in fact relying on that very test in according the house greater protection than he would be prepared to provide persons, papers, and effects?

The difficulties with *Kyllo's* analysis do not end here, however. Indeed, the most important problem posed by Justice Scalia's approach has to do with the legitimacy of *Katz* itself. *Kyllo* concludes with an approving citation of Chief Justice Taft's claim that "[t]he Fourth Amendment is to be construed in light of what was deemed an unreasonable search and seizure when it was adopted"³⁶⁴ As we have seen, Chief Justice Taft relied on this premise in *Olmstead* to hold that the Fourth Amendment cannot protect people against nontrespassory surveillance of their conversations.³⁶⁵ Scalia didn't endorse this conclusion in *Kyllo*, but his invocation of Taft's premise cast in doubt the foundation of modern privacy jurisprudence.

How, then, should *Kyllo* have been resolved? The answer to this is that the Court reached the right conclusion for very much the wrong reason. The proper framework was to ask whether a thermal imager identifies matters of personal vulnerability that people are likely to want to avoid disclosing to others. Heat waves, it is clear, can indicate lawful, as well as unlawful, activity—they provide evidence of substantial use of, say, a sauna or a microwave. Even when they provide information about high-intensity lighting, this information doesn't necessarily establish that someone is growing marijuana plants; it may turn out that the lighting is being used to fight a skin disease or simply to help someone gain a tan. These are not the activities people are most likely to want to shield from public scrutiny in our society. Privacy analysis, however, must make allowance for plausible and not wholly far-fetched sources of vulnerability. A rule permitting warrantless surveillance of

Justice Scalia wants to rethink these conclusions. But if he does not, then his dictum, and indeed his entire emphasis on the home *qua* home, is drained of its significance.

³⁶⁴ *Kyllo*, 533 U.S. at 40 (citing *Carroll v. United States*, 267 U.S. 132, 149 (1925)).

³⁶⁵ See *supra* note 50 and accompanying text.

heat waves from the home would most certainly increase this sense of vulnerability.

In contrast with the rule announced in *Kyllo*, the approach just outlined allows for the possibility of warrantless, sense-enhancing technological surveillance of the home, provided such surveillance poses no threat to privacy interests. In *Kyllo*, Justice Scalia proudly stated that the Court was announcing an exceptionless rule for technological surveillance of the interior of the home.³⁶⁶ But homes, like offices, luggage, purses, clothing, and so on, not only provide privacy, they also can be used to conceal contraband. Technology that is unable to distinguish between contraband and lawfully possessed items impermissibly interferes with privacy—thus the propriety of rejecting a device such as the thermal imager. But, as the Court noted in *Place*, technology that accurately identifies contraband and produces no false positives with respect to legally possessed items is compatible with the Fourth Amendment.³⁶⁷

Even if no such technology presently exists, it is essential to make allowance for its development. Consider, for example, the possibility of a machine that responds only to the existence of enriched uranium in a concealed place. No one has a privacy interest in possessing enriched uranium, so a machine that accurately identifies its existence should undoubtedly be upheld on Fourth Amendment grounds. *Kyllo*, however, prohibits police use of such a device when applied to homes. Similarly, *Kyllo* will stand in the way if a device is developed that responds solely to stolen merchandise with special tags attached to it, and the case will have a similar effect if a machine is invented that can detect illegally possessed firearms stored in a home.³⁶⁸ In this critical respect, *Kyllo* extends *beyond* what the Fourth Amendment requires.³⁶⁹ Had the Court considered technology

³⁶⁶ See *Kyllo*, 553 U.S. at 39 (The line drawn to protect the home, Justice Scalia stated, “must be not only firm but also bright . . .”).

³⁶⁷ See *supra* notes 230-40 and accompanying text.

³⁶⁸ The technology for this kind of search may well be available now. Also, the technology appears to have been developed for detecting explosives on gunpowder by placing taggants on it. See John J. Fialka, *Tracing Explosives Through Taggants Draws Heavy Fire From Gun Lobbies*, WALL ST. J., July 31, 1996, at A16.

³⁶⁹ In *Kyllo*, the Court stated that its rule “assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo*, 553 U.S. at 231. The rule outlined here would have the same effect, however but would not in the process sacrifice the legitimate public interest in discovering objects within the home that cannot be the subject of privacy interests. In short, the

in a more nuanced way, it could thus have created a rule that was neither over-, nor under-protective of privacy interests.

C. INTERACTIVE SURVEILLANCE

Our discussion so far has concentrated on observational, rather than interactive, surveillance. Observational surveillance, as I noted earlier, is passive in nature; its aim is to provide unobtrusive monitoring of a subject's behavior. Interactive surveillance, on the other hand, involves direct contact with a subject. This, however, is only one of its distinguishing features. With interactive surveillance, government agents try to penetrate human relationships to discover information or objects of evidentiary value. The penetration can be carried out by deception. Officials can pretend to be drug dealers, for example, or can pretend to be willing to accept bribes. But the penetration can also be carried out by acts of betrayal, as when government officials persuade an insider to provide information about other insiders, or when an insider decides on her own to betray others. Needless to say, deception and betrayal aren't mutually exclusive. For example, if an insider engages in an ongoing act of betrayal by reporting secretly to the government about her conversations with a suspect, the insider's actions can be said to involve an element of deception as well as betrayal.

The Court has set no Fourth Amendment limits on either deception or betrayal. Most of its decisions concerning these matters were reached prior to *Katz*; it has, however, shown no inclination to revise its approach in light of *Katz*. With the exception of the modest restraints imposed by the law of entrapment,³⁷⁰ there are no legal barriers to the government's use of deception and betrayal as means of gathering evidence. In numerous cases, some decided before and some after *Katz*, the Court has, among other things, approved undercover operations in which friends turn on friends,³⁷¹ in which

rule proposed here protects privacy of the home as it existed in the eighteenth century but does not freeze technology which does *not* threaten privacy at its eighteenth century level of development.

