TECHNOLOGY AND THE THRESHOLD OF THE FOURTH AMENDMENT: A TALE OF TWO FUTURES

James J. Tomkovicz[*]

I. INTRODUCTION

The notion that technological developments are mixed blessings is hardly a novel or recent revelation. Others have observed that the enhancements of human abilities afforded by innovative technologies are quite typically swords with two very sharp edges.[1] Our lives are both immeasurably en

[*] Professor of Law, University of Iowa College of Law.

I am enormously indebted to Professor Thomas Clancy and the National Center for Justice and the Rule of Law for the invitation to participate in this symposium and for the generous funding that enabled me to develop the thoughts in this article. My initial involvement in the issues explored in this article was as an advocate and friend of the Court in *Kyllo v. United States*, 533 U.S. 27 (2001). *See* Brief of Amici Curiae National Association of Criminal Defense Lawyers and The American Civil Liberties Union, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508). In that role, I was required to focus on the limited issue raised by the *Kyllo* case. Although I did have the opportunity to propose a general standard for evaluating the relationship between technology and Fourth Amendment regulation, I was constrained by the clients' wishes and by the primary objective–prevailing in the case before the Court. As a participant in this Symposium, I have been freed to examine the broader context, have been afforded the opportunity for impartial, dispassionate exploration of the questions raised, and have been afforded the invaluable benefits of critical insights from others with expertise in this field. A scholarly perspective has made it evident that the larger issue that underlay *Kyllo* is much more complex than I had thought while working on the brief in that case. The opportunity and the obligation to consider every angle and ramification have prompted a realization that difficult distinctions and analytical quandaries abound. I am much less sure now that I have or will ever arrive at the "right" answers. I believe I will be able to shed some light on some of the darker recesses of the maze. In so doing, I hope to advance the discussion at least a few steps in the right direction.

I wish to thank the other participants in this symposium–Professors John Burkoff, A. Morgan Cloud, Tracey Maclin, David Sklansky, Christopher Slobogin, and Kathryn Urbonya–for their most helpful insights. I am also indebted to Joe Christianson, Sean Helle, and Kyle Kaiser for excellent research and editorial assistance.

The National Center for Justice and the Rule of Law at the University of Mississippi School of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the United States Department of Justice.

[1] *See, e.g.*, Steven R. Salbu, *Symposium: Corporate Governance, Stakeholder Accountability, and Sustainable Peace: The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 657 (2002)

riched and seriously imperiled by advances in science and technology. The firearms that enable us to hunt more efficiently and to defend ourselves against human and nonhuman predators also enable disturbed adolescents to destroy the peace of educational sanctuaries and the lives of schoolchildren.[2] The automobiles that make it possible for us to travel great distances in short periods, bringing friends and families closer together, are deadly projectiles that take our families and friends from us when in the hands of careless or intoxicated drivers.[3] Airplanes magically fulfill humankind's dream of flight and bestow all the freedoms that dream affords, but in the hands of terrorists they have become the source of our worst nightmares.[4] Personal computers and the internet have opened worlds of information and fostered communication thought to be inconceivably futuristic not so long ago, and at the same time have empowered child pornographers and sexual predators with much more effective means of inflicting harm on innocent, defenseless members of our society.[5] While nuclear sources of power have been tamed and used to meet the ever-increasing societal demand for energy, they harbor a terrifying

(observing that the "advantages of technology come at a price" and referring to it as a "double-edged sword"); Michael L. Closen et al., *Notarial Records and the Preservation of the Expectation of Privacy*, 35 U.S.F. L. REV. 159, 173 (2001) (observing that technology is a "double-edged sword . . . because advances that promise to better the lot of society often threaten others in the process"); Jonathan Todd Laba, Comment, *If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imagers, Emerging Technologies, and the Fourth Amendment*, 84 CAL. L. REV. 1437, 1471-72 (1996) (discussing the "`plus' side" and the "`minus' side" of the technological "double-edged sword" in law enforcement contexts).

[2] *See* Greg Krikorian & Michael Krikorian, *Santee School Shootings*, L.A. TIMES, Mar. 6, 2001, at A1; Mark Obmascik, *High School Massacre*, DENVER POST, Apr. 21, 1999, at A1; James Brooke, *School Shootings Bewilder a Hunting Town*, N.Y. TIMES, June 28, 1998, § 1, at 12; *Witnesses Recount Shooting at Mississippi High School*, N.Y. TIMES, June 11, 1998, at A28.

[3] *See* Shari Roan, *Car Deaths Related to Alcohol Increase*, L.A. TIMES, Oct. 1, 2001, at S1; Nedra Pickler, *Drunken Driving Deaths Increase*, SEATTLE TIMES, Sept. 25, 2001, at A12; *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447, 451 (1990) (upholding suspicionless sobriety checkpoint stops as reasonable seizures in part because of the enormous number of deaths and personal injuries and the massive amount of property damage resulting from drunk driving).

[4] *See* Dean E. Murphy & Joel Brinkley, *A Nation Challenged: The Airports; Rethinking Security at Airports*, N.Y. TIMES, Sept. 19, 2001, at B1; *`A National Tragedy': Terrorism Hits New York and Washington*, WASH. POST, Sept. 12, 2001, at C16.

[5] *See* Margarette Driscoll, *Online Academy for Paedophiles*, SUNDAY TIMES (London), June 2, 2002, at 6; John M. Moran, *Ages 13 and 14 Are Magic Numbers for Online Predators*, CHI. TRIB., May 29, 2002, at C1; *Man Held in Slaying of Girl He Met on Web*, CHI. TRIB., May 22, 2002, at N14.

potential for accidental or intentional mass destruction.[6] Beneficent scientific research yields discoveries that save countless lives, developing drugs that ward off deadly diseases. In the wrong hands, however, the work of science can itself be deadly, spreading illness and devastation through unseen, "weaponized" agents.[7] So it has been with technologies of the past. So it is with technologies of the present. And, I venture to say, so it will be with technologies of the future.

The advantages and dangers of technological developments have significant impacts on the lives of individuals, the lives of communities, and, indeed, on the lives of entire nations. The efficacy and efficiency of governments are undoubtedly improved by scientific or technological progress. Social order can better be preserved and safeguarded with the aid of modern mechanisms. Faster cars, lethal weapons and nonlethal "stun guns," accurate DNA testing, computerized records, and electronic monitoring devices are just a few of the tools that have enabled law enforcement agencies to more effectively neutralize threats, detect crimes, apprehend and maintain control over suspects, and convict the guilty. We are all safer thanks to inventions and discoveries that assist those who keep us secure and safe against forces of violence and disorder. We should be grateful indeed for the impressive enhancements of human abilities afforded by research.

Technological devices in the hands of the government, however, are not an unmitigated blessing. Once again, the sword of technology has two razor-sharp edges. While one edge can be employed to preserve a nation's security, the other can imperil its very essence. Constitutional freedoms that define our country and make it a bastion of liberty can be severely diminished, even destroyed, by uses and abuses of the tools of progress. The reality, or even the threat of, unregulated electronic monitoring can chill First

[6] *See* Bill Nichols, *The World's Worst Nightmare Could Begin Quietly*, USA TODAY, June 4, 2002, at A1; Charlie Edgren, *Greater Nuclear Threat Slowly Emerges*, EL PASO TIMES, June 1, 2002, at 10; *Radiation Pills To Be Given Away*, N.Y. TIMES, June 1, 2002, at B4; Bill Keller, *Nuclear Nightmares*, N.Y. TIMES, May 26, 2002, § 6, at 22.

[7] *See* Michael R. Gordon, *U.S.: Al Qaeda Was Building Lab for Bioweapons*, CHI. TRIB., Mar. 24, 2002, at C6; Shannon Brownlee, *Clear and Present Danger*, WASH. POST, Oct. 28, 2001, at W8.

Amendment freedoms of speech, press and association.[8] Pharmacological truth serums that extract confessions against the will of the individual[9] or intrusions of cameras into courtrooms can undermine the Fifth and Fourteenth Amendment guarantees of due process.[10] Videotaped testimony out of an accused's presence can dilute, if not dismantle, the Sixth Amendment entitlement to be confronted with witnesses.[11] And official efforts to listen in on lawyer-client conversations in the name of national security can endanger that same provision's vital assurance of the right to the assistance of counsel.[12] Of greatest significance for present purposes, sophisticated eavesdropping equipment,[13] electronic tracking devices,[14] aerial surveillance,[15] and other tools that dramatically improve upon human perceptual abilities and enable the government to hear, see, and otherwise learn matters the people seek and wish to keep confidential can eviscerate the precious assurance of privacy safeguarded by the Fourth Amendment right against "unreasonable searches." What once were barriers to human senses are easily hurdled, and matters that were once inaccessible to those senses are brought within their reach by the products of innovation.[16]

Some probably believe that the gains afforded by science

---

[8] *See* Bartnicki v. Vopper, 532 U.S. 514, 533 (2001) (observing that the fear of being monitored can "`have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas'" (quoting PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967))); *see also* Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting); United States v. White, 401 U.S. 745, 764-65 (1971) (Douglas, J., dissenting); Lopez v. United States, 373 U.S. 427, 452 (1963) (Brennan, J., dissenting).

[9] *See* Townsend v. Sain, 372 U.S. 293, 308-09 (1963).

[10] *See* Chandler v. Florida, 449 U.S. 560, 581 (1981) (broadcast coverage of criminal proceeding, though not a *per se* violation of due process, can violate right to fair trial); Estes v. Texas, 381 U.S. 532, 535 (1965) (broadcast coverage of pretrial and trial proceedings did violate accused's entitlement to due process).

[11] *See* Maryland v. Craig, 497 U.S. 836 (1990); *id*. at 860, 861 (Scalia, J., dissenting).

[12] *See* Matthew Purdy et al., *A Nation Challenged: The Law: Bush's New Rules to Fight Terror Transform the Legal Landscape*, N.Y. TIMES, Nov. 25, 2001, § 1A, at 1; George Lardner, Jr., *U.S. Will Monitor Calls to Lawyers: Rule on Detainees Called `Terrifying,'* WASH. POST, Nov. 9, 2001, at A1.

[13] *See, e.g.*, United States v. White, 401 U.S. 745, 748 (1971).

[14] *See, e.g.*, United States v. Karo, 468 U.S. 705, 721 (1984); United States v. Knotts, 460 U.S. 276, 285 (1983).

[15] *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450 (1989); California v. Ciraolo, 476 U.S. 207, 213 (1986).

[16] For a thorough discussion of an array of technological innovations that pose serious threats to interests in the privacy of information about our lives, see A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468-1501 (2000).

and technology are not worth the risks and costs and would resolve the inevitable tension by halting the march of technological progress. I suspect that most of us, believing it is neither desirable nor possible to stand in the way of the juggernaut, prefer to embrace the advantages of scientific advancement while guarding against becoming the unwitting victims of our own genius. The latter approach seems sensible when addressing the exploitation of technological devices by those who enforce and administer our criminal justice system. There is nothing inherently objectionable about the government taking advantage of scientific and technological progress. We ought to support and endorse uses that promote greater safety and security by making police officers and prosecutors more effective. To require those who keep order to eschew the tools that improve their efficacy–especially when those who threaten social order are more than willing to use innovations to achieve their objectives–seems patently foolish. At the same time, vigilance against exploitations of novel developments that endanger the liberties at the core of our constitutional system seems equally essential. Official uses of technology that effectively circumvent and undermine the protections of liberty deemed fundamental to our nation's character and integrity are genuinely objectionable, even insidious. It is incumbent upon us to promote the government's exploitation of technology, but to keep it in check, to ensure that the sword is used to promote our nation's health and survival without threatening its spiritual vitality, and, indeed, its very identity.[17]

This article focuses on one relatively narrow, but quite significant, aspect of the delicate balance that needs to be struck when assessing law enforcement's use of scientific and technological advances. The concern here is with the relationship between technological developments and the "threshold" of the Fourth Amendment.[18] The central question

[17] I come to this project neither to praise the virtues nor to denounce the vices of science and technology. I think it is important to bring a balanced perspective to the task. I have a genuine appreciation for the special advantages I have as a result of those who spend their lives dreaming and devising new ways to expand the human potential. I am delighted that they equip those who labor to protect my family with ever more effective means of doing so. But I am also aware of and deeply concerned by the potential destructive impacts on civil liberties and, ultimately, on the character of our nation.

[18] The "threshold" of the Fourth Amendment refers to the dividing line

I address is when an exploitation of technology should be governed by Fourth Amendment constraints upon unreasonable searches.[19] The effort is to ascertain a constitutionally appropriate distinction between enhancements of human capabilities that should not be matters of Fourth Amendment concern and those enhancements that ought to be regulated by Fourth Amendment strictures. The sole objective is to determine which devices should be able to promote societal safety unfettered by Fourth Amendment demands and which ought to be restricted by that provision's "reasonableness" requirement.[20] As will become clear, the quite simple legal inquiry is when a use of technology should be deemed a

between those official actions that are governed by that provision and those that are beyond its reach. The decision by the National Center for Justice and the Rule of Law to devote this inaugural symposium to the relationship between technology and the Fourth Amendment is gratifying. Few subjects could be more significant or timely. I have often bemoaned the fact that the guarantees of that Bill of Rights provision are unappreciated by the people for whom it was adopted. The abusive practices that prompted this fundamental constitutional safeguard were deeply resented by our ancestors. *See* David Rudovsky, *The Impact of the War on Drugs on Procedural Fairness and Racial Equality*, 1994 U. CHI. LEGAL F. 237, 242. Their abhorrence of unjustified searches and seizures was so powerful that it was among the primary reasons for the revolution that gained our independence from Britain. *See* Timothy Lynch, *In Defense of the Exclusionary Rule*, 23 HARV. J.L. & PUB. POL'Y 711, 721-22 (2000); T. Taylor, Two Studies in Constitutional Interpretation, 38 (1969); N. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 100 (1937). Too often in modern times, the Fourth Amendment's safeguards are instead viewed as "technicalities" that lead to the release of guilty criminals. This symposium can engender the respect and reverence that the liberties enshrined in the Fourth Amendment deserve and can promote a genuine understanding of the central role that the "right to be secure against unreasonable searches and seizures" plays in defining the character of our free nation. The rapid growth of technological innovation and the graphic, devastating intrusion of terrorism into the daily lives of Americans are forces that jeopardize the vitality of the fundamental freedoms promised by the Fourth Amendment. This is indeed a most opportune time for conscientious and serious reflection upon the intricacies of the relationship between technology and those freedoms.

[19] For other discussions pertaining to this topic, see George M. Dery III & James R. Fox, *Chipping Away at the Boundaries of Privacy: Intel's Pentium III Processor Serial Number and the Erosion of Fourth Amendment Privacy Expectations*, 17 GA. ST. U. L. REV. 331, 338-49 (2000); George Dery III, *Remote Frisking Down to the Skin: Government Searching Technology Powerful Enough to Locate Holes in Fourth Amendment Fundamentals*, 30 CREIGHTON L. REV. 353 (1997); David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1 (1996); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549 (1990); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward An Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645 (1985).

[20] I do not address the subsequent question of when a regulated technological exploitation should be deemed unreasonable and, therefore, unconstitutional.

"search."

As the title suggests, this piece tells "a tale of two futures." One of those futures is the one that was unknown to the Framers of the Constitution but has unfolded in the years between 1791 and 2002. In considering that future–our past–the aim is to describe and evaluate how we have resolved questions involving technology and the Fourth Amendment's threshold. The second future referred to is the one still unknown to us. The objective here is to prescribe constitutionally defensible methods of understanding and resolving the thorny issues raised by the interface between technology and the Fourth Amendment. The article begins by briefly describing the legal background and context in which this particular inquiry arises. In Part II of the piece, I discuss the historical evolution of the Supreme Court's doctrine regarding when any governmental action constitutes a search within the meaning of the Fourth Amendment.[21] This part includes a thorough discussion of the currently controlling "reasonable expectation of privacy" doctrine that has developed over the past thirty-five years.[22] Part III describes and analyzes the modern[23] Supreme Court opinions and holdings concerning the interface between technology and the reach of Fourth Amendment control.[24] The discussion highlights doctrinal nuances particularly pertinent to exploitations of technological devices, constructs categories within which the variables that have proven dispositive or influential can be classified, and critiques the standards that have governed threshold technology determinations. The aim is a clear portrayal of the Supreme Court's understanding of the relationship between technological advances and the reach of the Fourth Amendment and of the potential deficiencies in that understanding. In the final section, Part IV, I venture onto a dangerous limb, proposing a general standard that might promote more defensible, consistent answers to past and future questions regarding whether the exploitation of a

[21] *See infra* notes 26-140 and accompanying text.

[22] *See infra* notes 98-140 and accompanying text.

[23] The term "modern" is intended to refer to those opinions and holdings that have been rendered since the landmark 1967 decision in *Katz v. United States*, 389 U.S. 347 (1967), that revolutionized Fourth Amendment threshold doctrine.

[24] *See infra* notes 141-422 and accompanying text.

novel device amounts to a search.[25] The meaning and intent of this standard are addressed in some detail.

II. AN HISTORICAL AND DOCTRINAL CONTEXT: THE SUPREME COURT'S DEVELOPMENT OF FOURTH AMENDMENT "THRESHOLD" DOCTRINE

The Fourth Amendment is an acknowledgment by the Framers of our Constitution that liberty and social order are in tension with one another. It reflects their best effort to strike and capture the most desirable balance between those two goals. It seems fair to say that their objective was to guarantee the maximum amount of individual freedom that would be possible in a nation that also aspired to be safe, secure, and enduring. They recognized that perfect order was possible only in repressive regimes that suffocate liberties and that unconstrained liberties would prevent self-preservation. Informed by their experiences with the dangerous practices of the British authorities they had revolted against, they provided that the government could engage in searches and seizures, but only if they were "reasonable" and only if warrants to do so met certain limiting requisites.

The balance struck is primarily reflected in the core requirement of reasonableness, but it is also inherent in the decision to limit the Fourth Amendment's coverage to "searches and seizures." The development of constitutionally defensible standards for resolving threshold questions is, thus, a critical part of an effort to honor and implement the Framers' resolution of the tension between order and liberty.[26] The significance of the threshold issue is hard to understate. If the employment of a new investigatory tool *is not a search* at all, it is outside the sphere of Fourth Amendment regulation, and government authorities are at liberty to use it whenever they wish, without need for prior justification. The "people" are wholly unprotected from any impacts the device may have on their lives.[27] On the other

[25] *See infra* notes 423-40 and accompanying text.

[26] Perhaps I should clarify a distinct, though not particularly radical, presupposition that guides and informs my analyses. I do not believe that it is our prerogative to prescribe or alter the constitutional balance. In my view, the central, limiting objective is to discern to the best of our sometimes inadequate abilities the balance intended by those who designed and adopted the Fourth Amendment and to develop governing doctrines that are faithful to that balance.

[27] Officials are, of course, subject to other constitutional and statutory constraints. It is often the case, however, that if a particular activity is not deemed a search, there is no meaningful legal restriction upon the government's

hand, if exploitation of a novel device *is a search*, the government is not free to use it randomly, but is instead constrained by the command of reasonableness that governs entries of homes and other private domains. The infringements occasioned by the use of that device will be kept in check.

These dramatically different effects of determining that a given practice–an exploitation of a particularly technology, for example–is or is not a search highlights the critical importance of the constitutional line that controls the inquiry. Controlling standards that more readily classify an activity as a search slant the constitutional balance in favor of liberty and yield a correspondingly less secure society. Standards that make it difficult for any practice to qualify as a search tip the scales in favor of safety and order at the expense of liberty. For the government, for society, and for each and every individual, the stakes are high indeed.

A. The Evolution of Threshold Doctrine in the Supreme Court

The evolution of Supreme Court threshold doctrine reflects three distinct phases that correspond to three landmark Fourth Amendment decisions: *Boyd v. United States*,[28] *Olmstead v. United States*,[29] and *Katz v. United States*.[30] During the first two periods, each roughly forty years in length, there were relatively few significant Supreme Court decisions. The basic doctrine spawned few embellishing details. The third phase has been distinctly different. In the thirty-five years since it began, a substantial number of significant Supreme Court decisions have generated an array of fascinating, intricate doctrinal specifics. The doctrine born in *Katz* has branched and blossomed as it has been called upon to furnish answers to a variety of difficult, unforeseeable threshold issues. Technological enhancements of human capacities have been the source of many of those issues.

ability to engage in it.

[28] 116 U.S. 616 (1886).

[29] 277 U.S. 438 (1928).

[30] 389 U.S. 347 (1967).

1. The *Boyd* Era: The Purpose of the Governmental Conduct Approach

The Supreme Court did not decide whether a government action was a search until 1886, almost a century after the ratification of the Bill of Rights. *Boyd v. United States*,[31] the Court's initial effort to define the scope of Fourth Amendment regulation, involved legislative, not technological, innovation.[32]

The United States instituted a forfeiture action against thirty-five cases of imported plate glass based on allegations of customs fraud.[33] To prove its case, the government sought information about twenty-nine cases of previously imported glass.[34] Acting under the authority of an 1874 federal statute, a judge issued an order requiring the claimants to produce the invoice for that glass so that the government could examine and copy it.[35] The statute provided that if a party did not comply with a production order the government's allegations concerning what it expected to prove "shall be taken as confessed" and that if the party did comply, the government could introduce what it discovered into evidence.[36] While objecting to the constitutionality of the production order, the claimants complied with the order.[37] They again objected when the government sought to introduce information gleaned from the invoice into evidence.[38] Following a jury verdict for the United States and entry of a judgment of forfeiture, the claimants appealed.[39]

At the outset, the Supreme Court observed that the issue of the reach of the Fourth Amendment[40] was "a very grave

---

[31] 116 U.S. 616 (1886).

[32] *Boyd*, 116 U.S. at 620-23. For scholarly analyses of the *Boyd* decision, see Robert L. Misner, *In Partial Praise of* Boyd*: The Grand Jury as Catalyst for Fourth Amendment Change*, 29 ARIZ. ST. L.J. 805, 811-17 (1997); Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 573-98 (1996); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 419-33 (1995); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 363-65, 377-409 (1974).

[33] *Boyd*, 116 U.S. at 617.

[34] *Id.* at 618.

[35] *Id.*

[36] *Id.* at 620.

[37] *Id.* at 618.

[38] *Id.*

[39] *Id.*

[40] The question of whether the order violated the Fifth Amendment prohibition on compulsory self-incrimination was also before the Court. *Id.* at 621.

question of constitutional law, involving the personal security, and privileges and immunities of the citizen."[41] It documented the ancestry of the 1874 statute, noting that it was passed in lieu of an 1867 enactment authorizing the issuance of warrants to enter premises and search for invoices, books, and papers, which, in turn, had supplanted an 1863 statute granting the authority to issue warrants for that purpose.[42] The Court pointedly observed that the 1863 Act was "the first legislation of the kind that ever appeared on the statute book of the United States,"[43] and that it "was adopted at a period of great national excitement, when the powers of the government were subjected to a severe strain to protect the national existence."[44]

To the contention that the 1874 act authorized unreasonable searches and seizures, the government responded that the process under that statute was "free from constitutional objection, because it [did] not authorize the search and seizure of books and papers, but only require[d] the defendant or claimant to produce them."[45] The Court's resolution of these opposing assertions yielded the first doctrine designed to define the scope of Fourth Amendment regulation.

The Court acknowledged that production orders did not involve "certain aggravating incidents" of the searches and seizures that were the clear targets of Fourth Amendment regulation for there was no "forcible entry into a . . . house [or] searching amongst . . . papers."[46] Nonetheless, the Court concluded that the "compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, [was] *within the scope of the Fourth Amendment . . . because it* [was] a material ingredient, and *effect[ed] the sole object and purpose of search and seizure*."[47] According to the Court, the forcible entries and searches governed by "the Fourth Amendment [were] almost always made for the purpose of compelling a man to give evidence against himself."[48] A compulsory production order

[41] *Id.* at 618.
[42] *Id.* at 619-21.
[43] *Id.* at 621.
[44] *Id.*
[45] *Id.*
[46] *Id.* at 622.
[47] *Id.* (emphasis added).
[48] *Id.* at 633.

"*accomplishe[d] the substantial object* of" those entries and searches and was subject to the same regulatory regime because it "*forc[ed] from a party evidence against himself*."[49] It was "the equivalent of a search and seizure . . . within the meaning of the Fourth Amendment" because "it contain[ed] their substance and essence, and effect[ed] their substantial purpose."[50] In the Court's view, a compulsory production order would not have found favor with our ancestors because it was, quite simply, an "old grievance which they . . . so deeply abhorred" clad in an "insidious disguise[]."[51]

The strong implication of *Boyd* was that any official action with the purpose of compelling a person to furnish incriminating evidence must be treated like the physical entries and searches known to the Framers. Official actions designed to accomplish the same objectives as those searches had to be subjected to Fourth Amendment regulation and satisfy the Fourth Amendment demand of reasonableness. In both design and impact, *Boyd's* "purpose-oriented" approach was expansive.[52] By rejecting the government's assertion that a command to produce papers and a physical entry to look for those papers were entirely different constitutional creatures,[53] the Court refused to confine Fourth Amendment scope to those practices that in physical character resembled the forcible entries experienced by our ancestors. To the *Boyd* majority, the question was one of substance, not form. Official actions would be treated as "equivalent to" searches and seizures or as searches and seizures "in disguise" when their "object and purpose" were the same–to force from a person evidence for use against him.[54]

---

[49] *Id.* at 622 (emphasis added).

[50] *Id.* at 635.

[51] *Id.* at 630.

[52] The *Boyd* Court's attitude toward the interpretation of fundamental guarantees was expansive in character. Toward the end of the opinion, after warning that "illegitimate and unconstitutional practices get their first footing . . . by silent approaches and slight deviations from legal modes of procedure," the Court declared that the "only" way to prevent that result was "by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance." *Id.* at 635.

[53] Concurring Justices in *Boyd* agreed with the government's claim that forced production under a court order was not a search within the meaning of the Fourth Amendment. *See id.* at 639 (Miller, J., concurring) ("There is in fact no search and no seizure authorized by the statute.").

[54] Whether the threshold doctrine employed in *Boyd* was intended to be an exclusive and comprehensive test for whether a search and seizure has occurred is uncertain. The purpose approach may have been intended as simply one way of evaluating a novel technique. It is arguable that the *Boyd* standard was at once both too narrow and too broad a gauge of Fourth Amendment reach. The

2. The *Olmstead* Era: The Textual-Historical-Physical Similarity Approach

Forty-two years passed before another significant issue regarding the breadth of the Fourth Amendment's regulation of searches prompted the Supreme Court to again address the standards for identifying and defining the threshold of the Amendment. *Olmstead v. United States*[55] marks the first in what is now a relatively lengthy series of Supreme Court threshold decisions precipitated by official exploitations of scientific or technological advances. The central question in *Olmstead* was whether wiretapping designed to intercept telephone conversations originating in private homes and offices was a "search" for purposes of the Fourth Amendment.[56]

The *Olmstead* defendants were convicted of a far-reaching conspiracy to violate the National Prohibition Act.[57] "The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers."[58] Without trespassing upon the defendants' property, the officers inserted small wires along the telephone lines leading from their residences

standard was arguably too narrow insofar as it did not encompass government activities that acquired, but did not "force," evidence from an individual. A subsequent decision diminished the force of this criticism by including "stealthy" invasions within the scope of Fourth Amendment coverage. Gouled v. United States, 255 U.S. 298, 306 (1921). It is also arguable that the *Boyd* standard was too narrow insofar as it did not include official conduct when the object was not to investigate. While the Court did refer to privacy and security as Fourth Amendment goals, it did not tie Fourth Amendment coverage to the existence of a privacy invasion. *Boyd*, 116 U.S. at 630. Moreover, the *Boyd* standard was arguably too broad insofar as it seemed to encompass all forcible acquisitions of evidence within the Fourth Amendment's domain. A different understanding of Fourth Amendment aims might lead to the conclusion that not every forcible acquisition of evidence threatens the values that prompted constitutional control of the conventional searches and seizures known to the Framers.

[55] 277 U.S. 438 (1927).

[56] *Olmstead*, 277 U.S. at 439. For scholarly discussions of the *Olmstead* decision, see J. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT (1966); Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 316-20 (1998); Cloud, *supra* note 32 at 609-17; William C. Heffernan, *Property, Privacy, and the Fourth Amendment*, 60 BROOK. L. REV. 633, 638-40 (1994); Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1360-62.

[57] *Olmstead*, 277 U.S. at 455.

[58] *Id.* at 456.

and from their chief office.[59] Agents testified to the contents of incriminating conversations they heard during many months of listening.[60]

The Supreme Court opined that the "well known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers and his effects; and to prevent their seizure against his will."[61] The *Boyd* Court, in fact, had emphasized this core concern with "the misuse of governmental power of compulsion."[62] In addition, "the [A]mendment itself shows that the search is to be of material things–the person, the house, his papers or his effects."[63] These two premises made it clear that the "[A]mendment does not forbid what was done" in *Olmstead*, a situation involving "no searching" and "no seizure" but only "the use of the sense of hearing" and "no entry of . . . houses or offices."[64] According to the majority, that provision does not apply to telephone wires that are "not part of [the] house or office," and while its language is to be "liberally construed to effect the purpose of the framers . . . in the interest of liberty," its words cannot be enlarged "beyond the possible practical meaning of houses, persons, papers, and effects, or so to apply the words search and seizure as to forbid hearing or sight."[65] Telephone users intend to transmit their words to those outside their homes, and neither the wires used to carry their words nor the words themselves are "within the protection of the Fourth Amendment."[66] Without an "official search and seizure of [a] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house `or curtilage' for the purpose of making a seizure," the Fourth Amendment simply is not implicated.[67] Consequently, the wiretapping in *Olmstead* "did not amount to a search or seizure within the meaning of the Fourth

---

[59] *Id.* at 456-57.
[60] *Id.* at 457.
[61] *Id.* at 463.
[62] *Id.* The Court noted that *Gouled v. United States* had "carried the inhibition against unreasonable searches and seizures to the extreme limit" by holding that a "stealthy entrance" was within Fourth Amendment control. *Id.* The Court asserted that the authority of *Gouled* had to be limited to its precise facts, explaining that the surreptitiousness in that case "became the equivalent to an entry by force. There was actual entrance into private quarters . . . and the taking away of something tangible." *Id.* at 463-64.
[63] *Id.* at 464.
[64] *Id.*
[65] *Id.* at 465.
[66] *Id.* at 466.
[67] *Id.*

Amendment."[68]

In essence, *Olmstead* restricted the reach of the Fourth Amendment to the sorts of governmental practices that had been the historical impetus for that guarantee and were described by its literal language and to others that shared certain physical similarities to those practices. Both history and the words employed by the Framers were thought to support the conclusion that a "search" requires a forcible (or at least stealthy) "entry" or "actual physical invasion" of a home, person, or other protected place and that a "seizure" occurs only when officials take possession of a tangible thing–a person, paper, or material effect. The acquisition of intangible verbal communications without physical breaches of protected enclaves did not share the critical attributes of either sort of conduct that the Framers intended to bring under constitutional control.