³⁷⁰ The entrapment defense focuses on a person's predisposition to commit a crime: "Where the Government has induced an individual to break the law and the defense of entrapment is at issue, . . . the prosecution must prove beyond reasonable doubt that the defendant was disposed to commit the criminal act prior to first being approached by Government agents." *Jacobson v. United States*, 503 U.S. 540, 549-50 (1992).

³⁷¹ See *Hoffa v. United States*, 385 U.S. 293 (1966).

government officials posing as customers have purchased drugs from unwitting dealers,³⁷² in which officials have worn electronic equipment to record the conversations of the people they were monitoring³⁷³—and the Court has reached these conclusions by turning aside time after time arguments that such conduct implicates the Fourth Amendment. As a matter of legal doctrine, then, schemes of betrayal and deceit are not subject to judicial review under the Fourth Amendment. In forging ties with others, people take the risk, the Court maintains, that the government has either planted friends among them or, the associations having been formed, that it has induced their friends to turn on them.³⁷⁴

In one respect, the Court's position is surely correct. The Fourth Amendment, it is clear, cannot be construed to provide full protection against government deception and betrayal. Many different kinds of undercover operations have nothing to do with privacy. For example, when government agents pose as buyers of narcotics or when agents pretend to take bribes from people seeking to evade taxes, no interest associated with privacy is implicated at all. The problem with the Court's position is that it has embraced the other extreme, with the result that its jurisprudence offers no protection against interference with even intimate relationships. Revising the Court's approach is by no means an easy matter. At the least, three different propositions must be considered by way of corrective. I outline the propositions here; later, I apply them to cases decided by the Court.

The first point to note is that people in intimate relationships can reasonably expect others engaged in relationships with them not to deceive or betray them. The "reasonably expect" in this sentence is simultaneously empirical and normative. In forging personal ties, people exchange confidences, the initial confidences serving not simply as tokens of interest but also as tests of reliability. Close personal ties are

³⁷² *Lewis v. United States*, 385 U.S. 206 (1966).

³⁷³ See *United States v. White*, 401 U.S. 745 (1971); *Osborn v. United States*, 385 U.S. 323 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

³⁷⁴ As the Court remarked in *Hoffa*, "petitioner . . . was not relying on the security of the hotel room [in which he engaged in conversation with an associate who, unbeknownst to him, was a government informer]; he was relying upon his misplaced confidence that Partin [the informant] would not reveal his wrongdoing." 385 U.S. at 302.

formed when these tests have been passed. In this critical sense, the exchange of confidences and the sharing of personal space define the boundaries of "interpersonal privacy"³⁷⁵ for specific relationships, with those boundaries policed by normative injunctions against deceit and betrayal. The Court, unfortunately, has made no allowance for interpersonal privacy. One can readily concede that claims of interpersonal privacy are often amorphous and so hard to enforce in practice, a point that will be explored later. It is simply implausible, however, to banish the phenomenon of interpersonal privacy altogether. Given *Katz's* adoption of privacy as an independent variable in Fourth Amendment analysis, this specific type of privacy must be given consideration.

The second point to bear in mind qualifies the first in one substantial respect. A liberal legal order, it is clear, cannot prohibit betrayal by those within intimate relationships; moreover, for pragmatic reasons, it also should not prohibit certain kinds of deceit within such relationships. The argument concerning betrayal is straightforward. Respect for individual autonomy requires the law to stay its hand when intimates choose to betray fellow intimates by revealing confidences or unusual quirks of behavior. This point holds true even in the face of privacy's injunction against betrayal, for while a liberal legal order must respect privacy and so must respect the spontaneously generated norms that enforce it, this order also must respect autonomy's trump claim that people may opt out of intimate relationships if they so choose.

The argument concerning deceit is more complex. Certain kinds of deceit within intimate relationships can indeed be prohibited consistent with the principles of a liberal legal order—think, for example, about legal prohibitions against deceitful concealment of one's capacity to transmit a sexually communicable disease.³⁷⁶ But deceit about one's affections—

³⁷⁵ Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. L. REV. 1 (1983).

³⁷⁶ The general principle involving fraudulent misrepresentation is:

One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation.

RESTATEMENT (SECOND) OF TORTS, § 525 (1977).

deceit about whether one genuinely cares for another person—is another matter. Even if it were desirable to adopt legal prohibitions in this context, major problems would arise if the government were to use criminal or civil law as enforcement measures. The relationships that come under the heading of interpersonal privacy are too fluid, and also too subtle in their structure, to lend themselves to legal oversight as to this kind of deceit.³⁷⁷ For insiders, then, both betrayal and deceit concerning affections are legally permissible options, a point that is not inconsistent with the fact that they are also normatively disfavored within the system of privacy.

The third proposition to be considered has to do with outsiders' use of deceit and betrayal to penetrate intimate relationships. It is because autonomy claims can override the claims of privacy that betrayal and deceit are acceptable options for insiders to intimate relationships. The same cannot be said for outsiders who want to use these stratagems to gain access to insiders' relationships. No autonomy claim is sufficiently strong to support an outsider's resort to such measures. On the contrary, outsiders who use deceit or who try to induce betrayal in order to penetrate intimate relationships can properly be charged with invading insiders' privacy. Here, then, is the most profound error in the Court's jurisprudence of undercover operations. Given the fact that close, personal relationships are matters of privacy, efforts by outsiders to gain access to these relationships by resort to deceit or betrayal invade that privacy. Because one of the basic axioms of Fourth Amendment case law is that the government is subject to the same norms as private parties,³⁷⁸ government resort to deceit and betrayal also stands as an invasion of privacy.

This principle is discernible in decisions holding parties liable for deliberate misrepresentation of the presence of sexually transmitted diseases. *See, e.g.*, Kathleen K. v. Robert B., 198 Cal. Rptr. 273, 277 (Cal. 1984).