Despite the Court's explicit endorsement of the view that constitutional provisions designed to protect liberty should be liberally construed,[69] its attitude toward the reach of the Fourth Amendment was unmistakably grudging and its definition of a Fourth Amendment search was exceedingly narrow. Unlike the *Boyd* Court, the *Olmstead* majority did not find the purpose of the law enforcement practice to be significant. Moreover, the *Olmstead* decision reflected a narrow conception of the Framers' objectives. The Court cared not whether wiretapping had impacts on the lives of individuals similar to those effected by physically invasive searches or seizures. The majority's fear that a different conclusion about the relationship between wiretapping and the Fourth Amendment would be unfaithful to history and to the literal terms of the constitutional text prompted it to ignore the powerful arguments of four dissenters who argued that the Court's limiting approach would permit novel developments to undermine constitutional freedoms.[70] The result was a threshold doctrine that hinged on form and had

[68] *Id.*

[69] *Id.* at 465.

[70] One can plausibly argue that the *Olmstead* majority's approach was in fact unfaithful to history. The focus on the specific practices known to the Framers and the confinement of the text to those practices yielded a result that is arguably incompatible with and unprotective of the broader objectives and values that motivated the adoption of shelter against unreasonable searches and seizures. *See id.* at 478-79 (Brandeis, J., dissenting) (discussing textual interpretations in light of changing technology).

little substance, promising that law enforcement use of technological innovations would not be hindered by Fourth Amendment constraints.

Over the next four decades, the Supreme Court decided a number of cases in which it adhered to and relied upon the *Olmstead* doctrine. Each involved the exploitation of a technological tool–an electronic device that enabled officers to enhance their hearing and eavesdrop on conversations that would have otherwise been inaudible. In the first of these decisions, *Goldman v. United States*,[71] officers secured access to an office adjoining one belonging to one of the petitioners.[72] When placed against the wall shared by the two offices, the "detectaphone" they used picked up and amplified conversations occurring in the adjoining office.[73] The Court held that the Fourth Amendment was not implicated, rejecting the petitioners' argument that *Olmstead* was distinguishable because in *Goldman* the speakers had not assumed the risk of interception by projecting their voices outside the office.[74] According to the majority, "no reasonable or logical distinction [could] be drawn between" the conduct in *Goldman* and the conduct in *Olmstead*.[75] Characterizing the *Olmstead* ruling as "the subject of prolonged consideration," the Court refused an invitation to overrule that decision and instead chose to "adhere to the opinion" of the *Olmstead* majority.[76] The *Goldman* majority evinced no doubt about the legitimacy of the restrictive threshold doctrine announced fourteen years earlier.

Another ten years passed before *On Lee v. United States*[77] reached the Court. In that case, a defendant made incriminating statements during a conversation with a government informant who "was wired for sound, with a small microphone . . . and a small antenna" which enabled a federal narcotics agent with "a receiving set" to listen in on the conversation.[78] On Lee objected to the narcotics agent's testimony concerning his incriminating remarks, alleging that the use of the listening device violated the Fourth

[71] 316 U.S. 129 (1942).
[72] *Goldman*, 316 U.S. at 131.
[73] *Id.* at 131-32.
[74] *Id.* at 135-36.
[75] *Id.* at 135.
[76] *Id.* at 135-36.
[77] 343 U.S. 747 (1952).
[78] *On Lee*, 343 U.S. at 749.

Amendment.[79] The Court first rejected the claim that the case was not controlled by the *Olmstead* doctrine because either the informant or the federal agent had "trespassed" onto his premises.[80] No trespass had occurred for there had been no "physical entry either by force, . . . by unwilling submission to authority, . . . or without any express or implied consent."[81] The Court then asserted that even if *Olmstead* was overruled the defendant's claim would lack merit.[82] On Lee "was talking confidentially and indiscreetly with one he trusted" and the government was able to eavesdrop on and overhear his words "with the connivance of" the individual to whom he was speaking.[83] That situation was not analogous to the wiretapping in *Olmstead* in which no party to the overheard conversations either agreed to or facilitated the government's listening.[84]

In sum, there was no search in *On Lee* because there was no physical intrusion of the sort required by the *Olmstead* doctrine. Moreover, even if the demand for a physical entry was eliminated, electronic eavesdropping by the government made possible by the cooperation of a party to a conversation would not trigger Fourth Amendment coverage. *On Lee* both reaffirmed the extant standard and added yet another basis for rejecting claims that particular government conduct—including the use of technology–constitutes a search.

In the early 1960s, the *Olmstead* doctrine began to show its age. In *Silverman v. United States*,[85] the Court sustained a claim that electronic eavesdropping was a search.[86] In that case, officers gained lawful access to a row house and "employed a so-called `spike mike' to listen to what was going on within the four walls of the house next door."[87] The device consisted of a "microphone with a spike about a foot

[79] *Id.* at 750-51.
[80] *Id.* at 752-53.
[81] *Id.*
[82] *Id.* at 753.
[83] *Id.* at 753-54.
[84] *Id.* at 754-55.
[85] 365 U.S. 505 (1961).
[86] *Silverman*, 365 U.S. at 511-12. This was the first time the Supreme Court had held that the use of a technological innovation to secure otherwise confidential information qualified as a search within the meaning of the Fourth Amendment and thus had to satisfy that provision's demands.
[87] *Id.* at 506.

long attached to it."[88] The "officers inserted the spike under a baseboard . . . and into a crevice extending several inches into the party wall, until the spike . . . made contact with a heating duct serving the house occupied by the petitioners, thus converting their entire heating system into a conductor of sound" and enabling the officers to hear "[c]onversations taking place on both floors of the house."[89] The petitioners invited a reconsideration of *Olmstead* and its progeny in light of "recent and projected developments in the science of electronics" that would dramatically enhance the ability to eavesdrop from a distance.[90] The Court, however, found no need to "contemplate the Fourth Amendment implications of . . . frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society" because the conduct in *Silverman* involved "an unauthorized physical penetration into the premises occupied by the petitioners" and, thus, satisfied the demands of the *Olmstead* doctrine.[91] *Silverman* was critically different from *Olmstead* because it involved "the reality of an actual intrusion into a constitutionally protected area."[92]

The *Silverman* opinion was significant for the threshold of the Fourth Amendment and its relationship to official uses of technological tools in a number of respects.[93] *Olmstead* could have been understood to require *both* a physical intrusion *and* the physical acquisition of tangible objects. *Silverman* established that the Fourth Amendment is concerned with the electronic and aural acquisition of intangible items–in this case, words–by means of physical intrusion.[94] In addition, the Court explicitly eschewed the requirement of a "technical trespass under local property law"[95] and held that the magnitude of the physical breach was irrelevant.[96] "Declin[ing] to go beyond" its earlier decisions "by even a fraction of an inch," the Court, in essence, held that any "actual intrusion into a

[88] *Id.*
[89] *Id.* at 506-07.
[90] *Id.* at 508.
[91] *Id.* at 509.
[92] *Id.* at 512.
[93] The *Silverman* opinion's significance should not be overstated. Because the holding in the case hinged on the presence of a physical intrusion, it did not open the door to dramatic expansion of the Fourth Amendment regulation of technological tools.
[94] *Silverman*, 365 U.S. at 512. Although not mentioned by the Court, this conclusion was a clear contradiction of one of *Olmstead's* premises.
[95] *Id.* at 511.
[96] *Id.*

constitutionally protected area" would be sufficient to trigger Fourth Amendment scrutiny.[97] The Court preserved the *Olmstead* doctrine, but interpreted it as narrowly as possible and at least hinted that in a future case the "implications" of "frightening paraphernalia . . . of an electronic age" might imperil the survival of *Olmstead's* stingy threshold approach.

3. The *Katz* Era: An Interest-Oriented Approach

In *Goldman*, *On Lee*, and *Silverman*, the Court was asked to reconsider the restrictive threshold doctrine announced in *Olmstead*. In *Goldman*, it found no reason to question the doctrine and relied on it to reject the defendant's claim. In *On Lee*, the Court evinced no hostility to *Olmstead* while finding no need to address its continuing legitimacy. In *Silverman*, the Court evinced some doubt about the prevailing conception of the Fourth Amendment's reach, but found it unnecessary to reconsider the doctrine. *Silverman* left the *Olmstead* doctrine alive, but far from well.

Just six years later, in another case that illustrated the advantages for law enforcement and the perils for citizens of technology designed to intercept conversations, a litigant once again urged the Court to abandon the controlling threshold doctrine. In *Katz v. United States*,[98] the Court had no easy way to avoid a confrontation with *Olmstead*. The defendant's claim had to be rejected if the actual intrusion criterion was applied. Moreover, if *Olmstead* was overturned, there was no apparent reason why the defendant would not be entitled to Fourth Amendment shelter. All but one of the Justices decided that it was time to pull the plug on *Olmstead's* life support.[99]

In *Katz*, federal agents "attached an electronic listening and recording device to the outside of [a] public telephone" and intercepted "the petitioner's end of telephone

[97] *Id.* at 512. Not long thereafter, the Court proved how serious it was in refusing to expand the *Olmstead* limitation by even the smallest increment. In *Clinton v. Virginia*, 377 U.S. 158 (1964), a case involving electronic eavesdropping accomplished by means of a *de minimis* physical intrusion–an intrusion that was apparently thumbtack-sized, *see* Clinton v. Virginia, 130 S.E.2d 437, 442 (Va. 1963)–the Court found that a search had occurred. *See Clinton*, 377 U.S. at 158.

[98] 389 U.S. 347 (1967).

[99] *See Katz*, 389 U.S. at 364 (Black, J., dissenting).

conversations."[100] The words intercepted provided evidence that helped the government convict him of violating a federal statute that criminalized use of a wire communication facility to transmit wagering information in interstate commerce.[101] In accord with the *Olmstead* approach, the Court of Appeals rejected the petitioner's Fourth Amendment claim because "`there was no physical entrance into the area [he] occupied.'"[102]

Before the Supreme Court, the government argued that the "surveillance technique . . . employed involved no physical penetration of the telephone booth."[103] The Court responded as if the *Olmstead* approach had already expired and was simply awaiting a proper burial. Acknowledging that "the absence of such penetration was *at one time* thought to foreclose further Fourth Amendment inquiry," the Court asserted that it had "since departed from the narrow view on which [*Olmstead*] rested."[104] That departure made it "clear that the reach of that Amendment *cannot turn upon the presence or absence of a physical intrusion into any given enclosure*."[105] The erosion of *Olmstead*'s "underpinnings" meant that its "`trespass'" doctrine could "no longer be regarded as controlling."[106] In its place, the Court offered a potentially expansive, painfully ambiguous, threshold doctrine. The electronic eavesdropping in *Katz* was a "search" because it had "violated the privacy upon which [Katz had] justifiably relied" even though it "did not happen to penetrate the wall of the booth."[107]

The *Katz* majority decided that the reign of the physical intrusion standard had to end because it could not adequately safeguard the important interests that had motivated the Framers of the Fourth Amendment. In the Court's view, privacy was a primary concern of those who abhorred unreasonable searches and seizures and a primary reason for providing a constitutional assurance against them.[108] In the modern world, scientific and technological advances had furnished means of breaching privacy without

---

[100] *Id.* at 348.
[101] *Id.*
[102] *Id.* at 348-49.
[103] *Id.* at 352.
[104] *Id.* at 352-53 (emphasis added).
[105] *Id.* at 353 (emphasis added).
[106] *Id.*
[107] *Id.*
[108] *Id.* at 350. The Court asserted that privacy was not the only Fourth Amendment value, observing that public seizures of persons and of property, for example, intrude upon interests other than privacy. *Id.*

physical intrusion. Threshold doctrine had to recognize and take account of that reality if it was to be capable of preserving the substance of the constitutional guarantee. The preferable approach was interest-oriented, an approach that focused on the core Fourth Amendment interest in privacy and evaluated whether governmental conduct jeopardized that interest. Under this approach, official actions that had impacts on privacy similar to those effected by the physical intrusions known to our ancestors had to be deemed searches.[109]

The *Katz* opinion contained two significant limitations. First, the Court noted that the reach of the Fourth Amendment did not extend to every governmental infringement upon privacy.[110] That guarantee "protects individual privacy against [only] *certain kinds* of governmental intrusion."[111] The meaning of this limitation seems relatively clear. The Court was merely acknowledging that privacy is a term used to describe a variety of concepts, and that not all of them are Fourth Amendment concerns.[112] Second, the Court indicated that only violations of "*justifiably* relied" upon privacy could qualify as searches.[113] The meaning of this limitation is more opaque and difficult to capture. Apparently, the intent was to suggest that even when the appropriate *kind* of privacy interest is implicated, particular circumstances might render it indefensible to claim an official deprivation of that interest.

There is ample reason to applaud the constitutional perspective adopted by the *Katz* majority and the reformation in threshold doctrine that resulted.[114] There is

---

[109] The recognition that privacy was a vital concern of the constitutional protection against unreasonable searches was hardly novel. Over eighty years earlier, in *Boyd*, the Court had expressed the view that protection of "the privacies of life" was central to the Fourth Amendment. *Boyd*, 116 U.S. at 630. *Katz* was revolutionarily different from *Boyd*, however, in prescribing a threshold analysis in which the critical decision hinged on whether privacy was violated.

[110] *Katz*, 389 U.S. at 350.

[111] *Id*. (emphasis added).

[112] The Court observed that other privacy interests could find protection from other legal sources. *See id*. at 350-51 & n.5 (noting that "[o]ther provisions of the Constitution," the First, Third, and Fifth Amendments, for example, "protect personal privacy from other forms of governmental invasion," and asserting that "the protection of a person's *general* right of privacy . . . is . . . left largely to the law of the individual States").

[113] *Id*. at 353 (emphasis added).

[114] I agree with Justice Marshall that interpretation of a constitutional

also reason to bemoan the serious deficiencies in the guidance provided by the *Katz* opinion. Because the reach of the Fourth Amendment was to depend on whether the government intruded on certain kinds of justifiable privacy interests, it is vital to have an accurate idea of the character of the privacy that is constitutionally safeguarded and of the bases for deeming assertions of privacy justifiable or unjustifiable. The Court provided little, if any, insight concerning these critical issues. It raised the questions, but left their resolution to the future. A new threshold era had begun, but the shape it would take was yet to be determined.

B. The Evolution and Development of Katz's *Interest-Oriented Threshold Doctrine*

The Court has never directly revisited the question of the "kinds of intrusion on privacy" that are the object of Fourth Amendment concern. Considering the theoretical and practical significance of that issue–and the helpful guidance an answer would provide–the failure to pinpoint the nature of the privacy interests that define the scope of constitutional regulation is somewhat disconcerting. The good news is that the Court has implicitly identified the types of intrusions on privacy that matter. The holdings, reasoning, doctrinal criteria, and language of a number of post-*Katz* threshold opinions–many of which have involved claims that exploitations of technology amounted to searches–establish that constitutional protection against unreasonable searches is primarily designed to protect the people's ability to keep information about their lives confidential.[115] The core value is, in essence, an interest in *secrecy*—in not having the details of our lives learned or exposed against our wishes.[116] The Framers prized this

safeguard should not be restricted by the literal meaning of its words when preservation of the values and purposes furthered by the provision call for a more expansive construction. *See* United States v. Oliver, 466 U.S. 170, 186-87 (1984) (Marshall, J., dissenting) (arguing that constitutional safeguards should be interpreted to effectuate their purposes).

[115] There may be other "privacy" interests—for example, the interest in quiet repose in one's home, *see* Tomkovicz, *supra* note 19, at 666 n.87, and the interest in maintaining control over one's own body, *see* Winston v. Lee, 470 U.S. 753, 766 (1985); Schmerber v. California, 384 U.S. 757, 771-72 (1966)—that are also concerns of the Fourth Amendment. It is clear, however, that confidentiality is the dominant privacy interest that underlies the guarantee's protection against searches.

[116] *See* United States v. Jacobsen, 466 U.S. 109, 119-20 (1984) (concluding that agent's reopening of package already opened by private party was not a search because there "was a virtual certainty" that the agent's conduct "would not tell him anything more than he already had been told" and "enabled the agent to

aspect of "the right to be let alone"[117] as an essential foundation of a free society, and gave it a central place among the basic liberties enshrined in the Bill of Rights. When a government activity deprives a person of this interest in "informational privacy" or confidentiality, that activity is deemed a search.[118]

This interpretation of Fourth Amendment values seems consistent with the historical impetus for that guarantee. The invasions known to the Framers violated privacy by breaching confidentiality and uncovering secrets hidden within homes and other enclosed spaces. Those physical intrusions gained access to concealed information about the colonists' lives by piercing barriers that safeguarded that information. When the authorities learned what the people possessed, did, and even thought within their homes, privacy in this most basic sense was lost. Logically, it seems sensible to conclude that searches were objectionable primarily because they breached secrecy. The sphere of confidentiality preserved by restricting those searches furnished a critical foundation for the ability to live full and genuinely free lives.[119]

---

learn nothing that had not previously been learned"); United States v. Karo, 468 U.S. 705, 715 (1984) (holding beeper monitoring to be a Fourth Amendment search because it revealed "a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant"); *id.* at 727 (O'Connor, J., concurring in part and concurring in the judgment) (contending that a homeowner who allows another's belonging into his home does not suffer a privacy loss when a beeper locates the belonging because "[i]t is simply not *his* secret that the beeper is disclosing"); Smith v. Maryland, 442 U.S. 735, 743 (1979) (suggesting that telephone subscribers do not have "any general expectation that the numbers they dial will remain *secret*") (emphasis added).

[117] *Olmstead*, 277 U.S. 438, 478 (Brandeis, J., dissenting).

[118] For a more complete discussion of the character of this "privacy" interest, see Tomkovicz, *supra* note 19 at 663-67, 669-70; *see also* JEFFREY ROSEN, THE UNWANTED GAZE 15 (2000) (describing "a more focused vision of privacy that has to do with our ability to control the conditions under which we make different aspects of ourselves accessible to others"); Froomkin, *supra* note 16, at 1463 (using the phrase "`informational privacy' as a shorthand for the ability to control the acquisition or release of information about oneself.").

[119] For a more complete discussion of how an entitlement to keep information secret enables other liberties to flourish, see Tomkovicz, *supra* note 19, at 667-77; *see also* Rosen, *supra* note 118, at 12 (suggesting that "[f]reedom is impossible in a society that refused to respect" privacy); *id.* at 215-17 (maintaining that "there are personal costs to the erosion of privacy" because privacy "is important . . . to allow individuals to form intimate relationships," privacy "is necessary . . . to protect important social relationships," and privacy plays a significant role in "the development of human individuality" by providing a "refuge . . . from the overwhelming pressures toward social conformity").

The other critical question raised by *Katz*–when does an individual have a *justifiable* claim that a privacy interest protected by the Fourth Amendment has been violated–has received a considerable amount of direct attention from the Supreme Court in the thirty-five years since *Katz.* Once again, much of that attention has been directed toward disputes over whether a particular technological enhancement of human capacities is subject to Fourth Amendment control. While the doctrinal scheme that has emerged from this attention may not be coherent, complete, or wholly consistent, it is intriguing, extensive, and reflective of the view that deprivations of secrecy are the core constitutional concern. A cursory summary of that doctrine follows. More attention will be devoted to the most germane details in the discussion of the Court's threshold technology decisions.

In a concurring opinion in *Katz*, Justice Harlan maintained that the Fourth Amendment protects "reasonable expectation[s] of privacy"[120] and that there were two prerequisites for a reasonable expectation. First, a person must "have exhibited an actual (subjective) expectation of privacy."[121] Second, "the expectation [must] be one that society is prepared to recognize as `reasonable.'"[122] Just one year after *Katz*, a majority of the Court adopted Harlan's description of the Fourth Amendment's object of protection as "reasonable `expectation[s] of privacy.'"[123] Eleven years after that, the Court warmly embraced Harlan's two-pronged inquiry for ascertaining whether a search has occurred.[124] That basic doctrine, as refined by additional criteria for determining whether society is prepared to recognize a particular expectation as reasonable, remains the Court's "lodestar"[125] for making Fourth Amendment threshold determinations.[126]

The first inquiry demanded by the Harlan approach is

---

[120] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[121] *Id.* at 361.

[122] *Id.*

[123] Terry v. Ohio, 392 U.S. 1, 9 (1968) (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

[124] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[125] *Smith*, 442 U.S. at 739.

[126] The decision to give the reasonable expectation of privacy doctrine control over the threshold of the Fourth Amendment has not gone unchallenged. *See* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (contending that the "self-indulgent" reasonable expectation of privacy standard, when "employed . . . to determine whether a `search or seizure . . . ' has *occurred* (as opposed to whether that `search or seizure' is an `unreasonable' one), . . . has no plausible foundation in the text of the Fourth Amendment").

whether a person has manifested an "actual (subjective) expectation of privacy."[127] The Supreme Court has paid little attention to the demand, and at times has ignored it entirely.[128] Moreover, the Court has spoken somewhat inconsistently and ambiguously about the nature of this demand. There are indications that the relevant question is whether the *particular individual* in a case actually expected privacy.[129] On the other hand, one can find support for the view that the proper inquiry is whether "people in general" in the same situation expect privacy.[130] Moreover, it is not clear whether the first prong focuses on expectations of privacy in general, from everyone, or on expectations of privacy from governmental officials.[131]

There is no good theoretical or practical reason for retaining the actual expectation prerequisite. That inquiry has never been determinative in a Supreme Court threshold decision. That may be because any factor that leads to the conclusion that an individual has not manifested a subjective privacy expectation also supports the conclusion that society is unprepared to deem an expectation reasonable. The inquiry is superfluous or duplicative, at best. At worst, it has the potential to mislead lower courts into denying legitimate

[127] The author of the actual expectation of privacy requirement later cast doubt on the validity of that demand, suggesting in a post-*Katz* opinion that the threshold inquiry "must . . . transcend the search for subjective expectations or legal attribution of assumptions of risk." United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[128] *See infra* note 130.

[129] *See* California v. Ciraolo, 476 U.S. 207, 211-12 (1986) (indicating that the question was whether "respondent . . . manifested a subjective expectation of privacy from *all* observations of his backyard"); Rawlings v. Kentucky, 448 U.S. 98, 104-06 (1980) (concluding that "petitioner had no legitimate expectation of privacy" in an acquaintance's purse in part because he admitted "that he did not believe that [the] purse would remain free from governmental intrusion"); *Smith*, 442 U.S. at 743, 745 (stating that "even if petitioner did harbor some subjective expectation" of privacy, it was not reasonable and concluding "that petitioner in all probability entertained no actual expectation of privacy").

[130] *See Smith*, 442 U.S. at 742, 743 (suggesting that the question is whether "people in general entertain any actual expectation of privacy in the numbers they dial" and referring to the actual "expectations of telephone users in general").

[131] The analysis in *Smith* focused on expectations of privacy from the phone company, not from the government. In the other cases that include any discussion of the actual expectations prong, there is no indication that whether one has an expectation of privacy vis-a-vis the authorities is relevant. The impression created is that the absence of an actual privacy expectation vis-a-vis any particular person could defeat a Fourth Amendment threshold claim.

Fourth Amendment claims.[132] Fourth Amendment threshold doctrine could only be improved by elimination of the "actual (subjective) expectation of privacy" demand.[133]

[132] *See, e.g.*, United States v. Robinson, 62 F.3d 1325, 1328 (11th Cir. 1995) (stating that to determine whether thermal imaging of a home was a search, the "focal issue [was] whether [the home dweller] had a subjective expectation of privacy in the *heat* generated by his indoor marijuana cultivation" and finding that he had "none"); United States v. Penny-Feeney, 773 F. Supp. 220, 226 (D. Haw. 1991) (holding that thermal imaging of residence was not a search in part because "defendants did not manifest an actual expectation of privacy in the heat waste [detected] since they voluntarily vented it outside"); LaFollette v. Commonwealth, 915 S.W.2d 747, 749 (Ky. 1996) (concluding that thermal imaging of residence was not a search in part because the "condition of appellant's residence offered no expectation of privacy as to heat emission").

[133] In form, the two questions described by Justice Harlan impose independent, conjunctive requirements. For a search to be found, both must be answered affirmatively. In substance, however, the first question–the "actual expectation" inquiry–has not played a meaningful role in threshold analysis. It has determined the outcome of none of the many threshold opinions of the Court since *Katz*. In the vast majority of those cases, the Court has acted in one of two ways. First, it has ignored the inquiry and passed immediately to the second question. *See, e.g.*, Hudson v. Palmer, 468 U.S. 517, 525-26 (1984); United States v. Knotts, 460 U.S. 276, 281-82 (1983). Second, the Court has paid no more than passing lipservice to the requirement, quickly conceding or assuming that an individual actually expected privacy. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338 (2000); California v. Greenwood, 486 U.S. 35, 39 (1988); *Ciraolo*, 476 U.S. at 211. The sole opinion with an extended analysis to the subjective privacy expectation of the claimant concludes that he had no such expectation, but then proceeds to reason that "even if" he did, it was not an expectation society was prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-43. The Court's opinions seem to implicitly acknowledge the uselessness of the actual expectations criterion.

In fact, there is a logical predicate for denying constitutional protection to people who do not actually expect privacy. If individuals conduct their lives in ways that show that they have no confidentiality interest in particular matters–when they choose to "publicize" information by words or deeds–it would be irrational to recognize a claim that the government "breached" their privacy by receiving that information. A person who truly fails to protect or who decides to reveal secrets can hardly charge those who see, hear, or otherwise learn of those secrets with a violation of privacy. Thus, "[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*, 389 U.S. at 351. Similarly, what a person proclaims from a street corner soapbox or leaves exposed on the back seat of her car can be heard or seen without violating any genuine interest in confidentiality.

Nonetheless, an appropriate Fourth Amendment result can be reached in such cases without the actual expectation inquiry. The second *Katz* criterion–whether society will recognize an expectation as reasonable–will deny protection based on the same conduct that demonstrates the absence of an actual expectation. In *Smith v. Maryland*, for example, in holding that the use of a "pen register" with telephone company cooperation to record numbers dialed from a home phone was not a search, the Court concluded that there was no actual expectation of privacy and that society was not prepared to recognize any expectation as reasonable for essentially the same reason–the claimant had knowingly and voluntarily chosen to convey the information acquired to the telephone company. *Smith*, 442 U.S. at 742-44.

The actual expectation prong is dangerous and potentially destructive of constitutional liberty insofar as it could enable the government or others to diminish the scope of Fourth Amendment protection. Announcements that

The second inquiry–whether society is prepared to recognize a privacy expectation as reasonable–has been determinative in the Court's decisions.[134] This inquiry has not been guided by actual assessments of society's attitudes, but instead by objective indicia of whether it is rational to validate an assertion that officials have deprived an individual of a cognizable interest in secrecy. The major, recurrent criteria are easily described.

Society is not prepared to recognize the reasonableness of an expectation of privacy if an individual has knowingly exposed the putatively private matter to the public[135] or has voluntarily conveyed the supposedly secret facts to a third party who has agreed to convey those facts to the authorities.[136] Society will not honor expectations of privacy if the government's conduct that is contested could not reveal any information at all,[137] could only reveal truly insignificant information,[138] or could only reveal information about the nature or presence of an illegitimate substance (*i.e.*, contraband).[139] Moreover, if there is no societal interest in protecting the privacy of the information that could be disclosed by the government's actions, society will not affirm

privacy invasions will occur or the actual occurrence of conduct that invades privacy interests could lead the people not to actually expect privacy. For that reason, the Court has observed that the "problems inherent in [a subjective expectation] standard are self-evident." *See Hudson*, 468 U.S. at 525 n.7. In addition, the Court has declared that in cases where subjective expectations are "`conditioned' by influences alien to well-recognized Fourth Amendment freedoms," the absence of subjective expectations would be irrelevant and, instead, "a normative inquiry would be proper." *Smith*, 442 U.S. at 741 n.5. There is yet another peril in the actual expectation inquiry, an ever-present risk that courts will misinterpret and misapply the criterion, declaring that no actual expectations exist in situations where it is both illogical and constitutionally indefensible to do so.

In apparent recognition of the unnecessary or redundant nature of the actual expectations inquiry, in subsequent cases that could have adhered to the logic of *Smith v. Maryland*, the Court has declined to conclude that a claimant's willingness to expose his actions to the public or convey information to a third party demonstrated an absence of actual privacy expectations. *See Greenwood*, 486 U.S. at 39-41; *Ciraolo*, 476 U.S. at 211-12, 213-14; *Knotts*, 460 U.S. at 281-83.

[134] The "Court has always emphasized the second of the[] two requirements." *Hudson*, 468 U.S. at 525 n.7.

[135] *See Greenwood*, 486 U.S. at 40-41; *Knotts*, 460 U.S. at 281-82.

[136] *See* United States v. Miller, 425 U.S. 435, 442-44 (1976); *White*, 401 U.S. at 749-50.