³⁷⁷ For a discussion of the rationale for abolishing the tort of alienation of affections, see Nathan P. Feinsinger, *Legislative Attack on "Heart Balm,"* 33 MICH. L. REV. 979 (1935).

³⁷⁸ The point is implicit in *Katz's* statement that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967). The Court explicitly acknowledged the axiom when it stated more than a decade later that "[w]ithout a warrant, [a government official] stands in no better position than a member of the public. What is observable by the public is observable, without a warrant, by [a] Government inspector as well." *Marshall v. Barlow's Inc.*, 436 U.S. 307, 314-15 (1978).

The points just made still allow the government considerable leeway in undercover operations. First, the government can use deceit and betrayal to penetrate relationships that have nothing to do with privacy—to penetrate commercial relationships, for example. Second, the government is not foreclosed from accepting defectors from intimate relationships. If someone decides on her own to reveal confidences acquired in the context of intimacy, the government certainly can't be said to invade privacy when it accepts information provided by the defector. What the government cannot do, consistent with the norms of privacy, is to take steps on its own to penetrate intimate relationships.

Admittedly, this principle is hard to apply. Difficult border-definition issues arise as to when a relationship involves personal ties, when the government is offering inducements to betrayal, and when an insider has defected of her own volition. Ease of application cannot, however, be the controlling principle of Fourth Amendment jurisprudence; otherwise, *Olmstead* would have to be preferred to *Katz*, and “fuzzy” concepts such as probable cause and reasonable suspicion would have to be rejected altogether. Rather, precepts that accurately reflect Fourth Amendment values (and the precepts just outlined are clearly successful in this regard) must be preferred to simplified versions of them unless substantial problems in application are encountered. In what follows, I argue that difficulties in applying the precepts just outlined are manageable: the precepts, I suggest, inject a tolerable, and appropriate level, of complexity into Fourth Amendment analysis. I begin by showing that there are many settings in which the precepts are not at all difficult to apply. I then turn to harder cases, showing that there are indeed some difficult border areas, but that even these do not pose insuperable difficulties.

1. *Nonproblematic Settings*

No difficulty is encountered in a given setting when it is clear that the relationship at stake is not an intimate one or when it is clear that someone's act of betrayal was not prompted by government inducement. A case decided by the Court in 1966, *Lewis v. United States*,³⁷⁹ will prove helpful in identifying the

³⁷⁹ 385 U.S. 206 (1966).

key elements of undercover operations that have no connection with personal relationships. A 1980 circuit court case, *United States v. Baldwin*,³⁸⁰ takes us to the other pole; it deals with an undercover operation that, incontestably, did involve close ties. For inducements to betrayal, we will have to go outside the range of reported cases. A well-known modern betrayal that has had repercussions in judicial proceedings—Whittaker Chambers's testimony about Alger Hiss—will prove helpful in this regard.³⁸¹

Lewis provides an example of a straightforward business transaction with no overtones of personal ties at all. Identifying himself as "Jimmy the Pollack," a federal undercover narcotics agent, who hadn't met Lewis prior to the call, phoned Lewis's home, saying that someone had told him Lewis would be able to sell him some marihuana.³⁸² Lewis responded, "Yes. I believe, Jimmy, I can take care of you"—and then provided the agent with directions for reaching his home, where the sale of marihuana occurred.³⁸³ Two weeks later, Lewis made another marihuana sale to "Jimmy" at his home.³⁸⁴

In *Lewis*, we thus encounter systematic deception by a government official, but no interference with interpersonal privacy. As Chief Justice Warren noted in his opinion for the Court, Lewis' "only concern was whether the [government] agent was a willing purchaser who could pay the agreed price." Warren continued: "During neither of his visits to [Lewis's] home did the agent see, hear, or take anything that was not contemplated, and in fact intended, by [Lewis] as a necessary part of his illegal business."³⁸⁵

But what about the locus of the illegal transaction—Lewis's home? Warren's argument is cogent here as well. He remarked:

The fact that the undercover agent entered [Lewis's] home does not compel a different conclusion. Without question, the home is accorded the full range of Fourth Amendment protections. But when, as here, the home is converted into a commercial center to which outsiders are

³⁸⁰ 621 F.2d 251 (6th Cir. 1980).

³⁸¹ See *infra* notes 406-09 and accompanying text.

³⁸² See *Lewis*, 385 U.S. at 207.

³⁸³ *Id.*

³⁸⁴ *Id.* at 207-08.

³⁸⁵ *Id.* at 210.

invited for purposes of transacting lawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street.³⁸⁶

According to Warren, then, the Fourth Amendment offers no protection against government officials' use of deception to enter the home when the homeowner has invited them into his residence for the purpose of transacting business with them. This is surely a sound result, one that focuses on the nature of the relationship at stake and the use someone makes of her home. If we generalize on it, we can see that government deception is legitimate (because interpersonal privacy is not at stake) in other types of relationships—in police decoy and sting operations, for example.³⁸⁷ Indeed, whenever government officials: (1) Have no prior acquaintance with the suspects they deceive; and (2) Confine their dealings to impersonal business transactions, there is no reason to say that the Fourth Amendment is implicated at all. This conclusion remains sound even when recording devices are used. If an undercover operation doesn't interfere with a privacy interest, then the fact that a recording device was used doesn't transform it into a Fourth Amendment concern.³⁸⁸

Now let us turn to the opposite pole—to a setting, described in the Sixth Circuit's opinion in *United States v. Baldwin*, where an undercover operation clearly interferes with interpersonal privacy.³⁸⁹ The operation at stake in *Baldwin* was initiated by the Memphis Police Department when it assigned officer Joseph Hoing to conduct undercover surveillance of Baldwin and the local nightclubs he operated.³⁹⁰ Hoing started out by taking a job as Baldwin's chauffeur and general handyman; later, he became a bartender, and then a manager, of one of Baldwin's

³⁸⁶ *Id.* at 211.