[137] *See* United States v. Karo, 468 U.S. 705, 712 (1984).

[138] *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984).

[139] *See* United States v. Place, 462 U.S. 696, 707 (1983); *Jacobsen*, 466 U.S. at 123.

the reasonableness of an individual's actual expectation of privacy.[140] Some, if not all, of these variables—if properly understood and applied—seem to be logically defensible indicia of whether constitutionally cognizable privacy interests are imperiled.

The development of the reasonable expectation of privacy threshold doctrine has occurred in a piecemeal, *ad hoc* fashion. No overarching scheme or analytical framework is evident in the Court's threshold decisions. The Court has never proffered a general vision of the nature of reasonable expectations of privacy or the character of the criteria that ought to dictate whether a search has occurred. Nonetheless, the rich array of threshold issues addressed over a thirty-five year span has produced a formidable and informative body of doctrine. Having established the legal context in which confrontations between technology and the Fourth Amendment arise, it is now time to turn to those confrontations.

III. THE THRESHOLD TECHNOLOGY DECISIONS: A DESCRIPTION, ANALYSIS, AND CRITIQUE OF THE SUPEME COURT'S UNDERSTANDING

The *Katz* revolution in threshold doctrine was precipitated by a head-on collision between technology and the Fourth Amendment and a recognition of the constitutional dangers posed by innovative enhancements of human sensory abilities.[141] This part of the article devotes

[140] There are three less significant criteria that have appeared in some threshold opinions. None has ever had decisive impact. On occasion, the Court has suggested that society is less prepared to recognize privacy interests if doing so will interfere with effective law enforcement. *See Hudson*, 468 U.S. at 526-27; Oliver v. United States, 466 U.S. 170, 182 n.13 (1984); *White*, 401 U.S. at 753; *see also* Tomkovicz, *supra* note 19, at 660. On the other hand, it has indicated that society is more inclined to honor privacy expectations if a claimant has property rights in the area involved. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979); *Miller*, 425 U.S. at 440-41; *see also* Tomkovicz, *supra* note 19, at 657-58. The Court has also suggested that society is more likely to honor privacy expectations if a physical invasion or intrusion of some sort has occurred. *See* Dow Chemical Co. v. United States, 476 U.S. 227, 237 (1986); *Ciraolo*, 476 U.S. at 213; *Karo*, 468 U.S. at 714; *Smith*, 442 U.S. at 741; *see also* Tomkovicz, *supra* note 19, at 658-59. The impediment to effective law enforcement criterion seems more appropriately factored in at the reasonableness stage of Fourth Amendment analysis–not in the threshold inquiry. The possession of a property interest or the occurrence of a physical intrusion might provide support for a violation of privacy claim. On the other hand, neither the absence of a property interest nor the lack of a physical intrusion should ever defeat a privacy claim in the post-*Katz* era.

[141] The recognition was implicit in the majority opinion, not the subject of explicit discussion. *See generally* Katz v. United States, 389 U.S. 347 (1967). Justice Harlan's well-known description of *Olmstead's* "physical intrusion"

attention to the Supreme Court's post-*Katz* threshold cases involving exploitations of the tools provided by science and technology. I classify ten cases within this category.[142] In eight of those decisions, the Court ruled that the Fourth Amendment did not regulate the government's conduct.[143] In the other two, both of which involved efforts to learn about activities inside private homes, the Court found Fourth Amendment searches.[144] After a brief chronological review of the relevant cases, I categorize the decisions, analyzing and evaluating the lessons each teaches regarding the relationship between the Fourth Amendment and technology.[145]

---

requirement as "bad physics as well as bad law" was also an acknowledgment of the perils created by scientific and technological advances in surveillance capabilities. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring).

[142] *See infra* notes 146-201 and accompanying text. I define technology broadly to include any device, tool, mechanism, or method that in some way augments or enhances ordinary human capacities. As will become clear later, I do not believe that the Fourth Amendment should be concerned with every sort of expansion of human potential afforded by science and technology. A mechanism should not trigger constitutional scrutiny unless it might alter human capacities in some way that threatens the interests sheltered by the Fourth Amendment. Consequently, devices that somehow increase ordinary human abilities to gain access to confidential or secret information–i.e., those that can threaten core Fourth Amendment privacy interests–are appropriate objects of Fourth Amendment attention. Devices that enable more efficient communication or speedier travel, for example, but have no potential impact on any interest that the Fourth Amendment was designed to protect, seem well beyond the scope of constitutional concern.

[143] *See infra* notes 146-67, 172-90 and accompanying text.

[144] *See infra* notes 168-201 and accompanying text. In what can best be characterized as a "curious" pattern without legal significance, all three holdings that technological exploitation is governed by the Fourth Amendment have involved individuals with short surnames beginning with the letter "K," and the decisions have occurred at precisely seventeen-year intervals.

[145] The fact that eighty percent of the decisions have found technological exploitation to be beyond the reach of the Fourth Amendment is noteworthy. That statistic alone does not establish bias or error by the Court. It is entirely possible that the sort of claim to reach the Court has typically involved creative efforts to stretch the borders of the Fourth Amendment. The pattern of decisions does make it clear, however, that any fear that the *Katz* approach to threshold doctrine would unjustifiably expand the boundaries of the Fourth Amendment was unfounded. *See Katz*, 389 U.S. at 373-74 (Black, J., dissenting) (expressing a fear that the Court had transformed the Fourth Amendment into a tool for restricting every governmental action with any impact on privacy, broadly-defined). The reasonable expectation of privacy doctrine has most certainly not produced widespread or suffocating constitutional control over official efforts to employ innovative surveillance tools. *Katz* is the *sole* decision in which a use of technology outside a home has been found to violate a reasonable expectation of privacy and thus to be a search. Moreover, not every potential threat to home privacy has prompted the Court to find Fourth Amendment coverage. *See, e.g.*, *Ciraolo*, 476 U.S. at 215 (aerial surveillance of

*A. A Chronological Summary of the Post-*Katz *Threshold Technology Decisions*

1. *United States v. White*: Electronic, Participant-Aided Monitoring of Conversations

The first threshold technology case reached the Court in 1971, just four years after *Katz*. In *United States v. White*,[146] government agents listened in on conversations by means of a radio transmitter that was concealed on the person of a willing, cooperative informant.[147] By means of this electronic eavesdropping, they heard White's incriminating statements regarding narcotics offenses.[148] The Supreme Court ruled that the agents did not conduct a search when they electronically eavesdropped on the conversations.[149]

2. *Smith v. Maryland*: Pen Register Perception and Recordation of Numbers Dialed from a Home Telephone

Eight years passed before another clash between technology and the Fourth Amendment brought a threshold issue to the Court. In *Smith v. Maryland*,[150] at the request of law enforcement agents, the telephone company installed a "pen register"[151] at its central office in order to record the numbers dialed from the defendant's residential telephone.[152] The device revealed a call placed to the

residential curtilage held not to be a search); *Smith*, 442 U.S. at 745 (holding that pen register monitoring of numbers dialed from phone of a private residence was not a search). Although the *Katz* opinion did subject a previously unregulated use of technology to Fourth Amendment control and at least suggested that officials would be considerably less free to exploit the products of scientific progress, the doctrine that has grown out of that decision has afforded generous breathing space for unfettered use of novel crime-detecting technologies. For the view that it has afforded too much breathing space for technological and other threats to privacy, see Rosen, *supra* note 118, at 34 (arguing that the Court has "pretend[ed] that all sorts of dramatic intrusions on privacy . . . [aren't] really searches . . . in the first place" and that "[t]he result" has been "a legal climate that constricted the constitutional protections for privacy at the very moment that techniques of surveillance were growing more invasive").

[146] 401 U.S. 745 (1971).

[147] *White*, 401 U.S. at 747.

[148] *Id.* at 746-47.

[149] *Id.* at 754.

[150] 442 U.S. 735 (1979).

[151] *Smith*, 442 U.S. at 737. "`A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.'" *Id.* at 736 n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)).

[152] *Id.* at 737.

telephone number of a robbery victim.[153] That call and other evidence acquired as a product of the pen register surveillance were used to convict the defendant of robbery.[154] The Supreme Court rejected the claim that the use of the pen register to detect the dialed numbers violated a reasonable expectation of privacy, holding that it did not constitute a search.[155]

3. *United States v. Knotts*: Beeper-Assisted Tracking of Public Movements

Four years later, another conflict between the Fourth Amendment and technology caught the Court's eye. *United States v. Knotts*[156] introduced the Court to a novel technological investigatory tool—a tracking "beeper."[157] Officers who suspected Knotts and others of involvement in narcotics manufacturing secured the consent of a chemical company to install a beeper in a container that the company subsequently sold to one of Knotts' cohorts.[158] By both visual surveillance and electronic monitoring of the beeper, officers tracked the car in which the chloroform container had been placed.[159] They lost both visual contact and the beeper signal at one point, but were subsequently able to locate the signal, which indicated that the container had come to rest in the area of a cabin occupied by Knotts.[160] Based on the information obtained from the surveillance and additional facts, officers obtained a warrant, searched the cabin, and discovered a drug manufacturing operation and contraband narcotics.[161] The Supreme Court unanimously held that the use of the beeper to follow and locate the can did not violate a reasonable expectation of privacy and, therefore, was not a search.[162]

---

[153] *Id.*
[154] *Id.* at 737-38.
[155] *Id.* at 745-46.
[156] 460 U.S. 276 (1983).
[157] "A beeper is a radio transmitter . . . which emits periodic signals that can be picked up by a radio receiver." *Knotts*, 460 U.S. at 277.
[158] *Knotts*, 460 U.S. at 278.
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *Id.* at 285.

4. *United States v. Place*: A Sniff of Luggage by a Drug-Detecting Canine

The same year, the Court addressed yet another threshold technology issue.[163] In *United States v. Place*,[164] the authorities used a narcotics-detecting canine to sniff luggage belonging to a man who had flown from Florida to New York.[165] After the dog reacted positively to one of two bags, the officers applied for and secured a search warrant and found a substantial amount of cocaine inside.[166] The Court opined that the use of the trained dog's heightened olfactory abilities to determine whether contraband was inside the luggage did not cross the Fourth Amendment threshold and trigger constitutional scrutiny.[167]

---

[163] While one might question whether drug-sniffing canines are a technological development, I include them in this section because they constitute a novel "scientific" development that enhances normal human capacities to perceive concealed, otherwise confidential information. Moreover, the Court's treatment of this technique has significant implications for technological devices with similar abilities to augment human faculties and reveal concealed, arguably private information. *See, e.g.*, Bob Mitchell, *Electronic `Drug Dogs*,' TORONTO STAR, Apr. 16, 2001, at 1 (discussing the mechanics of an "electronic sniffer" that can detect drug residues on swabbed objects); Tom Godfrey, *Customs Looks At Scanner; Hi-Tech Device in U.S. Detects Trace Bits of Drugs, Explosives*, TORONTO SUN, May 31, 2000, at 3 (discussing "American field tests on a hi-tech scanner that detects traces of drugs and explosives on passengers"); Paul W. Valentine, *Md. Receives Federal Drug-Fighting Grant*, WASH. POST, Jan 6, 1999, at A12 (discussing the use of "state-of-the-art ion-scan machines to detect traces of drugs on the clothing of people entering" prisons).

[164] 462 U.S. 696 (1983).

[165] *Place*, 462 U.S. at 696.

[166] *Id*. The Court held that the government had violated the defendant's Fourth Amendment rights because it had seized his luggage for an unreasonably prolonged period based on a reasonable suspicion that it contained contraband. *See id*. at 709-10. That holding is not pertinent here.

[167] More recently, in *City of Indianapolis v. Edmond*, the Court affirmed the threshold conclusion reached in *Place*, extending it to dog sniffs of vehicles on public roads. City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000). Even though the Court's conclusions in both *Place* and *Edmond* can be characterized as dicta, they leave no room for doubt regarding the Court's attitude toward dog sniffs of publicly-situated luggage and vehicles. While *Edmond* is yet another threshold technology decision by the Court, I do not discuss it separately because it adds nothing to the analysis set forth to justify the conclusion in *Place*.

5. *United States v. Karo*: Beeper Monitoring of In-Home Activities

In 1984, the Court again explored the relationship between tracking beepers and the Fourth Amendment. In

United States v. Karo,[168] government agents installed a beeper in a can of ether, substituted it for one ordered by the respondents, and monitored the signal from the beeper.[169] They located the can of ether in various locations, including private dwellings.[170] On two occasions they were able to ascertain that the can had not left, but had remained inside a particular residence.[171] The question presented[172] was "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance," infringed on the Fourth Amendment interests "of those who have a justifiable interest in the privacy of the residence."[173] For the first time since its decision in *Katz*, the Court held that official exploitation of a technological tool violated privacy and constituted a Fourth Amendment search.[174]

6. *United States v. Jacobsen*: Chemical Field Tests to Detect Contraband

The very same year, the Court resolved another threshold technology issue. In *United States v. Jacobsen*,[175] a federal agent subjected a trace of the powder found in a package to a chemical test that involved placing the powder in three test tubes of liquid.[176] The liquids in the test tubes took on a sequence of colors that indicated that the powder was cocaine.[177] The Supreme Court concluded that the chemical field test used to identify the substance was not a search because it did not violate a reasonable expectation of privacy.[178]

---

[168] 468 U.S. 705 (1984).

[169] *Karo*, 468 U.S. at 708.

[170] *Id.* at 708-10.

[171] *Id.* at 709-10.

[172] The *Karo* Court also discussed whether the "transfer" of a beeper-infected object to an individual constitutes a search or a seizure, holding that it constituted neither sort of Fourth Amendment activity. *Id.* at 711-13.

[173] *Id.* at 714.

[174] *Id.* at 721.

[175] 466 U.S. 109 (1984).

[176] *Jacobsen*, 466 U.S. at 111, 112 n.1. The Court also addressed the issue of whether the federal agent's "reopening" of the package that had already been opened by Federal Express employees constituted a search. *Id.* at 119. That threshold question is not discussed here because it did not involve use of a technological tool.

[177] *Id.* at 112 n.1.

[178] *Id.* at 126.

7. *California v. Ciraolo*: Naked Eye Aerial Surveillance Of Residential Curtilage

Two years later, the Court confronted the Fourth Amendment implications of using aircraft to fly over and see into backyards. In *California v. Ciraolo*,[179] the police received a tip that the respondent was growing marijuana in his backyard.[180] Because the two fences erected around the yard prevented ground-level observation, officers took to the air, and from an altitude of 1000 feet were able to "readily identif[y] marijuana plants."[181] Based on the tip and these observations, they obtained a search warrant, executed it, and seized seventy-three marijuana plants.[182] A five-Justice majority of the Court was persuaded that the aerial surveillance of the yard did not qualify as a Fourth Amendment search under the *Katz* test.[183]

8. *Dow Chemical Co. v. United States*: Photographic Aerial Surveillance Of Commercial Premises

In a companion case to *Ciraolo*, the Court further addressed the constitutional ramifications of aerial surveillance. *Dow Chemical Co. v. United States*[184] involved aerial surveillance of a chemical manufacturing complex by the Environmental Protection Agency.[185] From various altitudes within navigable airspace, a "commercial aerial photographer, using a standard floor-mounted, precision aerial mapping camera" took photographs of Dow's manufacturing premises.[186] The photographs yielded information not visible to unaided eyes.[187] When Dow became aware of this activity, the company sought and obtained an injunction against the EPA that barred further aerial photography.[188] The same five Justices that formed the

[179] 476 U.S. 207 (1986).
[180] *Ciraolo*, 476 U.S. at 209.
[181] *Id.* at 209.
[182] *Id.*
[183] *Id.* at 215.
[184] 476 U.S. 227 (1986).
[185] *Dow Chem. Co.*, 476 U.S. at 229.
[186] *Id.* at 229.
[187] *Id.* at 230.
[188] *Id.*

Ciraolo majority concluded, however, that neither the use of the aircraft nor the use of the camera brought the surveillance within the sphere of Fourth Amendment regulation.[189]

9. *Florida v. Riley*: Naked Eye Surveillance of Residential Property By Helicopter

Three years passed before the Court issued its third pronouncement on the interface between aerial surveillance and the Fourth Amendment. *Florida v. Riley*[190] involved naked-eye observations through openings in the roof and sides of a greenhouse situated on residential property.[191] An officer made the observations while circling over the property in a helicopter at an altitude of four hundred feet.[192] He saw what he believed was marijuana, obtained a search warrant based on his observations, and found marijuana growing in the greenhouse.[193] A majority of the Court again concluded that the officer had not ventured across the border defining Fourth Amendment territory.[194] His conduct was not a search.[195]

10. *Kyllo v. United States*: Thermal Imaging of a Home

The 1990s produced no Supreme Court threshold technology decisions. Early in the new millennium, however, the Court decided to resolve an issue that had been percolating in the lower courts for years. In *Kyllo v. United States*,[196] law enforcement officers who suspected that the petitioner was growing marijuana in his home decided to scan the dwelling with a "thermal imager"—a technological tool that could detect the relative amounts of infrared radiation emanating from the dwelling.[197] The thermal scan showed that some areas of the home "were relatively hot compared to the rest of the home and substantially warmer than neighboring homes."[198] An officer's inference that the

---

189 *Id*. at 239.
190 488 U.S. 445 (1989).
191 *Riley*, 488 U.S. at 448.
192 *Id*.
193 *Id*. at 448-49.
194 *Id*. at 450.
195 *Id*.
196 533 U.S. 27 (2001).
197 *Kyllo*, 533 U.S. at 29-30.
198 *Id*. at 30.

heat differentials resulted from the use of lights to grow marijuana indoors and other facts furnished the basis for a search warrant for the dwelling.[199] Inside, officers discovered a cultivation enterprise with over 100 marijuana plants.[200] For only the second time in the reasonable expectation of privacy threshold era, a majority concluded that an exploitation of technology did qualify as a search and, therefore, needed to satisfy the reasonableness requirement of the Fourth Amendment.[201]

B. Categorizing and Understanding the Influential Variables–An Assessment of the Constitutional Logic Underlying the Court's Threshold Technology Decisions

As mentioned earlier, the *Kyllo* case is the reason for my involvement in this project. The Court's decision in *Kyllo* is also the inspiration for this symposium devoted to the relationship between technology and the Fourth Amendment. *Kyllo* is a remarkable decision because the Court reached a conclusion out of step with the predominant view of the lower courts.[202] It is also remarkable because of the unpredictable configuration of five Justices who constituted the majority.[203] The most remarkable, even

---

[199] *Id.*

[200] *Id.*

[201] *Id.* For scholarly discussions and analyses of *Kyllo*, see Gregory S. Fisher, *Cracking Down on Soccer Moms and Other Urban Legends on the Frontier of the Fourth Amendment: Is It Finally Time to Redefine Searches and Seizures?*, 38 WILLAMETTE L. REV. 137 (2002); Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013 (2001).

[202] *See, e.g.*, United States v. Robinson, 62 F.3d 1325, 1330 (11th Cir. 1995), *cert. denied*, 517 U.S. 1220 (1996) (determining that thermal imaging was not a search because it did not reveal intimate details within the home and because there was no intrusion into the home); United States v. Ishmael, 48 F.3d 850, 857 (5th Cir.), *cert. denied*, 516 U.S. 818 (1995) (holding that the use of thermal imager was not activity governed by Fourth Amendment because it was "passive and non-intrusive" and did not disturb the sanctity of home); United States v. Myers, 46 F.3d 668, 670 (7th Cir.), *cert. denied*, 516 U.S. 879 (1995) (thermal imaging was not a search because the home dweller failed "to conceal or contain the heat emissions" and the defendant's expectation of privacy was not reasonable); United States v. Ford, 34 F.3d 992, 997 (11th Cir. 1994) (finding that imager use was not search because it disclosed only "waste heat" that was exposed to public and did not reveal "specific activities" in home); United States v. Pinson, 24 F.3d 1056, 1058-59 (8th Cir.), *cert. denied*, 513 U.S. 1057 (1994) (determining that thermal imager use was not Fourth Amendment activity because "no intimate details of the home were observed and there was no intrusion upon the privacy of the individuals within").

[203] Justice Scalia authored the majority opinion which was joined by Justices

astounding, aspect of *Kyllo*, however, is that it is the *first* majority opinion by the Supreme Court to directly address the general subject of the relationship between technological enhancements of human capacities and the scope of Fourth Amendment protection.[204] *Kyllo* is by no means a comprehensive discourse upon the subject of when novel developments ought to trigger constitutional scrutiny. It does not fill the longstanding analytical and doctrinal voids. Nonetheless, the opinion takes a long overdue and significant first step by both explicitly and implicitly acknowledging the importance of understanding the tension that exists and arriving at sensible Fourth Amendment resolutions of the issues raised by technological enhancements of human capacities.[205]

Souter, Thomas, Ginsburg, and Breyer. *Kyllo*, 533 U.S. at 29. Justice Stevens wrote a somewhat surprising dissent, joined by Chief Justice Rehnquist and Justices O'Connor and Kennedy, in which he deemed the privacy interests at stake to be "implausible" and "trivial." *See Kyllo*, 533 U.S. at 44-45, 51 (Stevens, J., dissenting).

[204] Dissenting Supreme Court Justices have explored the general subject in cases decided both before and after *Katz*. *See, e.g.*, *Dow Chem. Co.*, 476 U.S. at 240, 247 (Powell, J., dissenting) (asserting that the *Dow* decision marked a retreat from the standard adopted to ensure "that Fourth Amendment rights would retain their vitality as technology expanded the Government's capacity to commit unsuspected intrusions into private areas and activities" and "designed to ensure that the Fourth Amendment continues to protect privacy in an era when official surveillance can be accomplished without . . . physical penetration . . . or proximity"); *Ciraolo*, 476 U.S. at 218-19 (Powell, J., dissenting) (noting that *Katz* had recognized that a physical intrusion threshold standard "provides no real protection against surveillance techniques made possible through technology" because "[t]echnological advances have enabled police to see people's activities and associations, and to hear their conversations without being in physical proximity" and "to conduct intrusive surveillance without any physical penetration"); *Goldman*, 316 U.S. at 138-39 (Murphy, J., dissenting) (observing that "the conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials" and that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment"); *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) (predicting that the "progress of science in furnishing the government with means of espionage is not likely to stop," warning that the future may well bring scientific means of reproducing private papers without removing them "from secret drawers," of exposing "the most intimate occurrences of the home," and of venturing into the human mind, "exploring unexpressed beliefs, thoughts and emotions," and suggesting that the Constitution must be construed to provide "protection against such invasions of individual security").

[205] The majority observed that the question confronted was "what limits there are upon the power of technology to shrink the realm of guaranteed privacy," expressed concern over the erosion of home privacy that can result from "police technology," and announced a doctrine designed to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. Justice Scalia warned that adherence to the *Katz* Court's rejection of "a mechanical interpretation of the Fourth Amendment" was vital because a contrary approach "would leave the homeowner at the

Until I became immersed in this project, I had the very distinct impression that the Supreme Court's threshold technology cases were a collection of *ad hoc* opinions that reflected no general conception of the relationship between technology and the Fourth Amendment's reach. The need and the opportunity to examine those cases more closely have altered my impression. I now perceive a number of basic, foundational premises underlying the Court's analyses. Some of those premises are eminently logical, while others are questionable. The most serious flaws in the Court's reasoning have been the failures to explore the implications of those premises in sufficient depth. The object of this part of the discussion is to explore those premises, to identify their logical underpinnings, and to pursue in detail the issues they raise. I have devised four categories to assist my explorations of the Court's threshold technology reasoning: revelatory behavior, informational content, the nature and character of the technology, and the location of the privacy interest.

1. The "Revelatory Behavior" Premises

Each of the factors and holdings classified within the "revelatory behavior" category rest essentially on the notion that a person suffers no violation or deprivation of confidentiality or secrecy if information about her life has been perceived or acquired because of the person's choice to reveal or expose that information. Exposure, disclosure, and publicity are the antitheses of privacy, confidentiality, and secrecy. For that reason, no Fourth Amendment interest in informational privacy is jeopardized when officials merely take advantage of a person's willingness to reveal or expose matters. According to this reasoning, if a person has engaged in the sort of revelatory conduct that forfeits any genuine interest in secrecy, it should not matter that technological means of acquisition have exploited that conduct.

The basic logic underlying the revelatory behavior category is persuasive. The government does not intrude on

mercy of advancing technology . . . that could discern all human activity in the home." *Id.* at 35-36. Ultimately, the majority sought to develop a general standard that would protect constitutionally guaranteed privacy not only against the particular sort of thermal imager used in *Kyllo*, but also against "more sophisticated systems that [we]re already in use or in development." *Id.* at 36.

core Fourth Amendment privacy values by perceiving what a person chooses to reveal or by receiving what an individual chooses to convey.[206] As will be seen, however, applications of this basic logic to concrete situations give rise to subtle and difficult issues that require careful analysis. Care must be taken to avoid according revelatory behavior premises more influence in threshold determinations than is logically defensible. The Court's opinions, which reflect three variations on the revelatory behavior theme, have typically neglected critical issues. Facile, somewhat superficial, analyses have produced questionable conclusions in threshold technology cases.

a. The First Variation: The Technological Acquisition of Information Exposed and Accessible to Unaided Senses

The first variation on the revelatory behavior theme is the premise that no privacy violation occurs when technology is employed merely to perceive and acquire facts that ordinary, unenhanced human senses could also perceive and secure from lawful public vantage points. In *United States v. Knotts*,[207] the Court found that the use of a tracking beeper to monitor movements along public thoroughfares and arrivals at particular destinations did not violate reasonable expectations of privacy because the individuals being tracked "voluntarily conveyed" the information learned by means of the beeper to "anyone" in a public place "who wanted to look."[208] The Court observed that ordinary "[v]isual surveillance from public places . . . would have sufficed to reveal" everything disclosed by the beeper-assisted tracking of public movements.[209] Exposure of the details learned by a beeper to the unaided senses of members of the public defeats the legitimacy of any expectation that those facts will remain confidential. Because public exposure is inconsistent with privacy, it is irrational to accuse the government of breaching secrecy. Instead, officials have merely reaped the harvest of the traveler's willingness to "publicize" facts about her life. In such circumstances, the contention that society ought to respect an expectation of privacy is implausible.

Knotts instructs that when a technological device capable

---

[206] In these situations, the government does not intrude on a credible interest in confidentiality. However, it is possible that there are other Fourth Amendment values that are jeopardized in revelatory behavior situations.

[207] 460 U.S. 276 (1983)

[208] *Knotts*, 460 U.S. at 281, 285.

[209] *Id.* at 282.

of augmenting human perceptual capacities is employed to perceive no more than what *could have been* perceived lawfully by means of unsupplemented human senses, it does not jeopardize Fourth Amendment privacy interests and should not be subjected to constitutional regulation.[210] If simple visual observations of exposed movements from public places are not invasions of privacy—and no one would suggest that they are—then technological substitutes for unaided observations that detect nothing more than visual observations could capture are not invasions of privacy.[211] In such cases, exploitation of the technological device does not deprive an individual of a cognizable interest in secrecy. Instead, like the visual observations that are capable of sensing and learning the same details, the technological surveillance does no more than capitalize on the person's willingness to expose her life to public view.[212]

---

[210] In *Knotts*, the beeper did in fact enable officers to accomplish what they had failed to accomplish with unaided senses. Evasive maneuvers by the individual being tracked had resulted in a "failure of the visual surveillance." *Id.* at 285. The radio transmitter made it possible to pick up a cold trail and to discern where the chemicals had come to rest. In the Court's view, what mattered was that an officer who had been able to follow the chemicals "at a distance throughout [the] journey *could have observed*" all of the information discerned by the monitoring beeper. *Id.* (emphasis added). Without explanation, the Court decided that the determinative question is not what the authorities "would [actually] . . . have been able to do . . . had they relied solely on their naked eyes" in a particular case. *Id.* Instead, the determination of whether a technological enhancement is governed by the Fourth Amendment turns on whether it would have been possible, in theory or in the abstract, to use naked senses to learn what the technological device enabled the authorities to learn. *Id.*

[211] The Court did not deny that beepers are capable of expanding human sensory capacities, enabling the perception of matters inaccessible to ordinary senses. Indeed, just one year later, in *United States v. Karo*, the Court made it clear that when beepers are used to enhance normal senses they can trigger Fourth Amendment scrutiny. United States v. Karo, 468 U.S. 705, 715 (1984). The reasoning of *Knotts* is that the potential to augment perception does not implicate the Fourth Amendment if a technological tool is actually used to perceive nothing more than senses could perceive. *See id.* I agree that the relevant question is how a particular form of technology has been used, not what it is capable of accomplishing.

[212] Two additional observations by the *Knotts* Court that reflect upon this article's central inquiry merit mention. The Court intimated that the devices that enhance human sensory faculties—*i.e.*, that enable human beings to exceed the limits of their ordinary perceptive powers—might not be of Fourth Amendment concern if the expansion of human capacities is minor or limited. *Id.* at 282. For this reason, the use of a searchlight or field glass to see what could not otherwise be seen would be unregulated. *See id.* at 283 (quoting United States v. Lee, 274 U.S. 559, 563 (1927)). On the other hand, the Court also suggested that the "abus[ive]" use of tools that merely accomplish what could conceivably be accomplished by unaided senses might fall under the Fourth Amendment's

The basic reasoning underlying the *Knotts* opinion seems sound.[213] It is difficult to take seriously a claim that one has a legitimate privacy interest in details one exposes to unaided eyesight in public places. The Framers' core objective—preserving a sphere of confidentiality—is not threatened when the authorities use their eyes or ears to learn those details. There would seem to be no greater threat when the authorities use technological devices to gain access to the same details. If a person's conduct really does expose facts about his life to others, the use of efficient surveillance tools to gain access to those facts does not deprive that person of any genuine interest in confidentiality. The revelatory behavior forfeits the privacy interest that might otherwise be protected. Technology is not being exploited in a manner that could shrink the scope of the privacy guaranteed by the Fourth Amendment.[214]

Two issues that the Court did not explore, however, raise serious questions about its reliance on revelatory behavior to reject the claim that beeper monitoring of public movements constitutes a search. The first issue is whether members of the public *actually do* use ordinary senses to perceive the information that an electronic tracking device perceives. The second issue is whether members of the public *actually could* use ordinary senses to perceive that information. Both issues are tied to the plausible assumption that there is more informational content in a comprehensive awareness of an individual's public movements than in the knowledge of each of the separate movements that constitute an entire journey.[215]

It is undeniable that each discrete segment of a public journey is visible to the ordinary senses of the public.

---

regulatory regime. *Id.* at 284. According to the Court, "different constitutional principles" from those that governed in *Knotts* might apply if officers were to use electronic tracking devices to implement "dragnet-type law enforcement practices" such as "`twenty-four hour surveillance of'" citizens "`without judicial knowledge or supervision.'" *Id.* at 283-84. How and why the applicable principles might differ were left unexplained.

[213] Moreover, it is consistent with *Katz* wherein the majority warned 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*, 389 U.S. at 351.

[214] As will be discussed later, for those committed to honoring the Framer's objectives and preventing contraction of the liberties sought to be preserved in the Fourth Amendment, a critical question is whether a particular interpretation of the Fourth Amendment ensures that exploitations of technology do not diminish the privacy interests that are the concern of that provision.

[215] An awareness of the whole journey may, for example, contain greater informational content insofar as it discloses the sequence of a person's visits to different establishments or individuals and the length of time spent in each particular place visited.

Perhaps every step along the way is ordinarily seen by at least one individual.[216] Typically, however, no member of the public perceives a complete picture of the individual's movements. At most, a collection of unrelated individuals learns isolated bits and pieces. No one individual or entity is privy to the greater information contained in an awareness of the entire sequence of movements from start to finish. Perhaps it is possible for one individual (or a collection of collaborating individuals) to follow the traveler and learn everything, from start to finish, but in reality that rarely, if ever, occurs. That reality raises a significant question. Is the mere *possibility* of ordinary sense perception a sufficient reason to conclude that a person has forfeited his or her interest in confidentiality by engaging in revelatory behavior? Is it not arguable that if members of the public *do not* generally perceive what the tracking device perceives then the technological tool is in fact being used to acquire information that is effectively concealed? If these are common understandings shared by members of society, is it really logical or fair to assert that the traveler has chosen to engage in actions that have publicized the very same information that the beeper captures? There may be force to the Court's view that a person surrenders any protected interest in secrecy by choosing to put information in a place where it *could* be sensed by the public. On the other hand, there is a case to be made for the competing position–that forfeitures of confidentiality attributed to revelatory behavior should be based upon what the public *does* rather than what the public *can do.*[217]

---

[216] I am willing to concede this point for the purpose of this discussion even though it may well not be the case that every component of a journey is generally viewed by someone.

[217] The Supreme Court's decision in *Bond v. United States*, 529 U.S. 334 (2000), would seem to furnish powerful support for this competing view. Therein, the Court held that tactile manipulation of soft-sided luggage in excess of what the public generally constitutes a search even though the public could lawfully manipulate the luggage to a greater extent. *Bond*, 529 U.S. at 339. This conclusion strongly suggests that whether one can fairly be charged with revelatory behavior—that is, with knowingly exposing facts about her life to the public—ought to be measured by what one generally expects the public to sense, not by what it is possible for the public to lawfully sense.

It is noteworthy that if technological tracking of public movements were to be deemed violative of privacy because it yields more information than the public ordinarily acquires by unaided senses, then unassisted human tracking that reveals the same information would also violate privacy and constitute a search. If technology is regulated because it acquires more than the public usually

A second issue not addressed by the Supreme Court in *Knotts* poses an even greater challenge to the legitimacy of the Court's "no search" conclusion. The logical premise on which the Court's conclusion rests is that the technology was not exploited to acquire anything but details that unenhanced senses *could have* perceived. The validity of that premise is not entirely clear. The fallibility of human tracking, as illustrated by the facts of *Knotts*, engenders a potentially substantial risk that ordinary human capabilities would *not* be able to gain access to the information revealed by a comprehensive electronic record of a person's travels. Errors on the tracker's part or precautions and evasion by the person being tracked might well defeat effective surveillance and preserve the confidentiality of physically exposed facts. On the other hand, beepers are effectively invisible and unlikely to fail. It is difficult, if not impossible, to take precautions against surreptitious electronic monitoring. As a result, a technological tool such as a beeper might well be capable of accessing and gathering facts that ordinary human abilities could not perceive and acquire.[218] Put simply, assuming once again that there is additional content in a comprehensive picture of one's public movements, an electronic monitoring device might dramatically improve the chances of learning that content. If a technological device is used to uncover information about an individual's life that very likely could not have been uncovered without the device, then the threat to informational privacy is real. The exploitation of the device

acquires with its senses, then nontechnological means of acquiring the same information should also be regulated.

While at first glance unaided human tracking might seem inoffensive, upon further consideration there is nothing inherently implausible about the conclusion that the government threatens legitimate interests in secrecy and engages in a search when it puts human bloodhounds on our trails to determine where we go, who we visit, and how long we stay at various locations. The Court's suggestion in *Knotts* that abusive 24-hour surveillance by beeper could constitute a search evinces a sense that we are entitled to protection against extensive monitoring that enables the authorities to learn details that could be perceived by ordinary senses. *See supra* note 212. If that is the case, the question is whether less extensive efforts to document our lives ought to be regulated when they capture information that normally remains unseen and unlearned.

[218] The *Knotts* Court noted at one point that the mere fact that the government uses a technological device that enables greater investigative "efficiency" is not a reason to deem that device subject to Fourth Amendment control. *Knotts*, 460 U.S. at 284 ("We have never equated police efficiency with unconstitutionality, and we decline to do so now."). While that conclusion seems correct, it does not respond to the concerns raised here. The issue here is not greater *efficiency* than ordinary senses, but, rather, *a greater capacity to acquire information* than is otherwise humanly possible.

effectively discloses information that might well have remained unknown and confidential.[219] Whether differences in human and technological capabilities are sufficient to justify the conclusion that the technological means endanger constitutional values is a question worthy of serious attention.

The Court's conclusion in *Knotts* is not necessarily wrong. I am not certain what the Framers would have thought of a claim of privacy in public movements, though I certainly can imagine them being concerned with the threats posed by unfettered tailing. The point of this discussion is that there are unexamined questions that cast doubt upon the Court's simplistic conclusion that technological tracking devices merely exploit an individual's decision to expose his life to public view. The revelatory behavior logic on which the *Knotts* Court rested its conclusion that beeper use is not a search is flawed and incomplete, neglecting to address the potentially greater content in complete knowledge of a person's public movements, the likelihood that the public does not generally perceive that greater content, and the degree of probability that ordinary human beings using unaided senses could not actually perceive that content.[220]

---

[219] In this situation, the additional information could not even have been gathered by means of a physical intrusion. As will be seen in the discussion of the standard I propose for evaluating whether a technological exploitation crosses the Fourth Amendment threshold, in my view devices that provide access to information that is otherwise wholly inaccessible to unaided human senses should be subject to constitutional control. *See infra* notes 437-38 and accompanying text.

[220] For provocative discussions of the issues raised by the decision in *Knotts*, see Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 581, 584 n.124 (1990) (contending that "[t]here are marked differences between a police officer using his natural senses to observe a target suspect's movements and that officer using super-sensitive electronic devices to keep track of the target. . . . [T]he invasion by a beeper is ongoing and the electronic device's tracking is inescapable . . . ."); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 603 (1989) (maintaining that *Knotts* allows the government to undertake intrusive surveillance that is equivalent to "everyone in town pool[ing] their collective knowledge of a particular individual's travels and buil[ding] a daily record of every place the individual went, everyone visited, and the length of each stop" and suggesting that "if people expected such nosey behavior from others, evasive driving maneuvers might become the norms"); Arnold H. Loewy, *Protecting Citizens From Cops and Crooks: An Assessment of the Supreme Court's Interpretation of the Fourth Amendment During the 1982 Term*, 62 N.C. L. REV. 329, 353 (1984) (arguing that the assumption that what is learned from beeper use could also be learned by unaided surveillance is questionable because "the unseen beeper renders it impossible to know one is being followed" whereas visible surveillance, while "intrusive, . . . would at least

Genuinely revelatory behavior should forfeit privacy, but before high-tech tracking of our travels is deemed outside the purview of constitutional concern, persuasive responses to these concerns are essential.

b. The Second Variation: The Technological Preservation or Communication of Information Voluntarily Conveyed to Third Parties

The second variation on the revelatory behavior theme is the premise that the use of technology merely to preserve or communicate information that an individual has voluntarily decided to convey to a third party poses no threat to the privacy interests protected by the Fourth Amendment. The reasoning of *United States v. White*[221] illustrates the operation of this premise.

White was decided just four years after the Court had held in *Katz* that electronic eavesdropping without physical intrusion was a search.[222] The *White* plurality concluded that there was a crucial distinction between the conduct in the two cases.[223] Unlike *White*, "*Katz* involved no revelation to the Government by a party to conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police."[224] In the Court's view, one who puts confidences at risk by voluntarily disclosing them to another does not have a

leave the innocent citizen with the option to preserve his privacy" by choosing not to visit a particular place); Wayne R. LaFave, *Supreme Court Review: Fourth Amendment Vagaries (of Improbable Cause, Imperceptible Plain View, Notorious Privacy, and Balancing Askew*), 74 J. CRIM. L. & CRIMINOLOGY 1171, 1175-76 (1983) (calling the "assumed equivalence between mere `visual surveillance' and `scientific enhancement' in *Knotts* . . . troublesome," and declaring that "the two investigative techniques simply are not the same" because tracking devices go "`far beyond any ordinary powers of observation,'" "permit[] a much more extended and thorough surveillance of an individual than would otherwise be possible," and may enable law enforcement in the future "to carry out a volume of surveillance activity far beyond that which would otherwise be feasible with available manpower and resources").

[221] 401 U.S. 745 (1971).

[222] *Katz*, 389 U.S. at 353.

[223] *White*, 401 U.S. at 749.

[224] *Id.* According to Justice White, while the "no trespass" rationale of the *On Lee* decision could not "survive" *Katz*'s abolition of the *Olmstead* doctrine, the second, independent rationale for the result in *On Lee*—that the Fourth Amendment does not govern "eavesdropping on a conversation, with the connivance of one of the parties"—remained valid in the post-*Katz*, interest-oriented threshold era. *Id.* at 750. In dissent, Justice Harlan rejected the notion that the second *On Lee* rationale constituted an "independent ground" for the Court's holding. *Id.* at 774 (Harlan, J., dissenting).

justifiable expectation that those confidences will remain private from anyone to whom the intended recipient chooses to divulge them. Consequently, when the intended recipient shares them with others—including the government—no search occurs.

Every Justice apparently agreed that the government does not violate privacy when it merely uses "false friends" to acquire and share voluntary disclosures.[225] The individual's revelatory behavior—in this instance, not general public exposure but specific disclosure to another person—sacrifices any interest that the information will remain confidential from the intended recipient. Because those who willingly share their thoughts know (or should know) that the intended recipients are free to share disclosed information with others, the same revelatory behavior also undermines the legitimacy of an interest that the information will remain secret from anyone to whom the recipient chooses to reveal it. Both the initial loss and any subsequent loss of privacy are the result of the speaker's decision to disclose secrets, placing them beyond his control and taking the chance that they will be revealed further.[226] Neither the initial receipt of the information nor its later transmission to the government constitutes a "deprivation" or "violation" of privacy.

The Justices divided, however, over whether the use of technology—electronic recording and transmitting devices—dictated a different conclusion. Dissenters

[225] *Id*. at 751 ("[T]he conduct and revelations of an agent operating without electronic equipment do not invade . . . constitutionally justifiable expectations of privacy . . . ."). None of the concurring or dissenting Justices questioned the premise that unaided false friends pose no Fourth Amendment issues. *See id*. at 755 (Brennan, J., concurring in the result) (maintaining only that electronic monitoring and recording are subject to the Fourth Amendment); *id*. at 760 (Douglas, J., dissenting) (contending only that electronic surveillance must be controlled by Fourth Amendment constraints to avoid the development of a police state); *id*. at 784-90 (Harlan, J., dissenting) (maintaining that electronic monitoring, unlike the use of unequipped false friends, must be regulated by the Fourth Amendment because it has a much more dramatic impact on privacy and security).

[226] According to the Court, the speaker assumes "the risk" that his conversations will be shared with others, including the government. *See id*. at 752; *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (applying similar reasoning to a situation in which bank officials shared the information contained in customer records with the authorities); California v. Greenwood, 486 U.S. 35, 40-41 (1988) (applying similar reasoning to a situation in which a trash collector conveyed the contents of discarded refuse to law enforcement officers).

suggested that technologically-armed false friends ought to trigger Fourth Amendment scrutiny.[227] The *White* plurality[228] rejected the claim that the involvement of technology in the process should affect the analysis and alter the outcome. The Justices could perceive no constitutionally significant difference between the unaided informant who hears, remembers, and relates the information by mouth and the informant who records or transmits that information by electronic device.[229] If a speaker has no claim when a participant in a conversation listens to and orally recounts his conversations, he has no claim when the same participant records and hands over his captured conversations or when the participant transmits those conversations instantaneously to distant law enforcement agents. In all three instances, the government merely takes advantage of the individual's decision to put his or her privacy at risk; it does not intrude into a realm of preserved confidentiality.

The conclusion that the use of technology did not make a difference did not rest on the premise that speakers assume the risk of electronic recordation or transmission or on the premise that recording and transmitting devices do not enhance human capabilities. By affording means for accurate and complete preservation and instantaneous conveyance of information, these tools dramatically enhance human memory and communication capacities. As I read *White*, the addition of technology to the false friend equation made no difference because the technologies employed did not enable the authorities to breach the confidentiality of any information in which the speaker had retained a privacy interest. The technological enhancements were surely used to exploit the speaker's revelatory behavior more effectively, but they were not used in a way that increased or sharpened the government's ability to perceive or acquire concealed facts.[230] The government did not exploit technology to learn

---

[227] *White*, 401 U.S. at 790 (Harlan, J., dissenting) ("The Fourth Amendment does, of course, leave room for the employment of modern technology in criminal law enforcement, but in the stream of current developments in Fourth Amendment law I think it must be held that third-party electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society.").

[228] Only three additional Justices joined Justice White's opinion in *White*. Justice Black cast his vote with the plurality solely on the basis of his disagreement with the Court's holding in *Katz*. *Id.* at 754 (Black, J., concurring in the judgment).

[229] *Id.* at 752-53 (asserting that "there is no persuasive evidence that" there is a "substantial enough" difference "between the electronically equipped and the unequipped agent" to merit "discrete constitutional recognition").

[230] *Id.* at 753 (emphasis added) (asserting that the effect of the percipient

any private details that it could not have learned by relying on the hearing and reporting skills of an unaided informant. For these reasons, the government's exploitation of technology did not threaten the privacy interests sheltered by the Fourth Amendment and did not amount to a search.

The *White* Court's holding that technological means of surveillance did not implicate the Fourth Amendment rests squarely on two premises. The first is that the use of ordinary human faculties by a faithless third-party participant in a conversation to hear, remember, and report voluntarily divulged information does not deprive a trusting speaker of a protected Fourth Amendment interest in secrecy, but merely capitalizes on behavior that relinquishes privacy. The second essential premise is that when tools of technology are used to preserve and transmit divulged information more accurately and more quickly, they enhance memory and communication but occasion no greater breach of informational privacy. Together, these premises support the conclusion that when informants use electronic equipment to capture or transmit what they have been told, all losses of confidentiality are attributable to the foolish speaker's revelatory conduct.

I have always had doubts about the validity of the first premise—that the government's use of unaided false friends are of no concern to the Fourth Amendment. I wonder whether official efforts to recruit and place untrustworthy auditors in our presence either to encourage us to disclose or merely to receive information we are willing to share is as harmless to constitutional values as the Justices believe.[231] Obviously, if this premise is flawed—if unequipped informants who hear, elicit, and recount disclosures violate privacy and trigger Fourth Amendment control—then the use of electronic aids for the same purpose would also violate privacy. For purposes of this discussion, however, I accept the validity of the first premise. Because my concern is with the relationship between technology and the Fourth Amendment's reach, I focus attention on the Court's second

third party's use of an electronic device was merely to "produce a *more reliable* rendition of what a defendant has said" and "a *more accurate* version of the events").

[231] For an extended discussion of some of the reasons for my sense that the government's use of unaided false friends may pose cognizable threats to constitutional values, see Tomkovicz, *supra* note 19, at 728-29.

premise–that the threats to privacy from technologically-armed false friends are no different from or greater than the threats to privacy from their unarmed counterparts.

If faithless auditors equipped with electronic recorders or transmitters inflict no greater damage upon informational privacy interests, there is probably no reason to subject them to Fourth Amendment control. If the same facts can be perceived and acquired by the government whether ordinary human abilities or the more efficient mechanisms afforded by progress are used, then the Court is correct to conclude that this particular technological exploitation poses no cognizable threat to confidentiality.[232] A technological device that does not augment ordinary abilities to perceive or acquire information, but merely modifies the perception or acquisition processes in ways that have no impact on secrecy should not be an object of Fourth Amendment concern.

Once again, while the Court's basic logic is sound, its analysis of the implications of electronic participant monitoring is distressingly incomplete. There are reasons to question whether the impacts of technology are as limited and innocuous as the Court believes. Electronic recorders and transmitters may well enable the authorities to acquire *more* information than ordinary, unenhanced human faculties.[233] A human being's abilities to hear, remember, and recount are far from perfect. While there is a chance that a false friend *might* be able to perceive, recall, and report every word spoken by another, there is a sizeable, virtually inevitable, risk that human deficiencies will preclude full reception, retention, and communication of the critical information whose privacy has been put at risk by the

[232] Of course, if the use of technology in these situations endangers other Fourth Amendment values, a different conclusion would be justified. Based on my beliefs about the objectives of that provision, however, I see no other threat that would justify Fourth Amendment scrutiny. I do not deny that other Fourth Amendment interests exist and were the aim of the Framers. It seems likely that they were concerned, for example, with safeguarding an interest in quiet repose in our homes and an interest in bodily dignity and integrity. Situations in which technological means of surveillance are used generally pose no peril to these interests.

[233] Defensible constitutional solutions to exploitations of technology demand close scrutiny of the perceptive and acquisitive capacities of unaided human faculties and the perceptive and acquisitive capacities of the particular device at issue. If there is no difference between the two or if the difference is negligible, then the use of a technological device should be treated like the use of ordinary senses. However, if a modern development measurably improves human abilities to sense and learn information not accessible otherwise—or not accessible without engaging in behavior that would trigger Fourth Amendment regulation—then there is a substantial basis for concluding that its use does cross the Fourth Amendment threshold.

speaker's willingness to disclose it to another. Although electronic listening, recording, and transmitting tools could malfunction, the chance of that occurring is much smaller. By preserving a tangible record of conversations or instantaneously communicating a speaker's words to the authorities' ears, these devices increase the opportunities for the government to acquire information divulged. Devices that appear to merely accurately preserve and accelerate the transmission of conversations may also dramatically enhance the government's powers of perception and acquisition by eliminating human failings and deficiencies. The enhancements of memory and the acceleration of communication—indeed, the capacity to hear the exact words of the speaker as they are spoken, not a later rendition by a third-party—enable the government to perceive and to acquire information that would, in all likelihood, otherwise have remained private.[234] This reasoning suggests that false friends equipped with technological tools threaten the privacy at the core of the Fourth Amendment.[235]

It is possible that the additional dangers to informational privacy posed by the use of technological tools are insufficient to trigger constitutional scrutiny. Perhaps the chance that the government will learn substantially more information is negligible, small enough to ignore. It does not seem sensible, however, to conclude that there is positively no possible difference in the substance of what the authorities can gather by reliance on ordinary human abilities and what they can gather by reliance on electronic recording or transmitting devices. The differences, which could be quite substantial, ought to be analyzed and evaluated in deciding whether the use of electronic listening and recording devices by third persons triggers Fourth

[234] One difficult question for those who subscribe to this logic is whether *all* information gathered and passed along through electronic mechanisms is the product of a violation of privacy. The government could have learned some of the details by using an unequipped agent. The technology has merely ensured receipt of a complete account. The problem is that it is impossible to determine what could have been gained without the device.

[235] Another basis for concluding that the Fourth Amendment might be concerned with electronically-assisted false friends is the arguably more severe damage done to other freedoms that are furthered by our ability to preserve the confidentiality of information about our lives. *See* Tomkovicz, *supra* note 19, at 729 n.339.

Amendment scrutiny.

In sum, the *White* Court's assessment of an electronically-equipped agent as more efficient than the unaided agent, but as no greater threat to privacy, fails to account for the very real possibility that electronic devices increase the government's access to information it would otherwise be unable to learn, and casts doubt on the Court's threshold holding. There may be a plausible reason why the technological enhancement of the ability to learn the details of a person's life should not be governed by the Fourth Amendment. The flawed assertion that a mere false friend and a technologically-assisted false friend have the same abilities to secure, preserve, and communicate information, however, is not such a reason. In the absence of a more convincing rationale, the potential for increased harm to valued interests in secrecy furnishes a logical basis for holding that a third party's recordation or transmission of conversations is a search within the meaning of the Fourth Amendment.[236]

c. The Third Variation: The Voluntary Disclosure of Information to Technological Devices

The third variation on the revelatory behavior theme holds that the choice to disclose information to technological devices that provide access to otherwise imperceptible matters forfeits the Fourth Amendment privacy interest in those matters. *Smith v. Maryland*,[237] the landmark case in

[236] This conclusion is neither novel nor unprecedented. Dissenters in *White* would have held that technologically-equipped false friends pose cognizably greater threats to the "security" that is promised by the Fourth Amendment and must satisfy that provision's requirements. *See White*, 401 U.S. at 787 (Harlan, J., dissenting). Some state courts have concluded that the government's surreptitious employment of an electronic device to capture conversations violates the state's constitutional guarantee of privacy. *See, e.g.*, State v. Geraw, 795 A.2d 1219, 1220 (Vt. 2002) (concluding that the Vermont Constitution prohibits secret recordings of police interviews in the home "without the protection of a judicially authorized warrant"); Commonwealth v. Brion, 652 A.2d 287, 287 (Pa. 1994) (concluding that the Pennsylvania Constitution "precludes the police from sending a confidential informer into the home of an individual to electronically record his conversations and transmit them back to the police"); Commonwealth v. Blood, 507 N.E.2d 1029, 1034 (Mass. 1987) (stating that "in circumstances not disclosing any speaker's intent to cast words beyond a narrow compass of known listeners . . . it is objectively reasonable to expect that conversational interchange in a private home will not be invaded surreptitiously by warrantless electronic transmission or recording" and that the consent of one of the parties does not "alter[] the balance as to obviate the need for a warrant requirement"); State v. Glass, 583 P.2d 872, 879 (Alaska 1978) (holding that "Alaska's privacy amendment prohibits the secret electronic monitoring of conversations upon the mere consent of a participant").

[237] 442 U.S. 735 (1979).

which the Court endorsed Justice Harlan's two-pronged test for reasonable expectations of privacy, exemplifies this logic.[238]

As noted earlier, the *Smith* Court held that the use of a pen register to record numbers dialed from a residential telephone was not a search.[239] The majority first expressed doubt that telephone users have *actual* expectations of privacy in the numbers they dial because they realize that they have to convey these numbers to the telephone company, that the telephone company has facilities for making records of the numbers, and that the telephone company sometimes makes such records for business purposes.[240] The majority then concluded that even if the petitioner had a "subjective expectation that the phone numbers he dialed would remain private, this expectation [was] not `one that society is prepared to recognize as "reasonable."'"[241] The reason was that a person "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[242] In *Smith*, the petitioner had "voluntarily conveyed" the numbers he was dialing "to the telephone company" and "assumed the risk that the company would reveal to police the numbers he dialed."[243]

The Court's threshold reasoning in *Smith* bears a clear resemblance to its reasoning in *White*. Both rely heavily upon

---

[238] *See Smith*, 442 U.S. at 740.

[239] *Id.* at 745-46.

[240] *Id.* at 742-43.

[241] *Id.* at 743 (quoting *Katz*, 389 U.S. at 361).

[242] *Id.* at 743-44.

[243] *Id.* at 744. At an early, prefatory point in its analysis, the *Smith* Court also noted that the technology employed by the government "differ[ed] significantly from the listening device employed in *Katz*," because it did "not acquire the *contents* of communications," but, rather, only captured the numbers dialed. *Id.* at 741. It would be a mistake to conclude that this observation means that technology is not to be subject to Fourth Amendment oversight unless the information that is or can be acquired meets certain "content" standards. In the *Smith* opinion, the "content" factor does not appear to be an independently sufficient reason to deny Fourth Amendment protection. At best, it seems superfluous—a makeweight offered to bolster a conclusion rooted in other reasons. Moreover, subsequent decisions have indicated that as a general matter the Court looks unfavorably upon threshold distinctions based on the kind, quality, or amount of information acquired—particularly with regard to in-home activities. *See infra* notes 282-300 and accompanying text. If the "content" factor in *Smith* has any impact, it would seem to be a potential limitation on the scope of the Court's holding. The lesser content in numbers could provide a basis for distinction in a future case in which conversations are intercepted by the telephone company.

the sacrifice of privacy resulting from voluntary disclosures to third persons cooperating with the authorities. However, there is a critical difference in the use of technology in the two cases—a difference that yields quite distinct lessons. In *Smith*, the government did not use a device to accomplish the same perceptive and acquisitive purposes that it could have achieved by using ordinary human senses.[244] The pen register was essential to the perception and acquisition of the numbers dialed from the home telephone. The technology was used in a manner that did enhance human perceptive capacities, enabling the authorities to intercept information that could not have been seen, heard, or otherwise acquired by human senses. Without the pen register, the information would have remained confidential and unknown.

Despite this difference from *White* (and from *Knotts*), the Court reached the same conclusion—the official exploitation of technology did not violate a reasonable expectation of privacy and did not qualify as a search. The Court reasoned that the petitioner, aware that the phone company possessed and employed equipment that could sense and record the numbers that were dialed, had chosen voluntarily to convey the "numerical information to the telephone company and [had] `exposed' that information to its equipment in the ordinary course of business."[245] Moreover, in the current state of telephone technology, the "switching equipment that processe[s] . . . numbers is merely the modern counterpart" of a human operator.[246] A caller could not have made a plausible privacy claim in information revealed to the operator, and "a different constitutional result [was not] required because the telephone company has decided to automate."[247]

In essence, a claim that the use of a pen register intrudes upon privacy lacks merit because a person who uses a residential telephone freely elects to share the numbers dialed with phone company mechanisms, aware that those mechanisms can perceive and retain the numbers. It does not matter whether one chooses to share otherwise confidential matters with another person's naked senses, *i.e.*, the operator's ears, or with sophisticated mechanical sensors, *i.e.* a pen register. In either case, he takes the chance of

---

[244] Although I have concluded that this premise is questionable in *White*, it was the basis relied on by the Court to support the conclusion that the informant's use of a recording or transmitting device was not a search.

[245] *Smith*, 442 U.S. at 744.

[246] *Id.*

[247] *Id.* at 745.

perception, retention, and of divulgence to others. In an earlier day, by telling the operator the number he wished to reach, he contradicted the validity of a contention that the operator violated his privacy by learning the numbers. Today, by engaging in the revelatory behavior of dialing the telephone, he contradicts an assertion that the use of technology to learn the numbers deprives him of a legitimate interest in secrecy. It is unreasonable to expect or to claim privacy when one opts to surrender it to man or machine.[248]

The clear lesson is that when a technological device does augment human perceptive abilities, if the authorities employ it only to gain access to facts that an individual willingly conveys to the device, they merely take advantage of the individual's lack of regard for secrecy and cannot be charged with breaching an interest in confidentiality. Even if a device has the capacity to enhance human senses in ways that threaten informational privacy, if the manner of use involves mere exploitation of revelatory conduct, then the use does not constitute a search. Technology-aided acquisition of otherwise imperceptible details does not deprive a person of a cognizable privacy interest when the individual has made an informed, willing choice to disclose those details to the technology. Revelatory conduct surrenders confidentiality and defeats the claim that the government has infringed upon a constitutionally protected

[248] My explanation of *Smith's* logic reflects the view that the Court's reliance on the fact that a pen register is a modern, mechanical surrogate for the animate operators of an earlier era is *not* an independent and adequate basis for the Court's holding. As I read *Smith*, the Court's primary reliance was on the dialer's choice to disclose the numbers to the equipment with powers of perception and acquisition beyond those possessed by humans. *Smith*, 442 U.S. at 744-45. The discussion of the relationship between operators and pen registers and of the analogous role played by each was intended to bolster the conclusion that such revelatory behavior forfeits confidentiality even if a device with unique perceptive powers is needed to acquire the information. If I am correct, then the modern counterpart reasoning is either superfluous (*i.e.*, the same conclusion would have been reached without it) or limiting (*i.e.*, a search would not have been found, despite the choice to disclose information to the pen register, if there had been no human predecessor that served the same function). My sense is that the first alternative is the most likely.