³⁸⁷ For a discussion of such operations, see Gary T. Marx, *Police Undercover Work: Ethical Deception or Deceptive Ethics?*, in *POLICE ETHICS: HARD CHOICES IN LAW ENFORCEMENT* 83-115 (W. Heffernan & T. Stroup eds., 1985).

³⁸⁸ This argument provides support for the Court's conclusions in *Lopez v. United States*, in which a federal official secretly taped conversations with a bar owner after the owner offered the official a bribe not to enforce the law. *Lopez v. United States*, 373 U.S. 427, 430-32 (1963). The factual account in *United States v. White*, is so sparse that one cannot tell how the case would be resolved under the framework presented here. See *United States v. White*, 401 U.S. 745, 746-47 (1971).

³⁸⁹ *United States v. Baldwin*, 621 F.2d 251, 252 (6th Cir. 1980).

³⁹⁰ *Id.*

clubs.³⁹¹ As Hoing became better acquainted with Baldwin, he accepted an offer to share an apartment with him.³⁹² Hoing testified that although he occupied the downstairs bedroom and Baldwin the one upstairs, he had free access to all parts of the house.³⁹³ While in Baldwin's bedroom, he testified, he discovered on two different occasions white powder on a tabletop; the police laboratory analyzed the samples he provided and determined each was cocaine.³⁹⁴ Hoing also found white powder while cleaning the floorboard of Baldwin's car; a sample of this powder established that it, too, was cocaine.³⁹⁵ Baldwin was subsequently convicted for possession of cocaine.³⁹⁶

Here, then, is a particularly strong instance of a close, personal relationship created in the course of an undercover operation. Admittedly, courts face difficult problems in identifying such a relationship when parties claim friendship but not some other tie such as shared membership in a nuclear family or joint use of living quarters. The latter, however, is just what is at stake here. Indeed, there are few more serious tokens of trust than the granting of unlimited access to one's living quarters. We can thus say that a relationship of reciprocal, interpersonal trust exists when each party has given the other unimpeded access to jointly shared physical property. Moreover, we can also say that although mutual betrayal may well be acceptable under the Fourth Amendment (an issue that will be considered shortly), an operation in which a government agent deceptively creates the conditions of reciprocal trust amounts to a search (because it interferes with interpersonal privacy) within the meaning of the Amendment.

Given Supreme Court precedents on this issue, a lower court would, however, be hard-pressed to reach this conclusion. Certainly the Sixth Circuit was unwilling to do so in *Baldwin*. Citing two leading Supreme Court decisions on point—*Hoffa v. United States*,³⁹⁷ and *Lewis v. United States*.³⁹⁸—the Sixth Circuit

³⁹¹ *Id.*

³⁹² *Id.*

³⁹³ *Id.*

³⁹⁴ *Id.*

³⁹⁵ *Id.*

³⁹⁶ *See id.* at 252.

³⁹⁷ 385 U.S. 293 (1966).

³⁹⁸ 385 U.S. 206 (1966).

rejected Baldwin's claim that, acting in the absence of the probable cause and a warrant, Hoing conducted a search within the meaning of the Amendment when he took up residence in Baldwin's home.³⁹⁹ The court used *Hoffa* to affirm the vigilance theme that runs throughout the Court's jurisprudence operations—that the Fourth Amendment never offers protection against misplaced confidence in a friend.⁴⁰⁰ It then read *Lewis* to mean that a government official can legitimately gain entry to a home through misrepresentation of his identity.⁴⁰¹

We have already seen that Chief Justice Warren's *Lewis* opinion emphasized the extent to which *Lewis* had transformed his home into a place of business. When we review *Hoffa*, we shall see that the misplaced confidence in that case did not involve false friendship created *ab initio* by the government.⁴⁰² The Sixth Circuit thus had some room to maneuver. However, had it held the Fourth Amendment to have been implicated at the time Hoing moved into Baldwin's home, it would have had to rule not only in the absence of a Supreme Court precedent on the subject but also in the absence of any Court dicta indicating that there might be Fourth Amendment limits for undercover operations. Clearly, the doctrinal responsibility here is the Court's, not that of the lower courts.

Baldwin illustrates how intrusive police undercover operations can be under current law. What makes the case particularly significant is that it reminds us that the Court's "misplaced confidence" doctrine extends to relationships where intimacy is falsely established from the outset by government agents.⁴⁰³ Two features of the government operation deserve particular notice. First, Hoing was engaged in an indiscriminate, judicially unsupervised search from at least the moment he took up residence with Baldwin.⁴⁰⁴ A warrant should be required for such a search for the same reason that a warrant is currently required when police (who are identified as police) enter a home and then go through its contents looking for evidence of crime. On this analysis, an undercover agent

³⁹⁹ 621 F.2d at 252.

⁴⁰⁰ *Id.* at 252-53.

⁴⁰¹ *Id.*

⁴⁰² See notes 414-21 *infra* and accompanying text.

⁴⁰³ See notes 399-401 *supra* and accompanying text.

⁴⁰⁴ *Id.*

such as Hoing can properly be characterized as a perpetual audio and visual recording “device,” providing information about the entire range of intimate activities within a home.

Second, *Baldwin* is a case of outsider, not insider, betrayal. It is not a case in which an insider decides to betray another insider. Troubling as such conduct is, it must be understood to trump norms of trust within interpersonal privacy given a liberal society’s commitment to personal autonomy. In *Baldwin*, however, we have an outsider planning to abuse the trust he expects to gain. Conduct such as this is condemned when a gossip engages in it to secure information he wishes to have. Given the Fourth Amendment’s baseline of privacy norms in everyday life, it is also to be condemned when the government engages in it—and perhaps to be condemned even more strongly given the resources available to the government for penetrating interpersonal privacy.