It is possible that the operator surrogate reasoning provides an independent and adequate basis for the conclusion in *Smith*. Under that interpretation, if a modern technological device is a substitute for a human operative against whom there would be no legitimate privacy claim, the use of the device does not trigger Fourth Amendment coverage even if the individual has not voluntarily and knowingly chosen to reveal the information to the device. This seems to me to be an implausible reading of *Smith*. Moreover, the constitutional reasoning it reflects seems indefensible.

privacy interest. One cannot logically expect or demand secrecy from a sense-enhancing mechanism when one chooses to convey information to that mechanism, cognizant that it can be and is used to capture such information.[249]

The *Smith* Court's conclusion stands on two legs. The first leg is that no cognizable privacy breach occurs when the government recruits third-party recipients to acquire and report disclosures.[250] The second leg is that if the third-party uses technology that enhances human abilities to capture those disclosures, no cognizable intrusion on privacy occurs if the individual has knowingly chosen to communicate with the sense-enhancing device. As noted earlier, I have unsettled doubts about the conclusion that we cannot legitimately expect the government not to enlist confidantes to receive and report details we are willing to entrust to them. Those doubts grow even stronger in situations where

[249] For critical scholarly assessments of the Court's reasoning and holding in *Smith*, see WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §2.7(b) (3d ed. 1996) (calling *Smith* "a crabbed interpretation of the *Katz* test [which] makes a mockery of the Fourth Amendment."); Joseph D. Grano, *Crime, Drugs, and the Fourth Amendment: A Reply to Professor Rudovsky*, 1994 U. CHI. LEGAL F. 297, 308 (deeming the result in *Smith* "antithetical to the defining norms of a free society" and in "conflict with the Fourth Amendment's underlying purposes"); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 600 (1989) (maintaining that *Smith* "rests on a fallacy" and that the "governmental snooping" it permits "smacks of Orwell's Big Brother, protection from which is the essence of the fourth amendment"); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1254-55 (1983) (alleging that *Smith* betrays a "lack of concern for the innocent" and suggesting that because *Smith* leaves "government officials . . . perfectly free to learn every telephone number that any person dials, subject only to the cooperation of the telephone company," the decision has "an intolerable impact . . . on the innocent").

For illustrations of the judicial disagreement with the Court's handling of the issue addressed in *Smith*, see People v. Chapman, 679 P.2d 62, 67 n.6 (Cal. 1984) (observing that the federal courts' acceptance of "the fiction that there is no expectation of privacy in . . . outgoing telephone call records . . . because the user voluntarily conveys this information to a third party" stands in contrast to California's view); Commonwealth v. Beauford, 475 A.2d 783, 789 (Pa. Super. Ct. 1984) (opining that an individual who uses a home or office telephone "fully expects that the number he is about to dial will remain as private as the contents of the communication he is about to have" and that the "caller certainly evidences no intention to shed his veil of privacy merely because he chooses to use the telephone to make private contacts," and concluding that "a caller and the person he calls expect and are entitled to as much privacy in the fact that they are talking to one another as in what they say to each other"); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) (opining that a "telephone subscriber . . . has an actual expectation that the dialing of telephone numbers from a home telephone will be free from governmental intrusion" and that this expectation "is a reasonable one").

[250] For a discussion of this threshold reasoning, see *supra* notes 221-26 and accompanying text.

the third-party is a commercial entity or public utility.[251] Nonetheless, because my concern is with technology, I again assume the validity of the voluntary disclosure to third parties logic.[252]

The question is whether it should make a difference that the government-enlisted recipient of voluntary disclosures has employed a mechanism that perceives and retains information inaccessible to ordinary human faculties. In general, I agree with the second logical leg on which *Smith* stands. If a person has genuinely and freely chosen to communicate facts to a mechanism, knowing it can and does sense and record those facts, the person has no better claim that a breach of confidentiality has occurred than when he or she speaks to functioning ears or acts in front of percipient eyes. Knowing, voluntarily revelations to specialized machines should forfeit any interest in the secrecy of the information revealed.

The Court's application of this logic to the facts of *Smith*, however, reflects an insufficiently thorough analysis of the relevant variables. The Court failed to seriously address the implications of the possibility that telephone users do not expect the phone company to sense and retain local numbers, dismissing this concern with an assertion that dialers know the capacity to record exists and that recordation of local numbers sometimes occurs. If a realistic telephone user, in fact, would believe it to be quite unlikely (even extremely

[251] As Justice Marshall has said, in these situations the "choice" to convey the information is hardly as free as in situations involving optional conversations with other private persons. If one wants to function effectively in modern society, there is a need to share information with an increasing number of institutional entities. *See Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting) (contending that assumption of risk entails "some notion of choice," and that "[i]t is idle to speak of `assuming' risks in contexts where . . . individuals have no realistic alternative" because they must disclose information in order to take advantage of "a personal or professional necessity" like a telephone); *see also* Commonwealth v. Beauford, 475 A.2d 783, 789 (Pa. Super. Ct. 1984) ("In modern-day America the telephone call is a nearly indispensable tool used to conduct the widest range of business, government, political, social, and personal affairs."). Moreover, the choices among recipients of the information that must be furnished are restricted because there are finite numbers of banks, phone companies, and energy providers. In my view, these distinctions from the typical false friend case strengthen the argument that the people might be entitled to expect their government not to insinuate itself into relationships with such third parties–at least not without reason.

[252] Of course, if the first leg were invalid it would not be necessary to address the second leg. The third party's conduct would constitute a search whether or not a technological sense-enhancing device were used.

unlikely) that the phone company would capture the information conveyed, then it is arguably both illogical and unfair to charge phone users with revelatory conduct that sacrifices an interest in confidentiality. If those who dial local numbers have good reason to believe that those numbers will never be accessed by percipient human beings, but will merely be processed by insensate mechanisms, their decision to dial the telephone may not betray a lack of concern with or interest in preserving confidentiality. To the contrary, it may be both rational and legitimate for an individual to believe that she has acted in a way that will maintain secrecy from the third party phone company.

The Court's view is that by deliberately taking *any chance* that the telephone company *could* sense and retain the information for human review, the dialer forfeits a claim of secrecy. The magnitude of the risk known or taken is apparently irrelevant. While this position may be defensible, when the sole basis for denying constitutional shelter is that an individual has behaved in a way that surrenders confidentiality, the magnitude of the chance that revelation will actually occur seems highly relevant. The proposition is at least worthy of discussion. The reasoning that I find logical is that people who knowingly disclose information about their lives to others or others' technology cannot sensibly claim that it will remain secret from the recipients. When they have good reason to believe that there is little or no realistic chance of actual perception, it is rational to anticipate and to assert an interest in confidentiality. If *any risk* of perception and acquisition is to be treated like certainty, *i.e.*, as a basis for finding that privacy has been relinquished, a better explanation of why and how that result comports with the Fourth Amendment seems essential.[253]

[253] An explanation may be implicit in the Court's declaration that the technology at issue in *Smith*, the pen register, was a modern substitute for the hearing, remembering human operator of an earlier age and that the phone company's decision to automate ought not give rise to a privacy interest that would not have existed prior to automation. The likelihood of reception and retention by a human operator was great. Consequently, the decision to tell an operator the number one wanted to reach would have contradicted a claim that the number would remain secret from the operator. Perhaps the Court's view is that because modern switching equipment is essentially a "mechanical operator," the same conclusion must follow. That view is unpersuasive.

Whether a person should be charged with forfeiting interests in confidentiality ought to be judged by the realities of the world in which he has acted, not some no longer extant world. We live in a modern, automated world, a world of altered risks and expectations. If there is no reason to believe that modern equipment senses and retains the numbers like human operators, then the decision to dial telephones has different significance. Dialing is not genuinely revelatory behavior that is inconsistent with a desire for and anticipation of

My refrain is growing as familiar as the Court's analytical tendencies. The third variation on the revelatory behavior theme is basically logical. The choice to disclose information to a modern marvel with perceptive and acquisitive capacities that outstrip those of mere mortals is a reason for finding no deprivation of confidentiality. A genuine choice to disclose information to others' ordinary senses renders ludicrous the claim that we expected and are entitled to privacy from those others. The fact that we have made such disclosures to an inanimate mechanism that captures, preserves, and renders them accessible to ordinary senses should make no analytical difference. Nonetheless, before concluding that this principle governs any particular situation, it is essential to carefully evaluate whether it is fair to conclude that the individual has chosen to share facts with a technological device. An accurate picture of what the mechanism can do, of how it is actually used, and of common understandings, expectations, and risks is required.

2. The "Informational Content" Factors

A number of the Court's threshold technology decisions have relied upon factors that fall within an "informational content" category. These factors have been influential, sometimes dispositive, in resolving claims that technological exploitations have crossed the threshold of the Fourth Amendment. Once again, the Court has played three variations on the theme–the "no information at all" variation, the "only insignificant or illegitimate information" variation, and the "any detail about the home" variation. The first two have resulted in denials of constitutional coverage, while the latter has yielded Fourth Amendment regulation of surveillance made possible by technological tools.

The essential logic that underlies the category is that whether a constitutionally cognizable interest in confidentiality or secrecy is jeopardized can depend on whether the government's conduct might enable it to learn any facts entitled to Fourth Amendment protection. If informational privacy is the core interest safeguarded by constitutional control over searches–and I have previously suggested that this is a logically defensible proposition–then

privacy.

it seems eminently sensible to link the scope of Fourth Amendment governance to the potential for disclosures of matters with "informational content." There are two pertinent inquiries: whether any details might be revealed and whether those details are worthy of constitutional shelter.

a. The First Variation: Official Conduct that Can Reveal No Information at All

Conduct involving technological advances that has absolutely no potential to reveal any information to the authorities does not cross the Fourth Amendment's threshold and cannot qualify as a search. In *United States v. Karo*,[254] the respondents claimed that the transfer of a beeper-infected container to them was a Fourth Amendment search.[255] The Court's simple, direct response was that the "mere transfer . . . of a can containing an unmonitored beeper infringed upon no privacy interest" because "it [could] convey no information at all."[256] The act of delivering an object that has a beeper installed cannot, by itself, enable the authorities to learn any details, much less details that a recipient would wish to keep private. It cannot possibly uncover any facts about a person's life. For threshold purposes, it does not matter that *subsequent* conduct involving the beeper–*i.e.*, monitoring the electronic signal it emits–can reveal information.[257] Because no loss of confidentiality or secrecy can be occasioned by the transfer of an object laden with a beeper, that action alone does not qualify as a search within the meaning of the Fourth Amendment.[258]

---

[254] 468 U.S. 705 (1984). The Court's opinion in *Karo* makes an even more significant contribution to the third variation on the informational content theme–the notion that all in-home details are constitutionally protected. *See infra* notes 282-301 and accompanying text.

[255] *Karo*, 468 U.S. at 711.

[256] *Id*. at 712.

[257] *See id*. (observing that while the transfer of the beeper-laden container to Karo "created a *potential* for an invasion of privacy, . . . we have never held that potential, as opposed to actual, invasions of privacy constitute searches" and asserting that "[i]t is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence").

[258] *Id*. at 712-13. The respondents in *Karo* could not challenge the *installation* of the beeper because the can of chemicals was not in their possession at the time it was installed. *Id*. at 711. Nonetheless, the reasoning of *Karo* surely dictates the same threshold conclusion regarding the installation of a beeper that does not involve physical intrusion into the interior of the host object. In the absence of a physical intrusion that could expose the interior of the object, mere attachment of an electronic tracking device has no potential to reveal

The Court's threshold conclusion in *Karo* regarding the transfer of a beeper-infected object seems logically consistent with the purposes of the Fourth Amendment. If the core concern of the Fourth Amendment is informational privacy—*i.e.*, if the primary object is to enable "the People" to keep their lives confidential if they wish to do so–then the mere fact that a technological device has the *potential* to disclose private information should not trigger the application of the Fourth Amendment. There is no need for "preemptive" regulation based on future conduct involving the device. The placement of a listening device on a telephone booth ought not cross the constitutional threshold simply because that device, when activated, could capture confidential private conversations otherwise confined within the booth. Only when a technological mechanism is actually put to use in some fashion that risks revelation of confidential details should the mechanism raise constitutional concerns.[259]

information. *See, e.g.*, United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999) (holding placement of tracking device on undercarriage of vehicle was not a search in part because "the officers did not pry into a hidden or enclosed area"); United States v. Worthington, 544 F.2d 1275, 1281 (5th Cir. 1977) ("[a]ttempted use" of beeper installed on aircraft "is without significance" because "it malfunctioned shortly after its installation and its use produced no evidence whatsoever").

The respondents also claimed that the transfer of the container harboring the beeper was a "seizure" within the meaning of the Fourth Amendment. *Karo*, 468 U.S. at 712-13. The Court concluded that although the act of transferring the container was a "technical trespass," it was not a seizure because it effected no "meaningful interference with" the possessory interests in the container. *Id.* The same conclusion–that no *meaningful* interference with possession results–would undoubtedly apply to installation of a beeper in an object already in the possession of an individual.

[259] In opinions involving investigations without technological assistance, the Court has stretched the "no information at all" threshold criterion, expanding its influence. The Court has found that the Fourth Amendment's threshold is not crossed in situations where it is a "virtual certainty" that government conduct will reveal no information, *see* United States v. Jacobsen, 466 U.S. 109, 118-20 (1984) (holding reopening of package not to be a search because of virtual certainty that agents would not learn anything they did not already know), and in situations where there is not "a substantial likelihood" that the actions of the authorities will disclose any facts. *See* Illinois v. Andreas, 463 U.S. 765, 773 (1983) (holding opening of package already examined by government agents not a search because of lack of "a substantial likelihood" contents had changed in interim). It seems likely that these principles would also be applied to technological means of investigation.

In cases where the probability of revealing confidential details about a person's life is truly negligible, the Court's extension of this factor's influence seems defensible. The Framers might well have been unconcerned with acts that have virtually no chance of breaching valued interests in secrecy. In any

The physical intrusions that troubled our ancestors threatened to uncover confidential information about individuals' lives. If a particular use of technology can reveal no information at all, it does not pose analogous dangers to secrecy. Whether or not technology is involved, conduct that does not imperil the values that motivated the Framers should not be deemed a "search."[260]

b. The Second Variation: Official Conduct that Can Reveal Only Insignificant or Illegitimate Information

The second variation on the informational content theme, a theme which has found expression in two different technological contexts, is of questionable validity. In *United States v. Place*,[261] the Court deemed a drug-sniffing canine's examination of a piece of publicly-situated luggage not to be a search because the "investigative procedure . . . [was] so limited both in the manner in which the information [was] obtained and in the content of the information revealed."[262] With regard to the manner of the intrusion, the sniff did not involve an opening of the luggage or the exposure of other contents. With regard to the content of the potential disclosure, the sniff could reveal "only the presence or absence of narcotics, a contraband item."[263] Just one year later, in *United States v. Jacobsen*,[264] the Court held that a chemical field test used to determine the identity of a suspicious powder was not a search.[265] The investigative technique at stake "could disclose only one fact previously unknown . . . whether or not [the] powder was" contraband.[266] A negative field test result (a finding that the substance was not narcotics) would reveal "nothing of special interest," while a positive outcome (a finding of contraband)

situation in which there is a more than negligible chance that a private detail could be learned, however, there would seem to be no adequate reason to deem the government conduct outside constitutional purview. The searches that were the object of the colonists' antipathy were not "certain" to deprive a person of privacy.

[260] My agreement with the Court also rests on a belief that conduct of this sort poses no peril to other potential "privacy" interests that might well be entitled to Fourth Amendment protection–*e.g.*, interests in quiet repose or in bodily integrity and dignity.

[261] 462 U.S. 696 (1983).

[262] *Place*, 462 U.S. at 707. This holding has recently been reaffirmed and extended to canine-sniffs of vehicles in public places. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000).

[263] *Id.* at 707.

[264] 466 U.S. 109 (1984).

[265] *Jacobsen*, 466 U.S. at 120.

[266] *Id.* at 122.

would not infringe upon a "legitimate privacy interest" because "the interest in `privately' possessing" narcotics has been deemed "illegitimate" by Congress.[267] In sum, like a dog sniff, this scientific method had the potential to reveal concealed facts with exceptionally limited informational content.

Together, these two cases teach a simple, though controversial, lesson about the Fourth Amendment's regulation of human sense enhancements afforded by scientific progress. If the only information that a novel investigative technique can disclose is either the "insignificant" fact that contraband is not present or the "illegitimate" fact that contraband is present, the exploitation of that technique does not violate a reasonable expectation of privacy.[268] Disclosures of details so limited in content and character are not thought to pose meaningful threats to the central constitutional interest in confidentiality. *Place* and *Jacobsen* rest on an assumption that the Fourth Amendment is unconcerned with protecting the secrecy of matters that can be characterized as either insignificant or illegitimate.[269] Consequently, just like methods or mechanisms that can reveal no information at all, sense-enhancing technologies that can reveal only insignificant or illegitimate information, and nothing else, do not cross the Fourth Amendment threshold.[270]

---

[267] *Id.* at 123.

[268] Of course, the method must also be physically unintrusive in character. While *Katz* declared that a physical intrusion is not necessary for a Fourth Amendment search, physical intrusions into concealed spaces ordinarily engender sufficient risks of revealing significant, legitimate information to qualify as searches.

[269] Because the rationales for the Court's conclusions in *Place* and *Jacobsen* are not explained, the scope of the "insignificant" information category is unclear. It is possible that only the fact of nonpossession of *contraband* is sufficiently insignificant. On the other hand, nonpossession of *any item* may be too unimportant a fact to merit protection. Even a middleground is possible–i.e., nonpossession of some, but not all, items other than contraband could qualify as insignificant information.

[270] This reasoning has been applied by the Supreme Court only in contexts outside the home. The Court has shown enormous solicitude for in-home information, declaring that "in the home, . . . *all* details are intimate details" protected by the Fourth Amendment. Kyllo v. United States, 533 U.S. 27, 37 (2001); *see infra* notes 283-302 and accompanying text. It is uncertain whether the reasoning of *Place* and *Jacobsen* would be extended to in-home settings. When that issue comes before the Court, it could apply the *Place/Jacobsen* reasoning to residences, concluding that it overstated the case in *Kyllo* when it asserted that *all* details about home interiors merit Fourth Amendment shelter. Whether contraband is or is not present in a dwelling could be characterized as

In my view, the variation on the informational content theme reflected in *Place* and *Jacobsen* is constitutionally suspect. The Court has declared the determination that one is not in possession of contraband to be of no significance–*i.e.*, that no one could or should care about a breach of confidentiality concerning that unimportant detail. The Court has declared the possession of contraband to be illegitimate information–*i.e.*, while a person might well care about keeping that fact confidential, society is unwilling to provide shelter. The assumption is that there can be no constitutionally protected secrecy interest in such facts because the Framers were only concerned with protecting significant, legitimate matters.

The Court's premises are questionable interpretations of the Fourth Amendment not because they reflect implausible choices between privacy and societal protection. It would be reasonable to strike the constitutional balance by deeming certain relatively unimportant facts–such as the nonpossession of contraband substances–to be outside the reach of privacy protection and by declaring others–like the possession of contraband–to be odious and undeserving of constitutional shelter. The position has an inherent logical appeal. A society that adopted such a scheme could gain in safety and security without suffering devastating

unprotected, nonintimate details about the home. *See, e.g.*, United States v. Lingenfelter, 997 F.2d 632, 638 (9th Cir. 1993) (dog sniff not a search because individual did not have a legitimate expectation of privacy in contraband stored in his warehouse; individual would not have a protected privacy interest in fact contraband was in his home); United States v. Vasquez, 909 F.2d 235, 238 (7th Cir. 1990) (canine sniff used to detect presence of contraband in garage does not compromise a legitimate expectation of privacy). On the other hand, the Court could decide that homes are different, that the privacy interests in dwellings are so exalted that even these otherwise unworthy bits of information are safeguarded. *See, e.g.*, United States v. Thomas, 757 F.2d 1359, 1366-67 (2nd Cir. 1985) (holding use of dog to detect contraband in apartment violated "legitimate expectation that the contents . . . would remain private"); State v. Ortiz, 600 N.W.2d 805, 817, 820 (Neb. 1999) (concluding that canine sniff in apartment building hallway was a search of an apartment because "the information gained . . . as to the existence of contraband inside the apartment emanated from inside the apartment" and because "the police [were] able to obtain information regarding the contents of a place that has traditionally been accorded a heightened expectation of privacy"); United States v. Dicesare, 765 F.2d 890, 902-03 (9th Cir. 1985)(Reinhardt, J., concurring) (asserting that dog sniff of interior of apartment did constitute a search).

If the limitation on Fourth Amendment scope developed in *Place* and *Jacobsen* is legitimate, I do not believe that a line should be drawn between homes and other contexts. If the facts that one possesses or does not possess contraband are undeserving of constitutional protection outside the home, they seem undeserving of protection within the home. As will be seen, however, I have serious doubts about the validity of the "insignificant" or "illegitimate" information variation in *any* setting.

impoverishments of freedom and privacy. The question, however, is not whether that accommodation of the competing interests is plausible or reasonable. The relevant inquiry is whether that balance is the one struck in our Constitution.

The issue is complicated by the fact that those who designed our Constitution were unacquainted with dog sniffs, chemical field tests, or analogous means of investigation–*i.e.*, methods that could only reveal such limited information. It is possible that the Framers did strike the balance reflected in the Court's second variation on the informational content theme or, perhaps more to the point, that they would have struck that balance if they had known of investigative methods that could *only* breach the confidentiality of insignificant or illegitimate facts. If they had means of revealing only whether or not a person was involved in treason or seditious libel, it is conceivable that they would have permitted their unregulated use. Because I cannot exclude that possibility, I do not deem the Court's second variation to be clearly invalid.

Nonetheless, I am unpersuaded by the Court's interpretive choices. An individual may well value the privacy of and wish to keep confidential the fact that he is not in possession of contraband. Details about what a person is *not* doing provide information and insight into that person's life. It is not self-evident that the desire to keep such facts concealed and secret is undeserving of constitutional protection. The designers of the Constitution might well have decided that the people themselves are entitled to determine whether any information about their lives is significant enough to conceal. Moreover, an individual clearly has a strong, understandable interest in keeping private the fact of contraband possession. It would not have been unreasonable for the Framers to protect the freedom to maintain the confidentiality of such illegitimate details. The Fourth Amendment was adopted despite an awareness that the balance it struck between liberty and crime control–*i.e.*, the constraints imposed on official power to search–would afford breathing space for criminal conduct.[271] They might well have decided that a genuinely

[271] As the Court has acknowledged, while

> [c]rime, even in the privacy of one's own quarters, is . . . of grave

free society should provide privacy protection even for information about criminality.

The Court's conclusions to the contrary in *Place* and *Jacobsen* strike me as the purest form of *ipse dixit*. They derive no support from historical or other evidence suggesting that the Framers would have adhered to the view that there are classes of insignificant or illegitimate information that are unworthy. In neither *Place* nor *Jacobsen* did the Court explain the constitutional foundations for this second variation on the informational content theme. In the absence of logical support, one is left with a sense, if not a suspicion, that the Court's premises are rooted in mere speculation or in the Justices' own preferences rather than in the principles and values of the Framers.[272]

In addition, the second variation on the informational content theme requires distinctions between significant and insignificant and between legitimate and illegitimate facts.[273]

> concern to society, . . . [t]he right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance.

Johnson v. United States, 333 U.S. 10, 14 (1948); *see also* Arizona v. Hicks, 480 U.S. 321, 329 (1987) (stating that "there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all").

[272] *Cf.* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (observing that the expectations of privacy that society is prepared to recognize as reasonable "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable" and asserting that the Fourth Amendment does not "leave it to this Court to determine which . . . manifestations of the value of privacy `society is prepared to recognize as "reasonable"'") (quoting *Katz v. United States*, 389 U.S. at 361 (Harlan, J., concurring)).

[273] Distinctions based on the significance or legitimacy of information could lead to a potentially very slippery slope. So far, the Court has not extended the second variation on the informational content theme to encompass other information within the insignificant or illegitimate categories. In no case since *Place* and *Jacobsen* has it deemed another type of fact to be either insignificant or illegitimate. The explanation may be that no other means of investigation having such limited revelatory potential have appeared. When the occasion presents itself, perhaps we will learn that there are other bits of information about our lives–details about what we are doing or not doing–that simply do not deserve and are not entitled to privacy protection. The danger of such distinctions is illustrated by lower court opinions that have found additional kinds of information to be unworthy of constitutional shelter. *See, e.g.*, United States v. 15324 County Highway E, 219 F.3d 602, 604 (7th Cir. 2000) (basing conclusion that thermal imaging of home was not a search on fact that "heat emanations" from the home "were more like . . . the scent of drugs dogs can detect in luggage"); United States v. Robinson, 62 F.3d 1325, 1330 (11th Cir. 1995) (deciding that thermal imaging of dwelling was not a search because there was "[n]o revelation of intimate, even definitive, detail," but "merely a gross, nondiscrete bright image" and because "infrared surveillance . . . is analogous to the . . . [use] of drug-detecting dogs to locate contraband"); LaFollette v.

There are no readily apparent, constitutionally defensible criteria for deciding which details are sufficiently insignificant or illegitimate to be beyond the reach of Fourth Amendment shelter. We have no evidence that the Framers regarded certain facts as too unimportant or too unsavory to safeguard. Attempts to discern such lines can only be based on conjecture or our own views regarding the type of information that should or should not be entitled to privacy. I can find no persuasive basis for declaring the nonpossession of illicit substances to be "insignificant" while deeming the presence or absence of a can of chemicals in one's home to be a "critical" fact[274] or deciding that the relative warmth of one's home is an "intimate" detail.[275] Similarly, it is not self-evident why the possession of contraband is a constitutionally illegitimate detail while the possession of a "precursor" chemical used to manufacture contraband is a legitimate and protected fact.[276] The lack of constitutionally defensible criteria for making such decisions is further reason to reject the distinctions adopted by the Court.[277]

Commonwealth, 915 S.W.2d 747, 749 (Ky. 1996) (holding thermal imaging of residence not to be a search in part because "[u]nlike telephone taps or electronic devices that penetrate the walls of a home, heat waste does not disclose any fact intimate or personal about the occupant").

[274] In *United States v. Karo*, 468 U.S. 705, 715 (1984), the Court did deem that fact to be "critical" and deserving of protection. The Court indicated that if a beeper were to discern that a can of chemicals no longer remained in a house, it would breach an interest in privacy that merited protection. *Karo*, 468 U.S. at 715 (noting that subsequent monitoring of a beeper attached to an item that has been seen entering a home "not only verifies" the visual observations "but also establishes that the article remains on the premises"); *id.* at 716 (reasoning that beeper monitoring is constitutionally regulated because it allows the government "to determine . . . *whether* a particular article–or person, for that matter–is in an individual's home at a particular time") (emphasis added). The absence of such an object in one's home seems quite similar to the absence of contraband in one's luggage. As will be seen, I do not mean to cast any doubt upon the *Karo* Court's conclusion. I believe that it reflects a preferable interpretation of the Fourth Amendment's threshold.

[275] In *Kyllo*, the Court deemed this fact and all other facts about the home–including information about the character of the rug in one's entryway–to be "intimate" and deserving of protection. 533 U.S. at 37-38.

[276] In *Karo*, the government's use of a beeper to determine whether a can of precursor chemicals was in a home was deemed a search because that action could reveal the presence or absence of the can. 468 U.S. at 715.

[277] There is a similarity between the reasoning in *Place* and *Jacobsen* and the reasoning employed in *Oliver v. United States*, 466 U.S. 170 (1984), to support the conclusion that "open fields" are entitled to no Fourth Amendment shelter. *Oliver*, 466 U.S. at 177. The Court asserted that the activities that occur in open fields were not of a character to merit constitutional privacy protection. *Id.* at

I start from the premise that the Fourth Amendment bestows a right to choose which facts we wish to keep secret and that all facts we take adequate steps to conceal have legitimate claims to constitutional shelter.[278] Without evidence that the Framers held a different view, the declaration that some matters do not deserve protection seems presumptuous, speculative, and unprincipled.[279] I would assume that the Constitution grants an unlimited right to maintain the privacy of all information about our lives. Those who assert that there are constitutional limitations on the nature or content of the information we are entitled to keep confidential have not proven their case.

At the time the Constitution was adopted, the only means of learning whether a person was or was not in possession of contraband would have been by physical intrusions triggering Fourth Amendment scrutiny.[280] Scientific progress has afforded means of breaching the confidentiality of that same information without physical

178-79. While I do not necessarily agree with that assertion, the Court offered both textual and historical bases for believing that the Framers had decided to put information about matters occurring in privately-owned open fields beyond the protection of the Fourth Amendment. *See id.* at 176-81 (observing that the text of the Constitution does not mention open fields and relying upon the common law distinction between curtilage, which was protected, and open fields, which were not).

[278] This does not mean that the facts deemed insignificant or illegitimate by the Court are immune from government acquisition. It merely means that the use of technological methods to uncover those facts is subject to the same constitutional constraints as nontechnological means.

[279] Put simply, the conclusion that some information about our lives falls outside the sphere of Fourth Amendment protection has no apparent foundation in the text, history, experience, or values that should inform interpretations of that provision. *Cf.* United States v. Rabinowitz, 339 U.S. 56, 83 (1950) (Frankfurter, J., dissenting) (the determination of whether a search is reasonable requires "some criteria of reason" such as "the history or experience which [the Fourth Amendment] embodies and the safeguards afforded by it against the evils to which it was a response").

[280] Actually, a distinction between dog sniffs and field tests may well be in order. A canine sniff of luggage reveals some information that only a physical intrusion into luggage could have revealed in an earlier time. A field test, however, discloses effectively concealed information–the identity or nonidentity of the substance–that could not have been disclosed even by means of physical intrusion. The substance would have to have been "tested" in some manner to ascertain its identity. If there were a means of identifying what the substance was or was not that would not have triggered Fourth Amendment coverage, then a field test that reveals that same information should not be deemed a search. The reason for that conclusion, however, would not be that the information revealed was too insignificant or illegitimate. Rather, the reason would be that the field test merely uncovered information that would have been accessible to human senses at the time the Fourth Amendment was adopted without an intrusion governed by that provision. Put otherwise, the field test developed by science would not threaten diminution of the domain of privacy originally provided.

intrusion. Because the confidentiality of the details at issue would have been protected in an earlier time and because there is no evidence that those who drafted the Fourth Amendment did not value the entitlement to keep them secret, I would not declare those details to be constitutional pariahs. I would reject the second variation on the informational content theme, holding that exploitations of scientific advances to reveal *any* concealed, otherwise inaccessible information are within the purview of Fourth Amendment control.[281]

c. The Third Variation: Official Conduct that Reveals Any Information About the Home

The third variation on the informational content theme has provided significant support for the holdings in the only two post-*Katz* cases in which the Court has concluded that official uses of technological devices crossed the Fourth Amendment's threshold. In *United States v. Karo*,[282] the Court held that government agents conducted a search when they used an electronic monitoring device, a beeper, to locate a can of chemicals inside private residences.[283] The beeper twice enabled the agents to ascertain that the can had remained inside a particular home.[284] After setting forth the elementary propositions that expectations of privacy in homes are reasonable and that physical intrusions into dwellings violate those expectations and constitute searches,

[281] A device or method that can breach the confidentiality of any facts that could have been learned only by a physical intrusion when the Constitution was adopted is an effective surrogate for the conduct that the Framers subjected to a reasonableness requirement. If the novel investigatory means reveals only certain, limited sorts of information, the threat to confidentiality may well be less severe than the threat posed by physical intrusion. The difference, however, seems to be a difference in degree, not in kind. Over 115 years ago, in *Boyd v. United States*, 116 U.S. 616 (1886), the Court warned about "illegitimate and unconstitutional practices that get their first footing . . . by silent approaches and slight deviations from legal modes" and about "stealthy encroachments." *Boyd*, 116 U.S. at 635. The Court declared that judges must "liberally construe[]" the Fourth Amendment, avoiding interpretations that "lead[] to gradual depreciation of the right." *Id.* This wisdom and admonition seem most apposite in this context. Although the deviation reflected in *Place* and *Jacobsen* may be "slight," it is the sort of "stealthy encroachment[]" upon Fourth Amendment reach that diminishes and can lead to further "depreciation" of the privacy protected by that provision.

[282] 468 U.S. 705 (1984).

[283] *Karo*, 468 U.S. at 715.

[284] *Id.*

the Court declared that the same result had to follow when officials use "an electronic device to obtain information [they] could not have [otherwise] obtained by observation from outside the curtilage of the house."[285] While the Court acknowledged that electronic surveillance like the beeper monitoring in *Karo* is "less intrusive" than a physical entry,[286] it rejected the assertion that the result was "only a minuscule intrusion on protected privacy interests" in the home.[287] Instead, because the beeper monitoring "reveal[ed] *a critical fact about the interior of the premises*,"[288] it crossed the border of Fourth Amendment territory.

In *Kyllo*, an officer scanned an Oregon dwelling with a thermal imager, a mechanism that could detect the relative amount of infrared radiation emanating from the home. The device showed certain areas of the home to be warmer than others and revealed that the dwelling as a whole was warmer than neighboring homes. The question was whether this exploitation of technology had crossed the Fourth Amendment's threshold. Justice Scalia observed that while it had been difficult to apply the *Katz* reasonable expectation of privacy doctrine in some situations, in the home interior context "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[289] To guard against such technological erosion, the Court decided that the authorities trigger Fourth Amendment scrutiny whenever they use "sense-enhancing technology" that "is not in general public use" to obtain "*any information regarding the interior of the home* that could not otherwise have been obtained without physical `intrusion into a constitutionally protected area.'"[290] Because the use of a thermal imager on a residence satisfied this standard, it was deemed a search.

In *Karo*, the government had argued that because the

---

[285] *Id*.

[286] *Id*. This conclusion is apparently based on the fact that beeper monitoring from outside a dwelling without physical intrusion into the interior by a percipient human being leaves much of the privacy of the dwelling intact insofar as it does not breach the confidentiality of any other details sheltered by the home. Moreover, there is no threat to interests in quiet repose within the dwelling.

[287] *Id*. at 717.

[288] *Id*. at 715 (emphasis added).

[289] *Kyllo*, 533 U.S. at 34.

[290] *Id*. (emphasis added).

beeper discloses merely that an object is located in a home, its use "constitutes only a minuscule intrusion on protected privacy interests."[291] The Court strongly disagreed, responding that the danger to home privacy was significant because the location of an object within a home was "a critical fact about the interior of the premises."[292] In *Kyllo*, the government had asserted that thermal imaging did "not `detect private activities occurring in private places'" or "reveal any `intimate details.'"[293] The argument was essentially that the information that could be secured by the exploitation of the device–the relative amount of heat emanating from in-home activities–was insignificant and undeserving of constitutional protection. The majority categorically repudiated this contention, announcing that "protection of the home has never been tied to measurement of the quality or the quantity of information obtained," because "[i]n the home, . . . *all* details are intimate details."[294]

The Court's message seems clear. There is no informational content limitation on the protection afforded confidentiality in private dwellings.[295] At least in home settings, the nature or amount of confidential information that can be revealed by a technological tool is irrelevant.[296] There is neither a qualitative "intimacy" standard nor a quantitative "substantiality" standard that needs be met. *All* information, *every* fact, *every* detail is critical, intimate and entitled to the privacy protection afforded by the Fourth

---

[291] *Karo*, 468 U.S. at 717.

[292] *Id.* at 715.

[293] *Kyllo*, 533 U.S. at 37. The lower court opinion in *Kyllo* provided support for the government's contention. *See* United States v. Kyllo, 190 F.3d 1041, 1047 (9th Cir. 1999) ("The thermal emission scan performed on Kyllo's residence . . . did not expose any intimate details of Kyllo's life.").

[294] *Kyllo*, 533 U.S. at 37.

[295] In my view, *Karo* and *Kyllo* wholly undercut the suggestion in *Smith v. Maryland* that the fact that a pen register could only capture numbers dialed, not words spoken, supported the conclusion that no reasonable expectation of privacy was violated. *See Smith*, 442 U.S. at 744. Under the principle of *Karo* and *Kyllo*, the numbers dialed from a home telephone are critical and intimate facts about the home interior that merit Fourth Amendment protection. A device that could sense those numbers would be governed by the Fourth Amendment unless, as in *Smith*, there were other reasons to conclude that acquisition of the numbers was not a deprivation of privacy.

[296] As mentioned earlier, it remains possible that the fact that contraband is not or is present in a home *may* be an exception to this otherwise broad protection for home informational privacy. *See supra* note 204 and accompanying text.

Amendment.[297]

The Court's staunch refusal to distinguish between substantial and insubstantial and between intimate and nonintimate information has found expression only in cases involving home interiors. The critical importance of the home context to the conclusions reached in *Karo* and *Kyllo* is unmistakable.[298] It is uncertain whether these two opinions reflect a broader principle that governs technological intrusions in other private spheres–persons, inanimate possessions, offices and vehicles, for example.[299] In my view, the governing principle is eminently sound and consistent

[297] It is possible, however, that the amount or nature of the information disclosed by a particular technological tool could support the conclusion that technological intrusion would be reasonable on less than the showing needed to justify physical intrusion into a home. In *Karo*, the Court intimated that reasonable suspicion might be enough to justify in-home beeper monitoring. 468 U.S. at 715 n.5. The *Kyllo* opinion contained no similar intimation, but the possibility that thermal imaging on less than probable cause would be reasonable cannot be ruled out. Because my concern is with the questions of whether and when the Fourth Amendment provides any protection against particular technologies, I do not discuss the issue of diminished standards of reasonableness. A conclusion that lesser showings suffice because the threats to privacy are less severe is arguably consistent with the balancing analysis reflected in some of the Court's precedents. *See e.g.*, New Jersey v. T.L.O., 469 U.S. 325 (1985) (holding that standard for reasonableness of school searches is less than probable cause in part because of lesser threats to privacy); Terry v. Ohio, 392 U.S. 1 (1968) (holding that a frisk is reasonable on less than probable cause in part because the intrusion on privacy is less than that involved in a full-scale search). That conclusion is arguably inconsistent with the Court's unwillingness to endorse lower standards in other cases. *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366 (1993) (concluding that tactile manipulation of object in suspect's pocket for evidentiary purposes constitutes a sufficient intrusion on privacy to require probable cause); Arizona v. Hicks, 480 U.S. 321 (1987) (deciding that movement of turntable to inspect the bottom is sufficient invasion of privacy to require probable cause).

[298] For a thorough discussion of the importance of the home as a locational factor in threshold analyses, see *infra* notes 367-85 and accompanying text.

[299] One trying to read the Court's sparse tea leaves can find indicators pointing in each direction. On one hand there is the suggestion in *Karo* that the monitoring of a beeper to learn the contents of a storage locker might constitute a search. *See* 468 U.S. at 721 n.6 (stating that defendants had a "reasonable expectation of privacy" within a rented storage locker and, consequently, that beeper monitoring disclosing whether a container was inside the locker would have been a search); *see also id.* at 733 & n.8 (Stevens, J., concurring and dissenting) (asserting that Fourth Amendment protection against indiscriminate monitoring of beepers "is not limited to times when [a] beeper [is] in a home" and concluding that the *Karo* majority "seems to acknowledge" the validity of that view "since it indicates that the location of property can be private even when not in a home"). On the other hand, the opinions in *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), and *Florida v. Riley*, 488 U.S. 445 (1989), indicate that the Court could adopt a different view in contexts outside the home. Among the relevant variables relied on to deny protection in *Dow* was the fact that the aerial mapping camera did not disclose *intimate* information about the commercial curtilage. 476 U.S. at 238. And the plurality opinion in *Riley* cited the lack of *intimacy* of the facts learned in reaching the conclusion that the surveillance of residential curtilage was not a search. 488 U.S. at 452.

with a proper understanding of Fourth Amendment objectives. It ought to be generalized and extended to every setting in which reasonable privacy expectations exist. If a technological tool is capable of revealing concealed details and is exploited in ways that enable the perception of those otherwise inaccessible details, the substantiality or intimacy of the matters perceived should not affect the determination of whether the Fourth Amendment threshold has been crossed.

In *Kyllo*, Justice Scalia indicated that there was no constitutionally defensible basis for concluding that some in-home facts are unworthy of protection.[300] I am aware of no basis for believing that the Framers intended substantiality or intimacy limitations on the details that we are entitled to keep confidential in other arenas. Justice Scalia also relied in part on the "impracticality" of a distinction based on the quality or quantity of information that is or could be secured.[301] Impracticality also counsels strongly against efforts to determine which facts in other private domains are sufficiently substantial or private to merit protection. There are no ready criteria to guide such judicial determinations, at least none with roots in the Constitution. Efforts to draw and implement lines would be both unprincipled and costly.

In sum, absent a showing of some reason to believe that the Framers would have been unconcerned with physical searches that uncovered only certain amounts or kinds of information, we should not impose such an informational content limitation on Fourth Amendment coverage in threshold technology cases. Technological devices should not be deemed outside the reach of the Fourth Amendment based on judgments about the quantity or quality of the information they can or do disclose.

The content of the information that can be acquired by a technological device can be relevant to deciding whether the Fourth Amendment's threshold has been crossed. Confidentiality is not threatened by the government's use of

[300] 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained.").

[301] *Id.* at 38 ("Limiting the prohibition of thermal imaging to `intimate details' would not only be wrong in principle; it would be impractical in application, failing to provide `a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'") (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).

a scientific method or technological mechanism with absolutely no revelatory potential. However, when a device or technique does expand human perceptive or acquisitive capacities in ways that enable the authorities to access information that is otherwise imperceptible because it is effectively concealed in private spheres, the Fourth Amendment should be applicable. The notion of informational content provides a solid foundation for a singular, bright line of division between exploitations of technology that pose no threat to informational privacy at all and those that threaten to uncover otherwise confidential information about a person's life. In the absence of evidence that other distinctions were contemplated by the Framers, I advocate a simple, practical dichotomy between those innovations that can reveal nothing at all and those with the potential to uncover *any* confidential details that would otherwise be inaccessible. While less expedient and more restrictive of law enforcement than the current doctrine, this bright line seems more principled than one that calls upon the judiciary to divine which details about our lives are worthy and which are unworthy of constitutional shelter.

3. The "Nature and Character of the Technology" Variables

The third category of relevant variables in threshold technology opinions is the "nature and character of the technology." Each factor included here pertains to some aspect of the device or mechanism exploited by the government. Once again, there are three variations on the general theme: sophistication versus conventionality and the magnitude of sense enhancement, general availability to the public and general public use. The first two have been influential, but never determinative in threshold decisions, while the third variation has dictated the resolution of threshold issues.

a. The First Variation: Sophistication Versus Conventionality and the Magnitude of Sense Enhancement

Whether a technological tool is sophisticated or unique rather than conventional or ordinary and the extent to which it augments ordinary human capabilities have been influential considerations in threshold cases. Neither variable has been decisive, and the amount of weight to be accorded to each is uncertain.

The situation in *Dow Chemical Company v. United*

States[302] involved two different technological enhancements of human faculties. Officials employed both an aircraft and "a standard floor-mounted, precision aerial mapping camera"[303] to take pictures of commercial curtilage from navigable airspace. The Court found that this conduct did not constitute a search, basing that conclusion on a unique combination of several variables.[304] According to the majority, the use of the camera did not violate a reasonable expectation of privacy in part because it was a "conventional, albeit precise, commercial camera commonly used in mapmaking."[305] Officials had not used "unique sensory device[s]" or "highly sophisticated surveillance equipment."[306] Moreover, the photographs taken by the camera were "not so revealing of intimate details as to raise constitutional concerns."[307] Although the camera did enhance vision "somewhat" and provided "more detailed information than naked-eye views"[308] could have furnished, the surveillance did not involve electronic devices that "penetrate[d] the walls of buildings and record[ed] conversations" or photographic equipment that had the capacity to reveal "intimate details."[309] In sum, the "conventional" character of the camera and the relatively limited degree to which it increased ordinary human abilities to perceive otherwise inaccessible information contributed to the conclusion that the Fourth Amendment threshold was not crossed.[310] Thus, devices that are not

[302] 476 U.S. 227 (1986).

[303] *Dow Chem. Co.*, 476 U.S. at 229.

[304] *Id.* at 239. As will be seen, in addition to the conventionality and relatively small amount of sense enhancement, the Court relied on the general public availability of the camera and on the commercial curtilage character of the location surveilled.

[305] *Id.* at 238.

[306] *Id.*

[307] *Id.*

[308] *Id.*

[309] *Id.*

[310] *Id.* The Court asserted that "[t]he mere fact that human vision is enhanced *somewhat, at least to the degree here*, does not give rise to constitutional problems." *Id.* (emphasis added). The Court minimized the fact that "under magnification power lines as small as 1/2-inch in diameter [could] be observed" in the pictures that were taken in *Dow*. *Id.* at 238 n.5. The majority explained that these power lines could be seen "only because of their stark contrast with the snow-white background" and proceeded to point out that "[n]o objects as small as ½-inch in diameter such as a class ring, for example, are recognizable, nor are there any identifiable human faces or secret documents captured in such a fashion as to implicate more serious privacy concerns." *Id.*

sophisticated or unique and not capable of dramatic or substantial sense enhancement are less likely to cross the Fourth Amendment border.[311]

On the other hand, in *Kyllo v. United States*,[312] the Court's most recent word on the relationship between technology and the Fourth Amendment, the majority reasoned that the "relatively crude"[313] character of the thermal imager used and the fact that it did not and could reveal particularly intimate details could not be decisive because "the rule [that the Court] adopt[ed had to] take account of more sophisticated systems that are already in use or development"[314] and because in the home "*all* details are intimate details."[315] While *Kyllo* is not irreconcilable with *Dow*,[316] it suggests potential ambivalence about the relevance of the sophistication and extent of enhancement variables, raising questions and doubts about the influence they ought to have in threshold technology analysis.

In my view, the *Kyllo* majority's reluctance to tie the threshold determination to the lack of sophistication of the thermal imager or to the magnitude of augmentation of ordinary perception is a positive development. The Court has proffered no explanation for reliance on these attributes, and I perceive no logical constitutional premises that sustains the decision to accord them any influence. There is

---

[311] The Court's opinion in *United States v. Knotts*, 460 U.S. 276 (1983), arguably provides additional support for the relevance of these attributes of the technology at issue. In dictum, the Court indicated that the use of a "searchlight" or "field glass" to see what could not otherwise be seen by human eyes would not trigger Fourth Amendment scrutiny. *Id.* at 283 (quoting United States v. Lee, 274 U.S. 559, 563 (1927)); *see also* Texas v. Brown, 460 U.S. 730, 740 (1983) (asserting that the use of a flashlight to enable an officer to see the contents of a vehicle "trenched upon no right secured . . . by the Fourth Amendment," and concluding that "the use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection"). While neither the *Knotts* nor the *Lee* Court explained the rationale for this conclusion, one plausible explanation is that the devices referred to are conventional and do not dramatically enhance human perceptive capacities. In fact, they seem less sophisticated or unique and less expansive of human perceptive powers than the aerial mapping camera used in *Dow*.

[312] 533 U.S. 27 (2001).

[313] *Kyllo*, 533 U.S. at 36.

[314] *Id.*

[315] *Id.* at 37.

[316] *Kyllo* did not hold that the two considerations were irrelevant, but only that they could not support a different threshold conclusion for thermal imaging of private homes. *Dow* simply accorded the variables some influence in a situation involving aerial photography of commercial curtilage. *Kyllo* could mean that sophistication and magnitude of enhancement are irrelevant in home interior contexts. Alternatively, it could mean that while those factors deserve some influence, they are insufficiently weighty to tip the balance in home interior cases.

no apparent reason that the reach of the Fourth Amendment should hinge on whether a device is complicated or esoteric or on whether it increases perceptive and acquisitive powers substantially or modestly. If a tool unknown to the Framers provides additional access to *any* confidential details that could not have been sensed by unregulated means at the time the Constitution was framed, exploitation of that tool jeopardizes cognizable interests in informational privacy. The failure to subject such a scientific or technological development to the Fourth Amendment's reasonableness regime can only result in shrinkage of the privacy sought to be preserved by the Framers. If a device enables the authorities to gain *any* access that they would not have had at the time the Constitution was framed–at least not without intrusions that would have been regulated–its use should be governed by the Fourth Amendment. The result of making threshold determinations dependent on these is superficially appealing, but logically indefensible, criteria is infidelity to the aims of those whose wisdom protected us against unreasonable searches.[317]

I understand that the absolute, bright-line approach proposed could meet resistance. The notion that the use of a searchlight, flashlight, pair of binoculars or ordinary telephoto camera lens to perceive otherwise imperceptible details could qualify as a search might seem contrary to common sense and reflective of an excessively indulgent interpretation of the Fourth Amendment. I admit that intuition and instinct push me toward the contrary conclusion.[318] Nonetheless, I prefer the conclusions yielded

[317] Less sophisticated, more ordinary mechanisms that increase human abilities less substantially may well result in more limited losses of privacy. There is no basis, however, for concluding that the Fourth Amendment is entirely unconcerned with relatively small deprivations of privacy. If the amount of sense enhancement a device is afforded was truly negligible, perhaps the danger to privacy could be insufficient to trigger constitutional protection. I would reserve such an exception, however, for the rarest of *de minimis* cases. In any case in which the technological enhancement results in a measurable infringement on confidentiality it should be deemed a search and subjected to Fourth Amendment regulation. That is not to say that the showing necessary to render such a search reasonable might not properly depend on the magnitude of the privacy deprivation. *See supra* note 298 and accompanying text (discussion of the same possibility in connection with *Karo*).

[318] On the other hand, practicality provides substantial support for my conclusions. Not only are the sophistication versus conventionality and magnitude of enhancement variables theoretically unjustified, they require difficult distinctions between those devices that are sufficiently sophisticated or

by reason, logic, and adherence to the privacy protective goals of the Framers. Proponents of this variation on the nature and character of the technology theme must furnish persuasive constitutional justifications for allowing the conventionality and degree of enhancement to inform threshold inquiries. In the absence of such justifications, these variables should be declared irrelevant to threshold technology analysis.[319]

b. The Second Variation: The General Public Availability of a Technological Device

The majority opinion in *Dow* also relied on the premise that the aerial mapping camera used was "generally available to the public."[320] The implication is that the fact that a device is generally available to–that is, can be readily acquired by–members of the public militates against a conclusion that its use by the government to enhance the perception and acquisition of otherwise confidential information constitutes a search. How available a device must be to have such influence is entirely uncertain.[321]

The fact that members of the public *could* readily gain possession of a mechanism is not a reason for declaring its exploitation outside the realm of constitutional concern. The *Dow* Court offered no defense for according this variable any weight, and again I can discern no constitutionally logical

unique and those that instead are conventional and between a degree of enhancement that militates in favor of constitutional control and an extent of enhancement that counsels against regulation. There are no ready analytical standards for making these difficult decisions.

[319] As is evident, I categorically reject the notion that small privacy deprivations at the hands of technology are somehow acceptable or tolerable. As the *Boyd* Court recognized over a century ago, "the obnoxious thing in its mildest and least repulsive form" is still "the obnoxious thing." Boyd v. United States, 116 U.S. 616, 635 (1886). Reliance on these variables to find technological exploitation beyond Fourth Amendment reach permits "illegitimate and unconstitutional practices [to] get their first footing . . . by silent approaches and slight deviations from legal modes of procedure." *Boyd*, 116 U.S. at 635. The way to avoid that undesirable consequence is to "liberally construe[]" the vital Fourth Amendment safeguards, remaining ever "watchful" against "stealthy encroachments" upon "the constitutional rights of the citizen." *Id.* Although the *Boyd* Court's references to "silent approaches," "slight deviations," and "stealthy encroachments" were not aimed at technological threats, they seem eminently pertinent. They stand as admonitions against the conventionality and relatively small capacity for sense enhancement variables.

[320] *Dow Chem. Co.*, 476 U.S. at 238.

[321] Again, the notion of "general public availability" could be the basis for the *Knotts* Court's dictum that uses of searchlights and field glasses would not be governed by the Fourth Amendment. *See supra* note 312 and accompanying text. These tools might have been deemed beyond the reach of the Constitution because they can be acquired by the general public with relative ease.

foundation for reliance on mere availability alone, no matter how "general" it may be. The fact that members of the public *could* or *might* acquire a particular tool and *could* or *might* use it to access otherwise inaccessible, confidential information about individuals' lives does not bear upon, much less undermine, the legitimacy of the interest in preserving the secrecy of that information. Availability alone does not have a cognizable impact on the confidentiality of the facts that the device could empower actual possessors to perceive.[322]

When the government uses a sense-augmenting tool to perceive and learn details that would otherwise be inaccessible, it deprives individuals of genuine privacy interests that existed when the Fourth Amendment was adopted and have remained intact in modern times. The same conclusion follows whether the particular technology is unavailable, narrowly available, or generally available to members of the public. Absent some explanation of how the public availability variation on the nature and character of the technology theme is consistent with the objectives of the Framers, the Court should deem it inapposite to threshold technology determinations.[323]

c. The Third Variation: "General Public Use" of a Technological Device

A much more influential and intriguing variable within this category, one that has proven decisive in controversial threshold technology cases, is whether a particular device is in "general public use."[324] Alternatively, this factor has been

[322] As will be seen, I reach a different conclusion with regard to actual "general public use" of a technological tool because of the potential impacts that factor has on the scope of legitimate privacy expectations in contemporary society.

[323] The role and weight of the general public availability factor in *Dow* is indeterminate. The conclusion that use of the aerial mapping camera did not constitute a search rested on the conventionality of the camera, the relatively limited expansion of human perception, the general availability to the public, *and* the lesser privacy expectations associated with the area photographed. Without close analysis, this combination of factors might seem to provide substantial support for the Court's threshold conclusion. When examined carefully, however, it becomes apparent that most, if not all of these factors are logically irrelevant to threshold analysis. Together, they do not furnish a solid foundation for the decision that the use of the camera was not subject to constitutional regulation.

[324] The phrase "general public use" was adopted by the Court in *Kyllo v.*

described as whether public use of the technology is "routine,"[325] is "sufficiently rare,"[326] or occurs "with sufficient regularity."[327] When tools that enhance ordinary human abilities to perceive and acquire information that would otherwise remain confidential are generally or routinely used by the public, official exploitations of those tools do not cross the Fourth Amendment threshold.[328] If properly understood and applied, this variable is a potentially defensible determinant of whether technological exploitation constitutes a search. The Supreme Court, however, has misapplied the criterion, according it decisive influence in situations where the logical prerequisites for finding general public use were not present.

During the 1980s, the Supreme Court twice addressed aerial surveillance of residential property.[329] In the first and most significant of the cases, *California v. Ciraolo*,[330] officers flew over the defendant's backyard at the legally navigable altitude of 1000 feet, and, with their naked eyes, spied marijuana growing there. In *Florida v. Riley*,[331] a police officer hovered in a helicopter over a greenhouse at the lawful altitude of 400 feet, and by unaided vision was able to see what he believed to be marijuana. Both property owners claimed that the aerial surveillance was a "search" because it had intruded upon reasonable expectations of privacy in the areas surrounding their homes. The Supreme Court rejected these claims, finding the surveillance to be constitutionally

---

United States, 533 U.S. 27, 40 (2001).

[325] California v. Ciraolo, 476 U.S. 207, 215 (1986) (relying on fact that we live "[i]n an age where private and commercial flight in the public airways is routine").

[326] Florida v. Riley, 488 U.S. 445, 451 (1988) (observing that there was "nothing in the record or before us to suggest that helicopters flying at 400 feet are sufficiently rare in this country").

[327] *Riley*, 488 U.S. at 454 (O'Connor, J., concurring in the judgment) (stating that "the relevant inquiry" is "whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity").

[328] The *Kyllo* majority traced the "general public use" doctrine to "the Court's precedent," citing *California v. Ciraolo*, 476 U.S. 207, 215 (1986), as the source. *Kyllo*, 533 U.S. at 39-40 n.6. Although the majority indicated that it might be willing "to reexamine that factor" in an appropriate future case, *id.*, for the present, it retained the "general public use" limitation on the reach of the Fourth Amendment.

[329] In *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), the Court addressed aerial surveillance of commercial property. The holding in *Dow* regarding the government's use of an airplane to gain access to otherwise inaccessible information, *Dow Chem. Co.*, 476 U.S. at 239, also reflects the decisive nature of the "general public use" criterion. There is no reason, however, to discuss the *Dow* opinion here because it adds nothing to the analyses in *Ciraolo* and *Riley*.

[330] 476 U.S. 207 (1986).

[331] 488 U.S. 445 (1989).

unconstrained.

Ciraolo laid an analytical foundation that rested first on a very significant declaration in *Katz* concerning homes, privacy and public exposure. While rejecting the physical intrusion requirement and adopting privacy as the guide to Fourth Amendment scope, the *Katz* majority had conceded 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."[332] This concession was merely a recognition that informational privacy–the core Fourth Amendment value–is not threatened when an officer, from a legal, public vantage point, uses unaided senses to observe unconcealed facts about a home or other constitutionally protected location. The choice to expose activities to public view contradicts the reasonableness of any claim of confidentiality. Knowing exposure effectively "publicizes" the details, sacrificing the entitlement to secrecy the Constitution would otherwise provide. The *Ciraolo* Court deemed this logic relevant to naked eye aerial surveillance from lawfully navigable airspace. Because the flying public "could have [looked down and] seen everything that the[] officers observed" in Ciraolo's back yard, the officers could do so without crossing the Fourth Amendment threshold.[333] Whether observations are made horizontally from a public sidewalk or vertically from public airspace is of no importance. In either case, there is no deprivation or violation of privacy, but merely capitalization on the person's choice to forfeit confidentiality.

Four dissenters had no dispute with the majority's reasoning when applied to observations of residential property made from ground-level. In their view, observations made from aircraft are a wholly different constitutional animal. Airplanes, a product of technological innovation, afford access to information that was not available when the Bill of Rights was adopted. According to the dissenters, naked-eye aerial observations from the previously unattainable vantage points afforded by aircraft violate reasonable privacy expectations and must be subjected to Fourth Amendment constraints.[334] The contrary conclusion

[332] Katz v. United States, 389 U.S. 347, 351 (1967).
[333] *Ciraolo*, 476 U.S. at 213-14.
[334] *See id*. at 224-25 (Powell, J., dissenting) (concluding that the "aerial

ignores the central lesson of *Katz* and Justice Harlan's warning that technological developments would enable the circumvention and erosion of Fourth Amendment protection if the threshold doctrine did not evolve to meet the challenges posed.[335]

The majority's response to the dissent's powerful arguments was that its holding was fully reconcilable with the spirit of *Katz* and with Justice Harlan's concerns. The primary reason why the particular exploitation of technology in *Ciraolo*–use of an aircraft to occupy lawful airspace–did not threaten to undermine the privacy guaranteed by the Fourth Amendment was that "private and commercial flight in the public airways is routine."[336] The authorities do not deprive homedwellers of privacy when they exploit aircraft to gain access to information about homes and curtilage because the public uses the very same technology to occupy the same previously unattainable vantage point.[337]

---

surveillance undertaken by the police . . . constituted a `search'" and was subject to the warrant requirement because it violated the "reasonable expectation of privacy in [the homeowner's] yard").

[335] *Id.* at 215-16, 218 (arguing that the majority "today ignores" Justice Harlan's warning in *Katz* and fails to furnish adequate "protection against surveillance techniques made possible through technology"); *id.* at 222-23 (maintaining that the Court's holding authorizes the police to "use an airplane–a product of modern technology–to intrude visually into [a] yard," a result that is inconsistent with the spirit of *Katz* and insufficiently protective of the "constitutionally protected privacy right" at the core of the Fourth Amendment).

[336] *Ciraolo*, 476 U.S. at 215. The majority also replied that Justice Harlan had been concerned with "future electronic developments and the potential for electronic interference with private communications," not with "simple visual observations from a public place." *Id.* at 214. This additional reason for finding the enhancement of human capacities afforded by aircraft not to be a matter of Fourth Amendment concern is of much less significance. *Ciraolo* is the only opinion to give it expression, and it was unnecessary to the resolution of the claim that use of the airplane crossed the Fourth Amendment threshold. On the merits, the suggestion that technological advantages that enhance access to otherwise confidential information are of less concern if they do not constitute electronic interference with private communications is lacking in logical support. There is, quite simply, no reason that nonelectronic technological advances are less threatening to privacy. Moreover, there is no reason that private communications should be granted special protection not available to other sources of information about our private lives.