Now let us turn to clear cases of betrayal by insiders. As I have just suggested, the rationale for permitting insider betrayal is to be found in a liberal society’s commitment to norms of personal choice—in its commitment to letting people decide for themselves whether to sacrifice, for the sake of some other good, the trust established through mutual intimacy. A few evidentiary privileges do accord priority to personal trust.⁴⁰⁵ The norms of interpersonal privacy, which cover many relationships besides those protected by evidentiary privileges, don’t extend so far, however. These norms condemn outsider insinuation of intimacy for the purpose of betrayal (think of *Baldwin*, for example). At the same time, they recognize the risk of betrayal by an insider as a necessary concomitant of the freedom to choose intimates.

Given this general framework, the question courts must ask is whether the government has used its power to induce an insider to betray another. Admittedly, such a question will sometimes be difficult to resolve given the range of inducements available to the government in such settings. Some clear examples of betrayal freely decided upon can,

⁴⁰⁵ “The essence of the [marital] privilege is to protect *confidences* only The purpose is to insure subjectively the unrestrained privacy of communication, free from any fear of compulsory disclosure.” 8 WIGMORE ON EVIDENCE 648 (John McNaughton ed., 1961). Other privileges also protect relationships of trust: the attorney-client privilege, *see id.* at 541; physician-patient privilege, *see id.* at 818; and priest-penitent, *see id.* at 869.

however, be found—though they can be located only by going beyond reported cases since, quite understandably, there has been no litigation about betrayals undertaken without government prompting. A particularly telling instance of betrayal without government prompting is to be found in Whittaker Chambers' decision to turn on Alger Hiss. In discussing the Chambers-Hiss case, I take no position on the truth of the charges each advanced against the other. Rather, my concern is with facts not in dispute, in particular with the fact that Chambers was involved on a personal basis with Hiss prior to the betrayal and that Chambers provided evidence to the government without any prompting from it.

Chambers's conduct is of particular interest because he has written movingly about what it means to turn on a friend. In his 1952 memoir, *Witness*, Chambers sought to justify his decision to inform on Hiss; at the same time, he emphasized how sullied he felt by the entire experience. The informer, he wrote, "risks little":

He sits in security and uses his special knowledge to destroy others. He has that special information to give because he knows those others' faces, voices and lives, because he once lived within their confidence, in a shared faith, trusted by them as one of themselves, accepting their friendship, feeling their pleasures and griefs, sitting in their houses, eating at their tables, accepting their kindness, knowing their wives and children [T]he police protect him. He is their creature. When they whistle, he fetches a soiled bone of information.⁴⁰⁶

This third person account captures well the tension between loyalty and betrayal in Chambers's own experience with Hiss. In testimony Hiss ultimately did not challenge, Chambers revealed that during the mid-1930s, he and his wife, on befriending the Hisses, often dined with them at their home, sometimes stayed as overnight guests as well, received from them the gift of a car, and went on bird-watching expeditions with them.⁴⁰⁷ When Chambers turned to the government, then, he was turning on a friend, something he often emphasized in his congressional and courtroom testimony.⁴⁰⁸ Even more important for our purposes, Hiss himself was unable to identify

⁴⁰⁶ WHITTAKER CHAMBERS, *WITNESS* 454 (1952).

⁴⁰⁷ See SAM TANENHAUS, *WHITTAKER CHAMBERS: A BIOGRAPHY* 272-73 (1997).

⁴⁰⁸ See *id.* at 273.

any mercenary motive on Chambers's part in turning to the government.⁴⁰⁹

The uncontroverted facts about Chambers's decision to go to the government were that he did so in September 1939, immediately after the signing of the Soviet-Nazi nonaggression pact; that he did not gain immunity from prosecution for the information he provided; and that, in confessing he had been a courier for a Soviet spy ring in the mid-30s, he named Hiss and about a half dozen other officials of the American government as people who had provided him with information.⁴¹⁰ Whether Chambers *accurately* identified Hiss as a Soviet agent is still a matter of controversy.⁴¹¹ That he did so without inducement from the government—and that his testimony involved betrayal of a formerly close friend—cannot be open to doubt.⁴¹²

We can summarize a complex argument by noting the following points. First, deceptive government undercover operations do not implicate the Fourth Amendment when the relationship at stake is simply an impersonal business transaction. Second, even when interpersonal privacy is at stake, an insider's decision to betray another insider has no relevance to the Fourth Amendment as long as the government has taken no steps to induce the insider's betrayal. But third, the Fourth Amendment is indeed implicated when an undercover government agent deceptively forms a relationship of interpersonal privacy. We have concentrated so far on straightforward cases illustrating each of these points. Let us now turn to problem cases.

⁴⁰⁹ In his 1988 memoirs, for example, Hiss did not allege that Chambers acted for money. Rather, he characterized Chambers as "a possessed man and a psychopath." ALGER HISS, *RECOLLECTIONS OF A LIFE* 207 (1988).

⁴¹⁰ See *id.* at 162. Chambers's biographer, Sam Tanenhaus, reports that Chambers turned to the United States government immediately after learning about the Soviet-Nazi pact of August 23, 1939. *Id.* at 159. Chambers divulged his past, and also presented evidence of a Soviet spy ring in Washington, in a conversation with Adolf A. Berle, Assistant Secretary of State, on September 1, 1939, the day after the Germans began their invasion of Poland. *Id.* at 162.

⁴¹¹ Sam Tanenhaus, Chambers's biographer, reports on evidence discovered in 1993 in Moscow archives, tending to suggest that Hiss was indeed a Soviet agent. See *id.* at 518-19.

⁴¹² It must be borne that it was only after the Nazi-Soviet pact was signed (on August 23, 1939) that Chambers decided to speak to government officials about his work as a Soviet agent. See *id.* at 159.