[337] The Court did indicate that if aerial surveillance was conducted in a physically intrusive manner or if it was used in conjunction with other sense-enhancing technologies that could disclose concealed information about residential property, the Fourth Amendment would be applicable. *Id.* at 215 n.3 (quoting government's acknowledgment that "`[a]erial observation of curtilage may become invasive, either due to physical intrusiveness or through modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.'") (citations omitted). Like physical intrusion into the curtilage from ground level, it seems clear that physically intrusive aerial surveillance–an overflight that breached the upper border of the protected space surrounding a home–would cross the threshold of the Fourth Amendment.

In *Riley*, a plurality of the Court adhered to the basic logic of *Ciraolo*. The use of the helicopter to increase human abilities to observe matters occurring on constitutionally protected residential property did not cross the Fourth Amendment border because private and commercial helicopter flight in public airways was routine in the United States and was not "unheard of" in Riley's county.[338] There was no evidence that public flights at 400 feet, a lawful altitude for helicopters, were "sufficiently rare," and any member of the public in such an aircraft at that altitude "could have observed Riley's greenhouse."[339] Justice O'Connor, who provided the critical fifth vote for the holding in *Riley*, asserted that in determining whether the use of aircraft crosses the constitutional threshold it was critical to determine whether "members of the public travel" at a particular altitude "with sufficient regularity."[340] Only if a "vantage point [is] generally used by the public" is it fair to find knowing exposure and conclude that it is unreasonable to expect privacy against official surveillance from that vantage point.[341] Because there was "reason to believe that there [was] considerable public use of airspace at . . . 400 feet and above" and "no evidence to the contrary," Justice O'Connor agreed that the officer had not conducted a "search."[342]

Recently, in *Kyllo v. United States*,[343] the Court clarified the lessons that *Ciraolo* and *Riley* teach with regard to the relationship between technology and the Fourth Amendment. *Kyllo* held that the use of a thermal imager to detect heat emanations from a private home was a search. The Court announced that as a general rule the use of "sense-enhancing technology" to secure "any information regarding the interior of the home that could not otherwise have been obtained without physical `intrusion'" is a search if the technological device employed "is not in general public use."[344] Because the majority could "quite confidently say that thermal imaging [by the public] is not `routine,'" official

[338] *Riley*, 488 U.S. at 450.
[339] *Id.* at 451.
[340] *Id.* at 454 (O'Connor, J., concurring in the judgment).
[341] *Id.* at 455.
[342] *Id.*
[343] 533 U.S. 27 (2001).
[344] *Kyllo*, 533 U.S. at 34.

exploitation of the imager crossed the constitutional boundary.[345] The *Kyllo* majority explained that the "general public use" limitation on the standard for determining when technology is a matter of Fourth Amendment concern was the product of precedent–specifically, *California v. Ciraolo*.[346] Thus, the *Kyllo* Court explained and clarified a pivotal premise on which the threshold decisions in *Ciraolo* and *Riley* rested. In those cases, the exploitations of technology to afford access to otherwise confidential and inaccessible information about residential properties were not searches because airplanes and helicopters were technological advances that were "in general public use."[347]

The *Kyllo* Court recognized that scientific or technological enhancements of human abilities to sense and acquire previously inaccessible information imperil the vitality of Fourth Amendment privacy interests.[348] It also acknowledged that the use of aircraft to fly over residential property is an exploitation of technology that enables humans to observe and learn matters that could not be observed and learned in the late eighteenth century and that the consequence was a diminution of the privacy enjoyed at that time.[349] According to the Court, the aerial overflight

---

[345] *Id*. at 40 n.6.

[346] *Id*. The Court found no need to "reexamine" the limitation in *Kyllo* because of its confidence that thermal imagers were not in general public use. *Id*.

[347] The *Ciraolo* majority and *Riley* plurality had not used this doctrinal phrase. The opinions in those cases had observed that the public's use of aircraft to travel in navigable airspace was "routine," *Ciraolo*, 476 U.S. at 215; *Riley*, 488 U.S. at 450, and, alternatively, that it had not been shown to be "sufficiently rare." *Riley*, 488 U.S. at 451. The *Kyllo* majority believed that "general public use" was an accurate description of the basis upon which those opinions grounded the conclusions that the government's exploitations of technology did not trigger Fourth Amendment scrutiny. The Court also indicated that whether a device is in "general public use" and whether public use of a technological tool is "routine" are equivalent doctrinal inquiries. *See Kyllo*, 533 U.S. at 39-40 n.6 (declaring that use of thermal imagers by the public did not satisfy the *Ciraolo* exception because it was "not `routine'").

[348] *Kyllo*, 533 U.S. at 34 (warning that "[t]o withdraw protection" from the expectation of privacy in homes "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment" and asserting that the standard announced for evaluating whether technology crosses the constitutional threshold "assures preservation of that degree of privacy . . . that existed when the Fourth Amendment was adopted").

[349] *Id*. (stating that "the technology enabling human flight has exposed to public view (and hence . . . to official observation) uncovered portions of the house and its curtilage that once were private"). There can be little doubt that modern day descendants of Orville and Wilbur Wright's invention have bestowed upon humankind the ability to perceive matters that they could not have perceived when the Constitution was formulated except by means that would have been regulated by the Fourth Amendment. While aircraft do not enhance the sense of sight by making it more keen, they expand it dramatically by

decisions had already concluded that losses of privacy resulting from exploitations of technological tools are not matters of Fourth Amendment concern if the tools are generally or routinely used by members of the public.[350] *Ciraolo* and *Riley* give the government free reign to expand perceptive and acquisitive faculties when the public does so by the same technological means. In those cases, general public use of aircraft to occupy new vantage points justified the conclusion that the home dweller had "knowingly exposed" his property to public view and thereby contradicted the legitimacy of any privacy expectation in the matters exposed.[351]

Two aspects of the current general public use doctrine merit further elaboration. First, *Ciraolo* and *Riley* did not turn on whether fellow citizens actually exploited aircraft to perceive the matters observed by law enforcement. As long

affording perches that human eyes could not have occupied in an earlier age. (Manned flights by hot air balloon did not begin until 1783–two years after the Bill of Rights was adopted–and the first American flight was not until ten years later. Modern hot air ballooning is reported to have begun as late as 1960. PAUL FILLINGHAM, THE BALLOON BOOK 125-29 (David McKay Company, Inc. 1977)). Technology that furnishes new vantage points for the use of human senses surely can and does augment human perceptual abilities as dramatically as technology that sharpens or extends those senses. By increasing sensory capacities in either way, a technological tool can jeopardize privacy interests that would have been safeguarded against the only means of invasion possible in an earlier era. This is the main reason why the dissenters in *Ciraolo* believed that aerial overflights constitute Fourth Amendment searches.

[350] *Ciraolo* made it clear that it is constitutionally irrelevant that the authorities used aircraft for the specific *purpose* of surveillance while members of the public use planes to travel. 476 U.S. at 213-14. This conclusion that governmental "purpose" is irrelevant was later reaffirmed in *Bond v. United States*, 529 U.S. 334, 338 n.2 (2000) ("The parties properly agree that the subjective intent of the law enforcement officer is irrelevant in determining whether that officer's actions violate the Fourth Amendment."). Apparently, the Court believes that the government agents' "purposes" have no impact on the perils posed to privacy. I will not take issue with that premise.

[351] By explaining that the conclusion in *Ciraolo* was rooted in the general public use doctrine, the *Kyllo* majority made it clear that the holdings in *Ciraolo* and *Riley* could not be justified by the *Katz* "knowing exposure" principle alone. That rationale ordinarily applies only to cases in which details are exposed to ordinary, unaugmented human senses and faculties. As a general rule, when matters are perceptible only by technological enhancements, the conclusion that they are knowingly exposed is not justifiable. A contrary conclusion would enable technological advances to eviscerate the informational privacy sheltered by the Fourth Amendment. The knowing exposure principle is applicable to the authorities' use of perception-enhancing devices when, and only when, the devices used are in general or routine public use. A loss of privacy due to knowing exposure is the exception, not the rule, when technologically-augmented senses are employed to gain access to otherwise inaccessible information.

as the public routinely or regularly used the technology to occupy the improved vantage point (*i.e.*, flew in fixed-wing aircraft at 1000 feet or in helicopters at 400 feet) and *could have* used unaided senses to perceive what the authorities perceived (*i.e.*, had the ability to look down and see the marijuana), the authorities' *actual* perceptions from the vantage points made possible by aeronautical technology did not violate reasonable expectations of privacy. If the access gained by officials is no greater than the access regularly gained by the public, the authorities are apparently at liberty to exploit that access by perceiving and acquiring more than the public generally perceives and acquires. When members of the public regularly employ a device to occupy positions from which they *could* make observations, the government does not intrude upon Fourth Amendment interests when it occupies those same positions *and* takes advantage of the newfound opportunities to observe.

Second, none of the Court's opinions discuss the *extent of public use* necessary to invoke the "general public use" doctrine. *Ciraolo* and *Riley* simply declared air travel to be sufficiently routine. The *Kyllo* Court found it obvious that thermal imager use was not sufficient to qualify, but announced no standard for discerning when a device qualifies.[352] Thus, the central element of the doctrine remains undefined and unsettled. In light of the doctrine's potential to authorize unregulated technological incursions into the domain of confidentiality originally preserved in the Constitution, this deficiency is serious.

Unlike the other two variations on the nature and character of the technology theme, the general public use variation can find logical justification that accords with the core values of the Fourth Amendment. If properly understood and applied, general public use is a constitutionally defensible limitation on constitutional scope and a potentially appropriate determinant of whether a particular technology has crossed the threshold. The Court's invocations of the doctrine to justify the conclusions in the aerial surveillance decisions, however, are not reconcilable with the premises that support the general public use criterion and reflect a misconception of the prerequisites for reliance on general public use. I first set out the reasoning that can support the doctrine before explaining the circumstances in which it might properly influence threshold

[352] *Kyllo*, 533 U.S. at 40.

technology decisions and detailing the reasons why it cannot sustain the outcomes in the aerial overflight cases.

Members of the public who use perception-enhancing technology can gain access to otherwise imperceptible, confidential information. When the use of a particular technology is "general," "routine," or "regular," the details that can be learned through the augmentation of human faculties are effectively "exposed" to users. Once the use of a device is known to be (or should be known to be) sufficiently widespread, it may be fair to conclude that individuals who choose to engage in conduct that renders details about their lives perceptible by the device effectively sacrifice or forfeit the privacy interest they would otherwise have in those details. Their "revelatory conduct" yields public exposure that contradicts the legitimacy of any assertions of secrecy. As a consequence, they have no greater constitutional entitlement to confidentiality in the information revealed than those who knowingly expose in-home activities to naked-eye observations from lawful public vantage points.[353]

Enthusiasm for this logic should be tempered to some extent by the consequences that follow. When individuals are charged with sacrificing privacy because their conduct is accessible to technologically-enhanced public perception, the scope of the privacy that was protected prior to the arrival and use of the technology at issue shrinks.[354] It is arguable that such shrinkage is intolerable, that human ingenuity should not be capable of diminishing priceless constitutional liberties, and, consequently, that no matter how much the public exploits technological tools, governmental use of these tools to gain previously unavailable access to confidential matters should be constrained. According to this view, public

[353] For a fuller discussion of the logic of revelatory conduct in other situations, see *supra* notes 206-53 and accompanying text.

[354] Justice Scalia seemed to acknowledge the validity of this point when he asserted that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology," using the aerial overflight cases to illustrate this assertion. *Kyllo*, 533 U.S. at 33-34. He then observed that "[t]he question . . . is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* at 34. If information was inaccessible to unaided human faculties–except by means that would have triggered Fourth Amendment scrutiny–the interest in keeping the information confidential would have been sheltered by the constraints imposed by that provision. Officials would have been prevented from learning the details when they could not demonstrate that their conduct was reasonable.

use of technological innovations should not lead to losses of informational privacy vis-a-vis the government. We should not have to live our lives less freely and more circumspectly because confidentiality protective precautions that could prevent human perception are impotent against superhuman faculties afforded by science and technology.[355]

These concerns with technologically-caused shrinkage of constitutionally-sheltered privacy are legitimate. We should not lightly conclude that the Framers would have found such losses of freedom tolerable. It is possible, nonetheless, to reconcile the logic of the general public use criterion with Fourth Amendment premises and values. The logic supporting the general public use doctrine does not rest on the existence of technology alone or even upon mere public use of technology. It hinges upon societal acceptance of general, routine public use of a particular confidentiality-breaching device. Acceptance of general public use provides some evidence that "the People" no longer value the secrecy of the information accessible to technologically-enhanced senses. If the values jeopardized by widespread public use of a device that puts privacy at risk were sufficiently important, one might expect some indication of societal disapproval.[356] If regular public use of a device to access our secrets breeds no evident resentment and provokes no restrictive reaction, one might logically infer a general sentiment that the harm done to privacy is tolerable. If society no longer values and has insufficient concern with maintaining the secrecy of the information perceptible by the

[355] One might find some support for this argument in the stirring words of Justice Stewart in *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (emphasis added) (footnote omitted):

> [T]he values that [the Fourth Amendment] represents may appear unrealistic or "extravagant" to some. But the values were those of the authors of our fundamental constitutional concepts. In times not altogether unlike our own they won–by legal and constitutional means in England, and by revolution on this continent–a right of personal security against arbitrary intrusions by official power. *If times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important*.

[356] This indication could take the form of a legal provision that bars, sanctions or criminalizes the use of or restricts the availability of the technology. Electronic eavesdropping provides an illustration of how adverse societal reactions to the risks of neighbors snooping on our lives can find expression in legal restraints. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521 (2001). Perhaps even some less extreme, but nonetheless meaningful, expression of disapproval of the public's use of technology to gain access to private lives would suffice.

sense-enhancing tool, the authorities can plausibly argue that their exploitation of the mechanism in general public use does not deprive individuals of cognizable privacy interests. Instead, it merely takes advantage of the willingness to engage in "revelatory behavior," gaining access to knowingly exposed information in which there is no genuine secrecy interest.

In construing constitutional guarantees, it makes sense to take changes in both the technological and the attitudinal landscape into account.[357] The protection afforded by a living Constitution might expand or contract due to changes in the fabric of the society for which it was designed. The Framers sought to preserve against unjustified invasion a valued sphere of confidentiality. If modern society no longer values the secrecy of some information, it is not illogical to conclude that the Constitution does not safeguard the secrecy of that information. To tolerate a diminution of privacy in those circumstances–that is, when society has clearly evinced a lack of concern for privacy–does not necessarily betray original values or purposes.

To prevent excessive contraction of constitutional interests, however, the general public use criterion must be invoked only in situations where its logic applies. Official exploitation of a mechanism should be considered beyond Fourth Amendment reach *only* when the mechanism is *actually used by the public with sufficient regularity or routineness*. Moreover, mere public use in some fashion should not suffice. A finding that the public does not value the confidentiality of information can be justified *only if the public regularly or routinely uses the device to perceive that information*. If public use is limited, it does not justify the conclusion that society has accepted losses of privacy occasioned by unrestricted official use or that individuals have knowingly exposed matters learned by the authorities to public view. Restricted public use that does not in fact breach the secrecy of particular facts is more analogous to, and should be treated like, mere availability of a device that the public does not generally use.[358]

---

[357] *Cf.* Minnesota v. Dickerson, 508 U.S. 366, 382 (1993) (Scalia, J., concurring) (suggesting that the development of firearms might justify invasions of the privacy and security of persons that would have been impermissible before the advent of that particular technology).

[358] See *supra* notes 320-23 and accompanying text, for a discussion of the

A logical understanding and application of the general public use doctrine cannot support the Court's holdings in the aerial surveillance cases. The facts of *Ciraolo* and *Riley* did not provide a basis for concluding that society does not value the confidentiality of the matters the authorities gained access to by means of the vantage points made possible by aircraft. The public may well have used airplanes to occupy the same vantage points occupied by officers. There was no demonstration, however, that the public in fact used the access furnished by technology to actually perceive matters on the ground. There was no reason to believe that members of the flying public were regularly scanning (or even glancing into) residential property and observing the activities occurring there. There may have been "technical exposure" to naked senses in the sense that there was no physical barrier or obstruction, but there was no actual exposure to anyone except the authorities who surveyed the properties from the technologically-improved vantage points.[359] If the flying public does not routinely monitor our lives from above, then the absence of adverse public reaction, the lack of legal or other restrictions on aerial surveillance, does not evince a lack of concern for the privacy of activities on our residential property. Rather than evincing the lack of an interest in confidentiality, the failure to cover yards may simply reflect the well-grounded belief that what goes on there will not be observed or learned by those who fly in the public airways.

Put simply, the public generally, routinely and regularly uses aircraft for limited purposes and in limited ways. Members of the flying public do not exploit the enhanced opportunities for perception afforded by the improved vantage points. As a result, there does not seem to be a constitutionally adequate reason for concluding that the government's use of aircraft merely takes advantage of revelatory behavior. Instead, it would appear to infringe upon privacy interests in curtilage and homes that were valued when the Constitution was drafted and are still

illogic of relying on mere general availability of a device to the public.

[359] *See* Ciraolo v. California, 476 U.S. 207, 223-24 (Powell, J., dissenting) (maintaining that "the actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent," that "travelers" on such aircraft "normally obtain at most a fleeting, anonymous, and nondiscriminating glimpse of the landscape and buildings over with they pass," that the "risk that a passenger on such a plane might observe private activities, and might connect those activities with particular people, is . . . trivial . . . [t]herefore, people do not `knowingly expos[e]' their residential yards `to the public' merely by failing to build barriers that prevent aerial surveillance") (alteration in original).

valued today.

The *Ciraolo* Court did not disagree with my assessment of the realities. The basis for the conclusion was that the public routinely occupied the newly-available vantage point afforded by aircraft and *could* look down and see what the officers saw.[360] The Court did not declare that the flying public actually did regularly observe the matters the officers observed.[361] The logic that supports the "general public use" variable requires more than the *possibility* that the public *could* use the technology to improve perception and learn previously imperceptible matters. Unless it is shown that the public actually does make use of the improved abilities to access those matters and that society has accepted such public access, it does not seem constitutionally defensible to find forfeiture of entitlements to confidentiality that would have historically and traditionally been protected.[362]

---

[360] *Id.* at 213-14 ("Any member of the public flying in this airspace who glanced down *could have seen* everything that these officers observed.") (emphasis added).

[361] *Id.* at 213. The same was true in *Riley.* The decision was based on public presence in the airways, not public observations of residential property. Florida v. Riley, 488 U.S. 445, 450-51 (1988).

[362] The Court's recent holding in *Bond v. United States*, 529 U.S. 334 (2000), provides powerful support for this understanding and restriction of the "general public use" criterion. *Bond* held that an officer conducted a search by engaging in tactile manipulation of a soft-sided bag in more intrusive ways than are typical of the public's actual handling of such bags. *Bond*, 529 U.S. at 338-39. Officers do not intrude upon reasonable expectations of privacy if they touch and feel bags in the manner and to the extent that the public *actually does* touch and feel the bags. *Id.* They cross into Fourth Amendment territory, however, intruding upon preserved confidentiality interests, when they use their sense of touch to gain access to and learn more than the public generally learns about the contents of bags. *Id.* It does not matter that the public is in a position to manipulate bags more intrusively and could lawfully do so. *Id.* at 338. In my view, the *Bond* majority implicitly acknowledged that it is not logical to charge individuals with knowing revelatory behavior that defeats an entitlement to confidentiality unless the public actually engages in the conduct that renders that behavior perceptible. *See id.* at 338-39 (observing that "a bus passenger clearly expects that his bag may be handled," but "does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner," and concluding, therefore, that the agent's exploratory "physical manipulation" was a search that "violated the Fourth Amendment"). For purposes of determining whether "knowing exposure" has occurred, there is surely no reason to treat public uses of technology differently from public uses of ordinary human senses. Actual routine or regular public employment of the sense-enhancing device to perceive matters that officials have used it to perceive should be essential for the loss of privacy interests.

Language in *Kyllo* may reflect a recognition of the merits of this position. According to the logic I have explained, the pertinent question in *Kyllo* was whether the public engages in thermal imaging of homes and gains access to information about relative heat levels, not whether the public merely possesses,

If it is appropriate to link Fourth Amendment scope to actual public use of a particular sense-enhancing technology, a critical question arises: How much public use is necessary before an otherwise protected entitlement to confidentiality is defeated? Reflected in the current doctrine is a clear, and appropriate, conclusion that not just any amount of public use is sufficient to justify the conclusion that governmental exploitation is not a search. According to the Court, the public's use must be "general," "routine," or "regular" to render it no longer legitimate to expect that the information rendered accessible by such use will remain confidential.[363] The Court has not, however, prescribed the extent of public use of a technological enhancement that is sufficient to meet this requirement.[364]

While efforts to prescribe a bright-line standard in this area seem futile, if the "general public use" criterion is to be applied in a consistent and principled fashion, some sort of guidance is essential. The standard chosen should be rooted in the rationale for permitting general public use to diminish the scope of constitutional privacy protection. The constitutionally relevant inquiry is whether public use of the device to perceive otherwise inaccessible facts is *frequent* and *obvious* enough to make it logical to infer that society has accepted the losses of confidentiality that have resulted. "General" or "routine" public use should be found only when the *risk* of public access by technological means is high enough to fairly charge the individual with revelatory

carries or aims thermal imagers at homes. *Kyllo*, 533 U.S. at 35-36. The determinative inquiry was whether the public actually exploits the increased access to learn otherwise concealed details, not whether the public *could* do so. In declaring that governmental use of thermal imagers to scan homes was regulated, the *Kyllo* majority asserted that it could "confidently say that *thermal imaging* [was] not `routine.'" *Id*. at 40 n.6. Moreover, the majority did not even acknowledge the dissent's contentions that thousands of similar thermal imagers had been manufactured and that the device is "readily available to the public." *See id*. at 47 n.5 (Stevens, J., dissenting).

[363] In her important concurrence in *Riley*, Justice O'Connor stressed the determinative nature of the requirement that the public be present in the airways at the relevant altitude with "sufficient regularity." *Riley*, 488 U.S. at 454 (O'Connor, J., concurring in the judgment).

[364] In *Ciraolo* and *Riley*, the Court considered public use of the airways to be sufficiently routine but neglected to provide any additional insight into the extent of use that is sufficient. *Ciraolo*, 476 U.S. at 215; *Riley*, 488 U.S. at 450. After describing the controlling question as whether a device was "in general public use," the *Kyllo* Court could have endeavored to prescribe a standard for ascertaining when use is widespread enough to be considered "general." *Kyllo*, 533 U.S. at 34. Because the majority was "quite confident[]" that thermal imaging of residences by the public fell well short of the extent needed to qualify, it did not need to address the quantitative question. *Id*. at 40 n.6.

behavior that sacrifices and forfeits any interest in secrecy.[365] With regard to any particular technology, resolution of the general public use question involves two steps. First, a court must make a genuine effort to ascertain how many members of the ordinary public use the particular device at issue to perceive matters that are beyond the reach of ordinary senses *and* how often such use occurs.[366] Then, a court will have to apply the governing legal standard to the particular case, determining whether the extent of actual use by the public is sufficient to satisfy that standard.

4. The "Location of the Privacy Interest" Variables

I label the final major category of influential variables "the location of the privacy interest." The characters of the physical sites of putative privacy interests have had undeniable effects on the resolution of threshold technology issues. Three variations on the locational theme can be

[365] The extent of the public conduct and the risk of perception questions are not unique to cases involving technologically-aided perception and acquisition. One who stands in his uncovered front window or unfenced front yard and engages in conduct visible to naked eyes "knowingly exposes" that conduct to the public and has no legitimate expectation of privacy. *See* Katz v. United States, 389 U.S. 347, 351 (1967). One who places soft-sided luggage on a bus does not knowingly expose the contents to probing tactile manipulation by the public. *See Bond*, 529 U.S. at 338-39. In each case, there is a risk or likelihood that the public will learn information by the use of ordinary senses. When officers use their eyes in the first instance to perceive in-home conduct, they do not violate privacy because the risk of being seen by the public is sufficiently high to justify that conclusion. When officers use their fingers in the second situation to sense the contents of luggage, they do violate privacy because the risk of having contents felt by the public is too low to justify a contrary conclusion. There is no reason why the standard chosen for cases involving technology should be different from the standard for cases involving ordinary sense perception.

[366] The pertinent question is not how many members of the public have aircraft or imagers or other devices. If that were the question, then the relatively simple quest would be to measure the percentage of the general public in possession of the particular device. Because the relevant question focuses on the extent to which the device is used to access otherwise confidential information, the measurement task is more complex. I am not sure how best to execute that task. Perhaps one could measure frequency of use in terms of the number of days per year on which the public employs the particular mechanism to gain access or the number of times per year or week that the information that would remain concealed without the tool is actually learned by others or even the percentage of persons in the population who suffer such a loss of privacy of this sort in a particular time span. In the cases discussed–*Ciraolo*, *Riley*, and *Kyllo*–there seems to have been no real effort to measure the extent of public use. The Court simply declared private and commercial air travel to be sufficient and thermal imaging to be inadequate.

identified. The first is the unmistakable primacy of home privacy. The second is the devaluation of privacy interests in other private domains–particularly residential and commercial curtilage–resulting from the special respect accorded home privacy. The third is the low likelihood of prevailing with a Fourth Amendment threshold claim in public places.

a. The First Variation: The Special Vigilance Reserved for Home Sweet Home

The authorities are most likely to cross the Fourth Amendment's threshold when they employ technological innovations to investigate home interiors. It is not coincidental that the only two post-*Katz* instances in which the Supreme Court has found that an exploitation of technology crossed the Fourth Amendment's threshold–*United States v. Karo*[367] and *Kyllo v. United States*[368]–have involved official surveillance of private residences. In *Karo*, the Court observed that the question was "whether the monitoring of a beeper *in a private residence*" infringed on Fourth Amendment interests.[369] The Court's answer to that question began with the straightforward assertions that it is "obvious" that people expect privacy in their homes and that society deems those expectations "justifiable."[370] Beeper monitoring inside a home constituted a search because it revealed "a critical fact about *the interior of the premises*."[371] In *Kyllo*, the Court began its analysis of the relationship between thermal imaging and the Fourth Amendment by observing that although the limits of the *Katz* doctrine had been difficult to discern in some settings, for home interiors "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable."[372] Justice Scalia then warned that "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode" Fourth Amendment privacy.[373] To prevent that unacceptable consequence, the Court declared that any use of "sense-enhancing technology"

---

[367] 468 U.S. 705 (1984).
[368] 533 U.S. 27 (2001).
[369] *Karo*, 468 U.S. at 714 (emphasis added).
[370] *Id.*
[371] *Id.* at 715 (emphasis added).
[372] *Kyllo*, 533 U.S. at 34.
[373] *Id.*

not in general public use to perceive and learn "any information regarding the interior of a home that could not otherwise [be] obtained without physical `intrusion into a constitutionally protected area,' . . . constitutes a search."[374]

The in-home location of the privacy interests at risk in *Karo* and *Kyllo* clearly restricts the scope of the Court's holdings. It is uncertain whether the controlling principle of those decisions extends to other contexts. For present purposes, the important feature of each opinion is the powerful influence the locational factor had on determinations that the constitutional threshold had been crossed. The holdings that beeper monitoring and thermal imaging of private residences constituted searches were fueled by the special reverence accorded the privacy of home interiors and by a genuine hesitance to allow any technological diminution of home privacy.[375] The historical respect for homes and the clear intent of the Constitution's authors to preserve an entitlement to be left alone in our "castles" weighed heavily in favor of the results reached in both cases.

This is not to say that technologically-aided surveillance of private homes is always regulated by the Fourth Amendment. In *Katz*, Justice Stewart warned that the knowing exposure of matters to the public "even in [one's] own home" precludes Fourth Amendment protection.[376] Even home privacy can be surrendered or forfeited by conduct evincing a lack of, or insufficient interest in, maintaining confidentiality. *Smith v. Maryland*[377] proved that home interiors are not sacrosanct–*i.e.*, that behavior within the four walls is not always sheltered against technologically-

[374] *Id.* (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

[375] Emphasis on the special character of home privacy is not unique to technological contexts. In a variety of situations, "the Court since the enactment of the Fourth Amendment has stressed `the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.'" Oliver v. United States, 466 U.S. 170, 178 (1984) (Powell, J., concurring) (quoting Payton v. New York, 445 U.S. 573, 601 (1980)). *See, e.g.*, Steagald v. United States, 451 U.S. 204, 211-16 (1981) (stressing the significance of the home as a basis for holding that the Fourth Amendment requires a search warrant to enter the dwelling of one person in order to arrest another individual who does not reside there); Payton v. New York, 445 U.S. 573, 585-90 (1980) (emphasizing the importance of home privacy as a reason for concluding that entry of a person's dwelling to arrest that person for a felony requires an arrest warrant).

[376] Katz v. United States, 389 U.S. 347, 351 (1967).

[377] 442 U.S. 735 (1979).

enhanced eyes or ears.[378] Although the government used a pen register to perceive and record the numbers dialed from a private residence, the Fourth Amendment did not apply because the individual had voluntarily conveyed the numbers to the cooperating telephone company.[379] Nonetheless, the in-home setting generally lends considerable weight to threshold technology claims[380]

The Court is right to be exceedingly chary of technological threats to the privacy of dwellings. Heightened vigilance against not only physical, but also technological, breaches of the "firm line at the entrance of the house"[381] is soundly premised and amply warranted by historical purposes and an unaltered tradition of respect for home privacy.[382] Respect for home privacy has deep historical roots.[383] The high value that the Framers placed on home privacy suggests that they would have intended the Constitution to have the flexibility necessary to ensure that scientific and technological advances could not effectively deprive the people of the security and freedom provided by the right to keep matters inside dwellings confidential. Those who were intensely concerned with threats to home

---

[378] *Smith*, 442 U.S. at 745.