2. Harder Cases

The framework provided so far for thinking about interpersonal privacy has the distinct advantage, when compared with the Court's approach, of tracking the norms of everyday life. It emphasizes the difference between business and personal relationships; it allows for a distinction between use of the home as a place of business and the home used for intimate association; it also brings out the difference between betrayal initiated by an insider and betrayal induced by an outsider, such as the government. The Court's approach, on the other hand, makes allowance for none of these subtleties. Its sole virtue is ease of application. Indeed, because it allows the government free rein in undercover operations, at least as far as the Fourth Amendment is concerned, the Court's approach poses no problems of application whatsoever. The question we now confront is whether the difficulties that of course do arise in applying the everyday distinctions of privacy norms are so severe as to make the Court's "anything goes" framework superior. I suggest here that these difficulties are manageable, that in most instances, courts will be apply the categories of everyday experience in a principled way, and that the Supreme Court's approach should thus be repudiated.

Let us begin with the boundary question of where a business relationship ends and a personal one begins. *Lewis v. United States* provides us with a clear example of a relationship on the business side of this line, and *United States v. Baldwin* provides us with an equally clear example of a relationship that had become personal.⁴¹³ The facts in a case decided on the same day as *Lewis*, *Hoffa v. United States*,⁴¹⁴ show how the line can be blurred. While on trial on another matter, James Hoffa, president of the Teamsters Union, was frequently visited in his hotel room by Edward Partin, an official of a Teamsters local in Louisiana who was already acquainted with Hoffa.⁴¹⁵ At the time he made visits to the Hoffa hotel suite, Partin had already received two substantial benefits from the government: (1) He had been released on bail on a state criminal charge; and (2) Proceedings on a federal indictment had been postponed.⁴¹⁶ Hoffa was, of

⁴¹³ See *supra* notes 379-80 and accompanying text.

⁴¹⁴ 385 U.S. 293 (1966).

⁴¹⁵ *Id.* at 296.

⁴¹⁶ *Id.* at 298.

course, unaware of the fact that Partin was regularly reporting to the government about the plans Hoffa was formulating in his hotel room to bribe jurors in his current trial.⁴¹⁷ Partin's testimony about Hoffa's jury-tampering efforts proved critical in obtaining Hoffa's conviction on that charge.⁴¹⁸ Moreover, after testifying against Hoffa, Partin received further government benefits: state and federal charges against him were dropped, and his wife received four monthly installments of \$300 from government funds.⁴¹⁹

That Partin was induced to betray Hoffa is clear, then. Does this mean, though, that the Fourth Amendment was implicated by the betrayal? The Court, applying its free rein approach to undercover operations, answered this question in the negative. Hoffa, it asserted, was acting on his "misplaced belief" in Partin and so was not entitled to judicial protection.⁴²⁰ This, of course, is hardly a satisfactory answer, for it ignores the difference between misplaced confidence in a friend who chooses betrayal and misplaced confidence in someone who has been induced by an outsider to engage in betrayal. But even if the Court's analysis is too facile, one might argue that if Partin and Hoffa were merely business associates—as long as they never developed a relationship that extended beyond the discussion of Teamster business—then the government didn't interfere with Hoffa's privacy in using Partin as an agent.

This is surely a plausible argument. The problem, of course, is that it relies on terms such as "business associate" and "friend," terms that admit of differing degrees of strength. If courts were assigned the job of finding a mid-point on the continuum where a business associate, or an acquaintance, becomes a friend, the prospects for principled, consistent decision-making would be bleak indeed. Such an approach is unnecessary, however, for another framework is possible, and preferable. It is reasonable to suppose that when someone such as Partin—someone who has had business dealings in the past with his target for surveillance—enters the target's hotel room

⁴¹⁷ The *Hoffa* Court proceeded "upon the premise that Partin was a government informer from the time he first arrived in Nashville [where the Hoffa trial was taking place] . . . and that the Government compensated him for his services as such." *Id.* at 299.

⁴¹⁸ *Id.* at 296.

⁴¹⁹ *See id.* at 297-99.

⁴²⁰ *Id.* at 302.

on a broadly defined mission to find evidence of criminality, the person conducting the surveillance will be exposed to at least some of the exchanges typical of friendship. Partin's access to Hoffa's suite is, in this respect, distinguishable in principle from "Jimmy the Pollack's" access to Lewis's home.

In *Lewis*, Lewis as homeowner set the terms for a carefully circumscribed business relationship.⁴²¹ Because nothing of the sort can be said of Partin—because Partin was, in effect, a roving audio and visual device for the government—a warrant should have been required for his entry into Hoffa's suite. As a general matter, then, we can say that whenever an undercover agent will have a reasonable opportunity to gain access to private facts in the course of his work, a warrant should be required prior to his undertaking it. As the agent undertakes his work, he may in fact encounter nothing that can be classified as a private object or information. But this can't be known in advance. The critical point is that there is a reasonable likelihood of this. There having been no such likelihood in *Lewis*, a warrant wasn't required in that case. The likelihood having been present in *Hoffa*, a warrant should have been required there.

Now let us turn to another boundary-defining issue: the question of when the government can be said to have induced a betrayal. A troubling decision by the Supreme Court—troubling because it is not palpably wrong, but also not entirely satisfactory—is the 1974 case of *United States v. Matlock*.⁴²² This case helps to illustrate the problems at stake. In *Matlock*, evidence of the defendant's crime was obtained through a third party's consent to search his home. Aware that Matlock shared a home with his girlfriend, Gayle Graff, police officers didn't ask him for permission to search the home.⁴²³ Instead, after arresting him in the yard of the home, they went to the front door and asked Graff for permission to search.⁴²⁴ Although Graff later claimed she never consented to the search, the trial court concluded she had voluntarily done so.⁴²⁵ On searching the home, the officers found a gun and about \$5000 in cash in a

⁴²¹ Thus the significance of the Court's remark that Lewis "converted [his home] . . . into a commercial center to which outsiders [were] invited for purposes of transacting unlawful business . . ." 385 U.S. at 211.

⁴²² 415 U.S. 164 (1974).

⁴²³ *Id.* at 166.

⁴²⁴ *Id.*

⁴²⁵ *Id.*

diaper bag in the closet of a bedroom Matlock shared with Graff.⁴²⁶ This evidence was later used to convict him of bank robbery.⁴²⁷

If Graff had gone to the police and invited them to search her bedroom, this would be a clear case of betrayal initiated by an insider. Under those circumstances, the Fourth Amendment would be irrelevant to the search; indeed, an insider's betrayal would not implicate the Amendment whether the insider's motive was to even a score or to help in solving a crime. By contrast, if the police had offered Graff money in order to gain her permission to search, the case would involve betrayal induced by an outsider, with the result that the police effort to obtain evidence would (according to the principles outlined earlier) have to be characterized a search within the meaning of the Amendment.

Graff's actual conduct falls between these extremes. On the facts found by the trial court, Graff consented to the search.⁴²⁸ But did she do so while fearing reprisal from the police in the event of a refusal? Or did she believe at the moment of consent that she could say "no" without further complication? The *Matlock* record is too bare to provide an answer to these questions. Two factors, however, make the fear-of-reprisal hypothesis worth considering. First, as the Court emphasized, at the time police sought her permission to search, they did not warn Graff she had a right to refuse their request.⁴²⁹ This omission was consistent with Fourth Amendment practice. Although the Supreme Court has established elaborate safeguards to protect waivers in Fifth⁴³⁰ and Sixth Amendment⁴³¹ cases, it declined in *Schneekloth v. Bustamonte*,⁴³² decided a year

⁴²⁶ *Id.* at 166-67.

⁴²⁷ *Id.*

⁴²⁸ *Id.* at 166.

⁴²⁹ *See id.* at 167 n.2.

⁴³⁰ *See* *Dickerson v. United States*, 530 U.S. 428 (2000) (holding that safeguards for custodial interrogation established in *Miranda v. Arizona*, 384 U.S. 436 (1966), are of constitutional dimension).

⁴³¹ *See* *Johnson v. Zerbst*, 304 U.S. 458 (1938) (first announcement of waiver rules for assistance of counsel at criminal trials); *see also* *United States v. Wade*, 388 U.S. 218 (1967) (first announcement of rules for assistance of counsel at post-indictment, pre-trial lineups).

⁴³² 412 U.S. 218 (1973). It should be noted that *Schneekloth* was decided after the search was conducted in *Matlock*. *Schneekloth's* holding that no warning is required for Fourth Amendment consent did not undermine the government's position in *Matlock*. *See* *United States v. Matlock*, 415 U.S. 164, 167 n.2 (1974) ("*Schneekloth* . . .

before *Matlock*, to take a similar approach to Fourth Amendment rights.⁴³³ But while no warning was, legally required, the fact that none was given must be considered in light of another factor—Graff's denial that she ever consented to a search.⁴³⁴ Graff's denial may have been truthful, in which case there was no betrayal at all. The more interesting possibility, however, is that she agreed to the search out of fear of police reprisal and later, on hearing from a lawyer that she could have said "no" without repercussion, denied giving consent.

If we assume for a moment that this hypothesis is correct, can it be said that the government induced Graff to betray *Matlock*? The answer to this is not entirely clear. If someone (a particularly timid person, for example) unreasonably fears reprisal for a refusal when none is likely, then the person making the request can hardly be held responsible for the assent given. It's possible this was true of Graff. But a quite different possibility also has to be considered. If: (1) The person asked reasonably fears that refusal might cause displeasure and bring about police harassment; and (2) The officer making the request is aware of this fear and willingly exploits it to gain consent, then the government can indeed be said to have induced the consent. If this was true in Graff's case—if, for example, she reasonably feared that saying "no" to the search would lead to police harassment—then the government may have induced her betrayal of *Matlock*.

How should courts inquire into the issue of government-induced betrayal when conducting suppression hearings? The answer to this is straightforward. Indeed, no new rule is needed to deal with this concern, for trial courts need only heed *Schneckloth's* warning that "account must be taken of subtly coercive police questions, as well as the possibly vulnerable subjective state of the person who consents."⁴³⁵ *Schneckloth* was of course concerned with first party consent. Its framework, however, is also relevant to third party consent—or at least it is assuming a judicial commitment to the protection of

has . . . made clear, of course, that it is not essential for the prosecution that the consentor knew of the right to refuse consent in order to establish that the consent was voluntary.")

⁴³³ *Id.* at 227.

⁴³⁴ See 415 U.S. at 166.

⁴³⁵ 412 U.S. at 229.

interpersonal privacy. Given such a commitment, the proper resolution of *Matlock* should have been a remand to determine whether Graff was confronted with “subtly coercive” pressures to grant access to the space she shared with Matlock.⁴³⁶ Careful inquiry into such pressure is essential to protect interpersonal privacy from government interference.

Now let us turn to one last type of hard case, “hard” not because of a problem of boundary-definition but because an effective law enforcement technique stands in possible tension with the value of interpersonal privacy. When government officials offer a reward for the capture of a criminal, there can be no doubt that intimates who respond to the reward have been induced to do so by the government’s offer. Similarly, if an official offers an arrestee the chance of leniency if the arrestee will implicate someone he knows well, there can be no doubt that the official has offered an inducement. Because the government’s use of an inducement is unmistakable in these settings, the issue at stake is not one of boundary-definition. Rather, it is one of constitutional legitimacy, for government inducements to provide information about criminals are, on the one hand, highly effective law enforcement measures and, on the other, problematic given the Fourth Amendment commitment to protecting interpersonal privacy. If such inducements invariably implicate the Fourth Amendment, law enforcement would be severely hampered—hardly a palatable outcome. On the other hand, to uphold such inducements in every case would require rejection of the principle of interpersonal privacy—also an unacceptable outcome.

As it happens, each pole can be avoided. Let us note first why inducements don’t invariably implicate the Fourth Amendment. This point is easily made if we consider conduct that has nothing to do with interpersonal privacy. If, for example, a person who is unacquainted with the target of a government investigation sees the target on a street and, responding to a cash offer for help in leading to the target’s capture, calls the police, there is no sense in which interpersonal privacy can be said to be involved. Similarly, if a

⁴³⁶ *Matlock* was in fact remanded. See 415 U.S. at 171, 177-78. However, the Court remanded it not to consider the question posed here, but instead, to consider whether Graff had “common authority over or other sufficient relationship to the premises or effects sought to be inspected.” *Id.*

person's dealings with, say, a drug dealer have been limited to illicit purchases, interpersonal privacy cannot be at stake. Moreover, even when the Fourth Amendment *is* implicated, there will be many occasions when government inducements to betray will easily pass constitutional muster. If government officials have probable cause to believe that someone has committed a crime, an offer of a cash reward for the person's capture will then be constitutionally acceptable. With probable cause having been established, government interference in interpersonal privacy would be justified.

If we turn to the other pole—inducements that *do* implicate the Fourth Amendment—we will see that there are indeed troubling cases, that protection of interpersonal privacy will, on some occasions, undercut efficient law enforcement, but that this interference must be deemed salutary if we also value interpersonal privacy. The starting point for inquiry is this: what if an inducement is offered when probable cause has *not* been established? For example, what if a major crime has been committed and government officials, completely baffled about the identity of the perpetrator, offer a cash reward to anyone who provides information leading to the perpetrator's arrest and conviction? Here, a serious constitutional issue arises once interpersonal privacy is treated as a Fourth Amendment value, for the government's offer of a reward could induce an intimate to betray the perpetrator. A poignant instance of this can be found in the unabomber case, where David Kaczinski, in responding to an FBI cash offer for help in capturing and convicting the unabomber, provided critically important information about his brother Ted. The information David offered had little to do with Ted's actual crimes; David knew nothing of these. Rather, it had to do with Ted's habits of thought and way of life, matters that Ted undoubtedly wanted to keep private and that David had come to know through the development of a relationship of trust as he lived with his brother in Texas.⁴³⁷

Because the Court has shown no concern for interpersonal privacy, the FBI proceeded to interview David without having to consider David's betrayal of his brother's trust. The question we must ask is how a law enforcement agent could take steps to minimize the effects of such a betrayal while also fulfilling its

⁴³⁷ See ROBERT GRAYSMITH, UNABOMBER: A DESIRE TO KILL 377-385 (1997).

crime-solving function. The best way to answer this question is to consider the Court's reasoning in *United States v. Sokolow*, which approved the use of profiling research as a tool for establishing reasonable suspicion.⁴³⁸ The particular kind of profiling at stake in *Sokolow* had to do with drug couriers.⁴³⁹ But law enforcement agencies, it is important to understand, use profiles in other contexts as well.⁴⁴⁰ Certainly profiles are a particularly helpful tool in cases where an anonymous perpetrator has repeatedly inflicted violent harm on others. Whatever the aim of a profile, its effect is to focus police attention on a cluster of factors, none of which involves illegal conduct, but that when "taken together . . . amount to reasonable suspicion."⁴⁴¹ In *Sokolow*, the drug courier profile included (1) paying for plane tickets with cash, (2) traveling to cities that are a source for illegal drugs, (3) staying in such cities for less than forty-eight hours, and (4) having no luggage to check.⁴⁴² For complex cases such as that of the unabomber, an individualized profile is developed, one that tries to capture the characteristics of a perpetrator simultaneously conversant with the technology of death and with the rhetoric of those opposed to technology.

Working with an individualized profile of this kind, government officials can limit the scope of the interviews they conduct with people volunteering information. If someone volunteers information that has no bearing on the profile from which they are working, the police can terminate the interview quickly. By contrast, if the information provided corroborates the profile, the police will have established reasonable suspicion, which in turn will justify further investigation of the details of the suspect's personal relationships. This cautious, stage-by-stage approach will undoubtedly frustrate some law enforcement investigation, but it will do so for the sake of the privacy values that lie at the heart of the Fourth Amendment. Moreover, there is reason to believe that the frustration will not be substantial. The "reasonable suspicion" standard will allow the government substantial leeway in conducting investigations.

⁴³⁸ *United States v. Sokolow*, 490 U.S. 1, 7-11 (1989).

⁴³⁹ *Id.* at 10 n.6.

⁴⁴⁰ See generally BRENT E. TURVEY, *CRIMINAL PROFILING: AN INTRODUCTION TO BEHAVIORAL EVIDENCE ANALYSIS* (1999).

⁴⁴¹ *Id.* at 9.

⁴⁴² See *id.* at 8-9.

To insist on more would be to discount privacy interests for the sake of unimpeded investigative power.

CONCLUSION

In giving meaning to *Katz's* reasonable expectations test, the Supreme Court has produced a caricature of the privacy norms that prevail in everyday life. On the Court's account, privacy is a matter of constant vigilance. It is available only to people who seek full concealment for objects and information; it is achieved only through assumption of risk through betrayal by government informants; and it offers no protection against those outsiders who wish to subject insiders' conduct to permanent surveillance. By contrast, I have argued that the privacy conventions of everyday life are best understood in terms of a forbearance model, one that requires individuals seeking privacy to take certain reasonable steps to indicate their desire for it but that then requires restraint on the part of outsiders. In this Article, I have outlined the key features of the forbearance model, explained how it applies to both the solitary individual and to interpersonal privacy, and then used the model to assess critically the Court's post-*Katz* decisions. Were the Court to adopt the forbearance model, the result, I have contended, would be a jurisprudence that captures the privacy norms of everyday life and that thus places modest, but wholly justified, limits on law enforcement activities.