[379] *Id.* at 743.

[380] Even in *Smith*, dissenting Justice Stewart, the author of *Katz*, expressed a belief that the in-home location of the conduct sensed by the pen register militated in favor of a contrary conclusion. *See id.* at 747 (Stewart, J., dissenting) (relying in part on the fact that "information obtained by pen register surveillance . . . emanates from *private conduct within a person's home* or office–locations that without question are entitled to Fourth . . . Amendment protection") (emphasis added).

[381] Payton v. New York, 445 U.S. 573, 590 (1980).

[382] The reference to technological "breaches" is by no means intended to endorse a requirement that a particular device must gain access to information about a home interior by somehow passing through the home's walls. The *Kyllo* Court correctly rejected the notion that technological tools do not trigger Fourth Amendment regulation unless they somehow physically pierce the exterior walls of a home. *See Kyllo*, 533 U.S. at 35 (observing that the Court had already rejected the notion that the technology had to in some sense pass through the walls of the home). A technological device can shrink the entitlement to privacy in the home by passively receiving information that passes outside the home but is imperceptible without either the sensory enhancements of the device or a physical intrusion into the home. *Id.* at 33-36.

[383] *See* Wilson v. Arkansas, 514 U.S. 927, 931 (1995) (observing that "the common law generally protected a man's house as `his castle of defence and asylum'") (quoting 3 WILLIAM BLACKSTONE, COMMENTARIES *288); *Payton*, 445 U.S. at 596-97 (asserting that the common law's "zealous and frequent repetition of the adage that a `man's house is his castle,' made it abundantly clear that both in England and in the Colonies, `the freedom of one's house' was one of the most vital elements of English liberty") (footnote omitted); *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1358-60; Robert J. Leibovich, Note, *Privacy Goes Camping: Staking a Claim on the Fourth Amendment*, 26 U. MEM. L. REV. 293, 294-97 (1995).

privacy posed by physical entries surely would have been deeply troubled by nonphysical threats to those same privacy interests. There is no basis for believing that the Framers placed less value on any particular aspect of in-home privacy or viewed any information about home interiors as undeserving of constitutional shelter.[384] Moreover, the emphasis on home privacy also reflects contemporary values. Time has not diminished society's reverence for the home and for the freedom to keep confidential whatever we choose to do within our private residences.[385] For these reasons, the decision to subject technologies that afford access to *any* otherwise imperceptible details about the home to Fourth Amendment constraints is legitimate, logical and laudable.

b. The Second Variation: The Harmful Impacts of Reverence for Home Privacy on Other Private Domains

Like technology itself, the special reverence for home privacy can be a very sharp, two-edged sword. The fact that a technological device has posed a threat to home privacy has militated strongly in favor of constitutional protection against exploitation of that device. When the privacies jeopardized have been situated outside homes, the Court has been inclined to reject claims that technologically-aided surveillance crossed the Fourth Amendment threshold. For official conduct directed at locations outside the home, the Court has taken assertions of secrecy less seriously, has been less vigilant against technological threats and has been more willing to find the Fourth Amendment irrelevant. In my view, the primacy of home privacy has had corrosive impacts on entitlements to secrecy in other domains. A devotion to home privacy has led the Court to undervalue other confidentiality interests.

The tendency to discount informational privacy interests located outside dwellings seems misguided. If a domain harbors privacy interests entitled to protection against the physical intrusions known to our ancestors, those interests

---

[384] *See Kyllo*, 533 U.S. at 37 ("In the home . . . *all* details are intimate details.").

[385] In a recent reflection on the meaning and status of privacy in American society, Jeffrey Rosen contends that the shelter provided for home privacy has diminished over time. *See* Rosen, *supra* note 118, at 26-53. In his view, courts, including the Supreme Court, have permitted "legal protection for privacy at home . . . to atrophy over the past few decades." *Id.* at 52-53.

should also be shielded against technological surrogates. The fact that the privacy at stake may rank lower in the Fourth Amendment scheme than in-home privacy does not support and should not prompt a contrary conclusion. The paramount importance of home privacy does not mean that privacy interests in other areas are unimportant, unworthy or undeserving.[386] Our ancestors' special reverence for home privacy is consistent with respect for entitlements to keep our lives confidential in other domains–both domains they knew and those that would emerge over time.[387] The Constitution guards against unreasonable searches of locations other than residences, providing entitlements to maintain confidentiality when we venture into the world outside our homes.[388] There is no basis for concluding that the reach of the Fourth Amendment does not extend to technological threats to interests outside the home or that constitutional privacy entitlements are somehow less valuable when the risks are posed by means other than physical intrusion.[389]

The aerial surveillance cases provide illustrations of the influence of the locational factor and of the dangerous tendency to devalue privacy interests outside dwellings. In both *California v. Ciraolo*[390] and *Florida v. Riley*,[391] the Court held that the observation of matters in residential curtilage from aircraft flying in lawful airspace did not violate reasonable expectations of privacy.[392] The holdings that no

[386] As society has evolved and our lives have become more mobile, as we spend more and more of our waking hours away from home, there may be even more reason to prize our right to preserve secrecy outside dwellings and to be concerned with novel perils generated by scientific and technological progress. While privacy of the home is still highly valued, it is arguable that changes in the nature of our society have elevated the value of extra-home privacies.

[387] See *United States v. Chadwick*, 433 U.S. 1 (1977), for support of these arguments. Therein, the Court rejected the government's claim that the warrant rule governed only the especially significant privacy interests present in homes and private communications, holding that private repositories located in public places are also entitled to its protection. *Chadwick*, 433 U.S. at 7, 11. According to the Court, "the Framers were men who focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth." *Id.* at 9.

[388] *Id.* at 7.

[389] These lessons, I believe, are reflected in the landmark holding in *Katz* that the privacy of conversations in public phone booths is entitled to protection against interception by technology that does not breach the physical integrity of the booth. Katz v. United States, 389 U.S. 347, 353 (1967). The negative impacts of devotion to home privacy result from a constrictive attitude toward Fourth Amendment values that stands in stark contrast to the expansive attitude of the *Katz* Court.

[390] 476 U.S. 207 (1986).

[391] 488 U.S. 445 (1989).

[392] *Ciraolo*, 476 U.S. at 213-14; *Riley*, 488 U.S. at 450.

searches had occurred rested primarily on the homedwellers' knowing exposure of the facts to views from mechanisms in general public use.[393] The Court did not explicitly cite the nature of the locations at issue as bases for rejecting the threshold claim.[394] Nevertheless, there is reason to believe that the results in both cases were influenced to some extent by the fact that the information learned was situated outdoors in areas surrounding the homes rather than inside home interiors.

In *Ciraolo* and *Riley*, the authorities used technological advances to learn about otherwise imperceptible activities on residential property surrounding homes[395]–areas clearly entitled to Fourth Amendment protection.[396] The Court observed that the officers' conduct did not physically intrude into the areas,[397] did not interfere with use of the property,[398] and posed no risk of disclosing "intimate associations"[399] or other "intimate details connected with the use of the home or curtilage."[400] These same considerations would not have influenced the threshold inquiry if the details perceived by technological sense enhancements had been located inside dwellings.[401] They militated against Fourth Amendment protection *because* the area surveilled was exposed land outside homes.[402] The less private location targeted by technology provides at least a partial explanation for the Court's refusal to take seriously the very plausible contention that there was in fact no real "knowing exposure" because the flying public does not observe what happens in

[393] *See supra* notes 329-51 and accompanying text.

[394] *Ciraola*, 476 U.S. at 213-14; *Riley*, 488 U.S. at 449-50.

[395] *Ciraolo*, 476 U.S. at 209; *Riley*, 488 U.S. at 448. In *Riley*, the information learned was also located inside an outbuilding that was in a state of disrepair. *Id*.

[396] *See* Oliver v. United States, 466 U.S. 170, 180 (1984) (holding residential curtilage is entitled to Fourth Amendment protection).

[397] *Ciraolo*, 476 U.S. at 213.

[398] *Riley*, 488 U.S. at 452 (observing that there was no interference with normal use and "no undue noise, and no wind, dust, or threat of injury").

[399] *Ciraolo*, 476 U.S. at 215 n.3.

[400] *Riley*, 488 U.S. at 452.

[401] *See* Kyllo v. United States, 533 U.S. 27, 34-35 (2001). For technological explorations of home interiors, the lack of penetration through the walls is irrelevant, *id*. at 35, and "*all* details are intimate details," *id*. at 37.

[402] *Ciraolo*, 476 U.S. at 213-14; *Riley*, 488 U.S. at 449-50. The Court did suggest, in *Oliver v. United States*, that the character of residential curtilage might support diminished standards of reasonableness. *See Oliver*, 466 U.S. at 180 n.11 (declining to decide whether curtilage is entitled to same degree of protection afforded homes and other highly private areas).

residential curtilage.[403] Technology afforded access, enabling the government to breach the confidentiality of information that it could not have learned in an earlier age. However, because it was not used to learn details about home interiors, the Court was less inclined to find that the constitutional threshold had been crossed. In sum, the locational factor influenced the majority's conclusion that naked eye aerial surveillance was not regulated by the Fourth Amendment.

One need not speculate about the powerful negative effects of the locational factor in *Dow Chemical Co. v. United States*.[404] Prominent among the array of reasons for concluding that photographic aerial surveillance was not a search was the "commercial curtilage" character of the area at issue.[405] While the *Dow* majority did not deny all Fourth Amendment protection for this domain, it refused to find that the privacy of the area had been violated by the combination of two technological enhancements (an airplane and a precise mapping camera) that together made it possible to perceive facts otherwise entirely inaccessible without physical trespass.[406] The conclusion that this technologically-enabled breach of secrecy was unregulated–despite the fact that it enabled the acquisition of information that could only have been accessed in an earlier day by a regulated physical intrusion–rested in large part on the relatively low ranking of the location involved. Because the land surrounding the manufacturing facility was a far cry from a home, and was even less deserving of protection than the land immediately surrounding a home, it was accorded *no* shelter against the enhanced perception afforded by aeronautical and photographic technologies.

The reasoning of the aerial surveillance decisions and their implications for threshold technology inquiries are questionable at best, dangerous at worst. If a location is entitled to constitutional shelter–*i.e.*, if it is a sphere in which Fourth Amendment interests in confidentiality are protected against physical or other intrusions—then

---

[403] Four dissenters believed that contention had merit. *See Ciraolo,* 476 U.S. at 223-24 (Powell, J., dissenting). For further discussion of this argument, see *supra* notes 360-63 and accompanying text.

[404] 476 U.S. 227 (1986). The overt reliance on the character of the location at issue in *Dow*, 476 U.S. at 239, provides an additional reason to believe that the factor was influential in *Ciraolo*, a companion case to *Dow*.

[405] *Id*. at 239. The Court maligned the area as closer to open fields than to residential curtilage. *Id.* at 239.

[406] *Id*. at 238-39. The aircraft enabled the officers to occupy a new vantage point otherwise unavailable to flightless homo sapiens, and the camera was able to capture small details imperceptible to unaided human eyesight.

technological surrogates for the regulated intrusions should also be governed. Advances in the capacity to perceive and acquire concealed facts about individuals' private lives should not be allowed to shrink entitlements to secrecy in these domains merely because the interests jeopardized are not as exalted as home privacy interests. The relatively lower rank of these interests in the Fourth Amendment hierarchy[407] is not a rational basis for refusing to guard against novel methods of breaching confidentiality.[408]

In sum, the Court's reliance on the character of locations to restrict the reach of the Fourth Amendment in residential and commercial curtilage contexts is seriously flawed.[409]

---

[407] The point in the text is that *even if* the location is one in which privacy interests are less deserving, that fact alone should not be relied upon as a basis for a negative threshold conclusion in cases involving technological sense enhancement. I do not concede that privacy interests in residential curtilage are markedly less deserving of shelter. Perhaps the fact that the residential curtilage is out-of-doors and exposed does diminish the worth of the confidentiality interests in that domain. It is far from certain, however, that the privacy interests in the areas surrounding homes merit considerably less respect than the interests inside homes. After all, the curtilage is the area into which the privacies of the home extend. *See* Oliver v. United States, 466 U.S. 170, 180 (1984). Moreover, residential curtilage furnishes important protection for home interiors by providing a "buffer zone" into which the authorities may not intrude without justification.

[408] It may provide a reason for demanding lesser showings of reasonableness than is the norm for technological and other invasions of home privacy. *See supra* note 298 and accompanying text. The fact that the diminished character of the privacy interests in a location can appropriately be factored into the Fourth Amendment balance when assessing the *reasonableness* of a search is an additional reason not to rely on the locational variable as a basis for outright denial of any protection.

This is not to suggest that the norm should be diminution of Fourth Amendment reasonableness demands based on the character of locations and privacy interests. We should be on guard against the too facile conclusion that because a privacy interest lies outside the home it merits only diminished Fourth Amendment protection. The presumption, not easily overcome, should be that "a search is a search" and that the full protection of the Fourth Amendment applies. *Cf.* Arizona v. Hicks, 480 U.S. 321, 325 (1987) (concluding that mere movement of a turntable inside a dwelling is a search that is reasonable only upon probable cause).

[409] In *United States v. Place*, 462 U.S. 696 (1983), in deciding that a dog sniff was not a search, the Court pointed out that the item examined was a piece of luggage situated "in a public place." *Id.* at 707. The implication was that the location rendered the luggage less deserving of protection. Moreover, in *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), the canine sniffs at issue were aimed at vehicles on public roads. *Id.* at 34-35. Vehicles, especially those in public places, are notorious for their diminished expectations of privacy. *See* Wyoming v. Houghton, 526 U.S. 295, 303-04 (1999); California v. Carney, 471 U.S. 386, 391-92 (1985); United States v. Chadwick, 433 U.S. 1, 12-13 (1977).

My analyses of the Court's reasoning in the curtilage cases is equally pertinent to other domains in which Fourth Amendment privacy interests exist

While the exalted character of home privacy should prompt sensitivity to technological surveillance of dwellings, there is no reason why special vigilance against technological and other threats to home privacy should yield a lack of or lesser vigilance when novel mechanisms afford access to other constitutionally-sheltered domains. If an area deserves some measure of Fourth Amendment protection, technological tools that enable the authorities to effectively violate confidentiality by perceiving facts that were previously perceptible only by regulated means cross the constitutional threshold. Fidelity to the Framers' objectives and respect for their values dictate this conclusion.

c. The Third Variation: The Denial of Privacy in Public Places

The final variation on the locational theme is the disinclination to find protected privacy interests in public places. The fact that technology is employed to acquire information *situated in a public place* militates strongly against and is likely to defeat a threshold technology claim. The decision and reasoning in *United States v. Knotts*[410]

but may be less valuable than home privacy interests. The relatively lower expectations of privacy in either publicly-located effects or in vehicles on the road should not be the basis for concluding that no search has occurred. Whenever a technological tool has been used to breach the confidentiality of information concealed by the effect or vehicle, the Fourth Amendment should be concerned. Effects, vehicles and other areas of our lives in which there are entitlements to keep information secret and concealed should be safeguarded against devices that make it possible to access, perceive and learn that information. The special value of home privacy should not prompt the neglect of other privacies essential to security and freedom.

The conclusion in *Katz v. United States* that conversations in telephone booths are protected against electronic eavesdropping is consistent with and supportive of my views. 389 U.S. 347, 359 (1967). The fact that Mr. Katz spoke outside his home and in full view of the public did not count against, much less defeat, his claim that a privacy-violating exploitation of technology had occurred. Because the government had used a sense-enhancing device to gain access to information that would otherwise have remained confidential (barring a regulated physical intrusion) the Court concluded that the government had searched within the meaning of the Fourth Amendment. *Katz*, 389 U.S. at 352.

In addition, the majority opinion in *United States v. Karo* intimated that if an electronic beeper were employed to access information about the contents of a rented locker in which an individual has a legitimate expectation of privacy, a Fourth Amendment search would occur. 468 U.S. 705, 720 n.6 (1984). In my view, this suggestion reflects a proper interpretation of the relationship between technology and the threshold of the Fourth Amendment. The privacy interests in rental lockers, though less significant than those within homes, are valued and worthy of constitutional protection. The confidentiality of details about our lives concealed in such repositories should be safeguarded not only against physical invasion, but also against technological surrogates for physical invasion.

[410] 460 U.S. 276 (1983).

illustrate the influence of the public place variable.[411]

In *Knotts*, official monitoring of a beeper attached to a can of chemicals was found not to be a search because individuals do not have legitimate expectations of privacy in movements on public thoroughfares and in other public locations.[412] While the logical basis for the holding that the exploitation of technology in *Knotts* was unconstrained was that members of the public could have seen all of the details learned with their naked eyes,[413] it seems fair to conclude that the Court was less willing to question that conclusion because of the location of the matters claimed to be secret.

At first glance, the influence accorded this particular locational variable seems eminently sensible. The location of information in a genuinely open, public place seems inconsistent with a legitimate expectation of privacy in that information. Truly public venues are not typically thought to be places in which individuals have or maintain secrecy interests. Because public domains are the antitheses of privacy, when individuals enter those domains they surrender entitlements to confidentiality they would otherwise possess.

In my view, this logic is unimpeachable when the details perceived and acquired by a novel technology are also capable of being perceived, and are perceived, by unaided human senses.[414] I have serious questions, however, about the application of this logic to situations in which sense-improving mechanisms enable the authorities to learn publicly-located matters that would have remained unknown in an earlier era. Undetectable tracking beepers enable officials to acquire comprehensive records of public travels with much lower risks of failure than those inherent in ordinary sense surveillance by fallible human beings.[415]

---

[411] *Knotts*, 460 U.S. at 281-82. The reasoning in *United States v. Place*, 462 U.S. 696 (1983), also demonstrates the influence of the factor. In deeming a dog sniff of luggage not to be a search in that case, the Court stressed that the opinion was confined to luggage that was situated "in a public place." *Place*, 462 U.S. at 707.

[412] *Knotts*, 460 U.S. at 281. In contrast, when the beeper monitors activity inside a home–even the mere movements, presence or absence of an inanimate object–a search does occur. For a discussion of *United States v. Karo*, see *supra* notes 282-88, 291-92, 367-71 and accompanying text.

[413] *See supra* notes 207-12 and accompanying text.

[414] See *supra* notes 213-20 and accompanying text, for a more complete discussion of this question.

[415] See *supra* notes 218-19 and accompanying text, for a discussion of this

Although the additional information that can be gathered is not physically or technically concealed, it might well remain secret and confidential from ordinary human senses. Sensitive listening devices can furnish abilities to listen to conversations in public places that unaided ears could not possibly access because the parties have lowered their voices and ensured that they are out of the range of potential eavesdroppers. These conversations are located in and gathered from a public place. Nonetheless, the information perceived by technological means would not have been perceptible by ordinary senses and could not have been learned by the government at all–not even by means of physical intrusion–at the time the Constitution was framed. Technological advances alone have brought it within reach, making new breaches of confidentiality possible.[416]

My point is simple. The location of information in a public place does not necessarily nullify confidentiality even if the information is not shielded by a physical barrier. Physical barriers to human senses are not always essential to preserve secrecy, and the absence of those barriers should not be dispositive in deciding whether novel devices threaten confidentiality. Privacy can exist "in plain sight" and has done so for centuries. A public setting is not inherently inconsistent with an interest in confidentiality. For these reasons, knee-jerk reliance on the public place factor to reject Fourth Amendment threshold claims is not justifiable. It is not implausible to contend that when the authorities use technology to access publicly-situated and physically-exposed details that otherwise would not or might not be perceptible to human faculties they violate privacy. If the exploitation of a device enables the government to learn details that could not or would not have been learned at all by means known to the Framers, not even by methods subject to constitutional regulation, categorical rejection of a privacy claim based on "public location" does not seem sensible. In cases where it is arguable that privacy interests do exist in public locales, I would not dismiss Fourth Amendment

premise.

[416] Instances in which technological tools can access information about public matters that are not physically enclosed but are inaccessible to ordinary human senses could undoubtedly be multiplied. For example, some items located in public places are too small or too distant to be seen by human eyes from lawful vantage points. Details about those items can be brought within range of perception by high-powered devices that dramatically improve human vision or by mechanisms that bestow "night vision," making it possible to see matters in public places that human eyes could not otherwise see because they are concealed by "cover of darkness."

threshold claims out of hand based on the dubious assumption that privacy interests worthy of constitutional protection cannot exist in public domains.

It is far from clear how the Framers would have reacted to the situations hypothesized. When novel devices afford access to matters that previously could have been perceived only by physical intrusions into concededly private places, one can logically infer that the Framers would have subjected the technological alternatives to constitutional regulation. When mechanisms enable the authorities to uncover matters that could not have been learned by any means known to those who lived in the late eighteenth century, the same conclusion does not necessarily follow. The details learned by the new mechanisms remained private because it was not possible to perceive them. Because there was no means of gaining access, there was no need to contemplate or provide legal protection. As a consequence, we are left without insight into whether our ancestors valued the secrecy or confidentiality of the information that technology has brought within reach.

I am uncertain whether those who valued the privacy of information concealed behind physical barriers would have also valued the privacy of publicly-situated, but imperceptible information. If government agents had devised means of hearing remote, lowered voices or of seeing tiny details or matters hidden by darkness, would the Framers have cared about the confidentiality lost enough to subject those new methods to constitutional control? If those same agents suddenly had acquired superhuman tracking powers analogous to those provided by beepers and could make comprehensive and detailed records of public movements too complicated to be reliably documented by ordinary human trackers, would the Framers have cared about the secrecy lost enough to restrain those new powers?

While I have no ready answers to these difficult questions, I believe they are the sorts of inquiries that need to be pursued. When technology enables the authorities to learn "public" details of our lives that they previously could not have learned, when it renders us poorer from a privacy standpoint than we would have been in an earlier age, we should not deny constitutional protection without close, careful analysis of the ramifications. If the interests jeopardized by technological sense enhancements are sufficiently like those the Framers did value, constitutional

regulation seems justifiable.[417] Simple reliance on public location alone is no substitute for the scrutiny essential to honor Fourth Amendment objectives.

In sum, the Supreme Court's threshold technology opinions have placed unwarranted reliance on locational variables.[418] The emphasis on the importance of home privacy has prompted vigilance against technological incursions on homes, but has cast an unfortunate shadow over other protected domains.[419] Moreover, the instinctive tendency to treat entitlements to privacy in public places as nonexistent permits technological ingenuity to imperil values that may well deserve constitutional protection. In *Katz*, Justice Stewart declared that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase `constitutionally protected area'"[420] and that "the Fourth Amendment protects people, not places."[421] I have always found these pithy declarations to be catchy, but not particularly instructive. I now believe that they capture important constitutional insights, reflecting an acknowledgment that we do have constitutional entitlements to confidentiality outside our homes, even in phone booths and other public places, and a recognition that the Fourth Amendment's reach should not be restricted based on the site of the privacy interest jeopardized by technology.[422] Put simply, the guarantee against unreasonable searches is concerned with technological encroachments upon the privacies of life both inside and outside our castles.

---

[417] I am inclined to put the burden on those who believe that "public privacy" is entitled to no constitutional shelter to provide persuasive reasons why those who sought to preserve an entitlement to keep conversations, letters, and other details confidential inside homes, pockets, and other enclosures would not have cared at all about similar confidentiality interests once they are taken into public places.

[418] *See supra* notes 366-417 and accompanying text.

[419] *See supra* notes 367-85 and accompanying text.

[420] *Katz*, 389 U.S. at 347, 350.

[421] *Id.* at 351.

[422] Justice Harlan agreed that the Fourth Amendment protects people, not places, but noted that determination of the protection afforded ordinarily requires reference to a place. *Id.* at 361 (Harlan, J., concurring). His meaning may have been that there are relevant threshold variables that are intimately related to the nature of the place involved. I do not dispute that position. To the extent, for example, that genuine knowing exposure results from behavior in a public setting, the claim that privacy has been violated is undermined. My criticism of the Court's analyses is directed at the tendency to rely on location alone to restrict the scope of constitutional shelter against technology.

IV. REFLECTIONS UPON AND A PROPOSAL FOR DEFINING THE

RELATIONSHIP BETWEEN TECHNOLOGY AND THE FOURTH AMENDMENT THRESHOLD

Having explored the complexities of the Supreme Court's threshold technology opinions and the understandings of the relationship between technology and the Fourth Amendment implicit in those opinions, it is time to reflect on a few aspects of the central question and to propose a general standard for deciding when technological exploitation ought to be governed by the Fourth Amendment. My aim throughout is fidelity to the aims of those who designed and adopted that provision. In my view, the objective should be to safeguard the interests our ancestors valued, giving force and effect to the balances they struck.[423] Our own biases or desires for greater privacy or security or our resentments of technological innovations and their impacts upon our lives should not be allowed to distort the boundaries of the Fourth Amendment by expanding that provision's reach. On the other hand, fears of or desires to tame particular threats to society–the drug epidemic or terrorism, for example–should not prompt us to contract the scope of Fourth Amendment protection by ignoring the real threats to freedom posed by novel surveillance mechanisms. My preference is to trust the wisdom of those who designed our Constitution.[424]

At the outset, this devotion to original values prompts me to take issue with a potential concession implicit in the *Kyllo* opinion. Justice Scalia asserted that the overarching "question . . . is what limits there are upon th[e] power of technology to shrink the realm of guaranteed privacy."[425] If his intent was to concede that the mere development of technological tools *should* be allowed to diminish Fourth Amendment freedoms, then I respectfully disagree. I see no reason why our cleverness and creativity in increasing human abilities should lead to any constriction of

[423] The goal should be "to preserve that degree of respect for the privacy of persons . . . that existed when the [Fourth Amendment] was adopted–even if a later, less virtuous age should become accustomed to considering all sorts of intrusion `reasonable.'" Minnesota v. Dickerson, 508 U.S. 366, 380 (1993) (Scalia, J., concurring).

[424] Adherence to the values and objectives of the Framers can be an elusive goal. In many ways, the world we inhabit and the society we know would have been alien to those who lived more than two centuries ago. Technological developments of the past two centuries, both simple and elaborate, could scarcely have been the subjects of their dreams. It can be difficult to determine how they would have resolved questions that confront us today. Nevertheless, we should make every effort to seek guidance in their aspirations and goals and should be prepared to confess uncertainty when it is the result of our effort.

[425] Kyllo v. United States, 533 U.S. 27, 34 (2001).

fundamental values. Perhaps Justice Scalia did not mean to suggest that the law should allow technology itself to shrink the scope of Fourth Amendment privacy. He may have meant to express the less troubling idea that no matter how hard we try to safeguard Fourth Amendment privacy, technology will inevitably have some corrosive impacts. I might well agree with that assessment of reality. It is also possible that Justice Scalia merely meant to acknowledge that the current law has tolerated a certain amount of technologically-induced shrinkage. That conclusion seems beyond dispute.[426] Justice Scalia's meaning may have been even more complex. He might have meant that there are situations in which not simply the fact that technology exists, but that fact coupled with other circumstances, justify some diminution of the privacy that would have found shelter in an earlier age. I do not rule out that possibility.

My sole dispute is with the suggestion that the development of mechanisms that enhance perceptual, sensory and other faculties requires the surrender of any of the legal protection for privacy that the Bill of Rights was designed to provide.[427] Technological increases in human abilities to breach confidentiality are an insufficient reason to compromise the effort to preserve original values. I find it inconceivable that the Framers would have expected (or desired) scientific or technological circumvention of fundamental protections. Consequently, I would respond to the question highlighted by Justice Scalia in simple, straightforward terms: Science and technology have *no* inherent power to shrink the domain of privacy guaranteed by the Constitution. We should be vigilant against that danger and determined to interpret the law in ways that prevent it from happening.

That conclusion leads me to another basic, still quite general, assumption about the relationship between innovative devices and the Fourth Amendment threshold. In my view, the guarantee against unreasonable searches and

[426] *See* ROSEN, *supra* note 118, at 25 ("It is surprising how recently changes in law and technology have been permitted to undermine the sanctuaries of privacy that Americans took for granted throughout most of our history.").

[427] *See* ROSEN, *supra* note 118, at 25 ("There is nothing inevitable about the erosion of privacy, just as there is nothing inevitable about its reconstruction. We have the ability to rebuild private spaces we have lost. But do we have the will?").

seizures should constrain every official use of technology that threatens injury to the interests underlying that guarantee. Exploitations of scientific and technological tools should be regulated when they jeopardize the vitality of the liberties the Fourth Amendment is designed to shelter. Technological threats to the core constitutional interest in informational privacy should be of particular concern.[428]

To determine whether Fourth Amendment values are jeopardized, a useful initial step is an evaluation of the character of the augmentation of human capacities made possible by a particular mechanism. Devices that enhance ordinary human sensory faculties in ways that render information about people's lives more accessible should presumptively be objects of Fourth Amendment concern. Because innovations within this category have the power to breach legitimate interests in secrecy, they threaten entitlements to informational privacy that the Framers valued. The mere fact that a device is *capable of* intruding upon Fourth Amendment interests should not, however, be enough to trigger the application of that guarantee. The determinative question should be whether officials have *actually employed* the mechanism in ways that threaten genuine interests in confidentiality.

Based on these premises and the lessons learned from the threshold technology precedents, I have arrived at the following proposal: Official exploitation of a scientific or technological device should be considered a Fourth Amendment search at least when the effect is to enhance, augment or supplement human sensory abilities or other capacities in ways that have made it possible for the authorities to gain access to any information that otherwise would have been, or is highly likely to have been, imperceptible or inaccessible or would only have been, or is highly likely only to have been, perceived or acquired by

[428] This assumption is far from remarkable and hardly novel. It underlies the conclusion in *United States v. Karo*, 468 U.S. 705 (1984), that monitoring a beeper inside a residence constitutes a search because, from a privacy standpoint, it is an effective surrogate for official presence within the home. *Karo*, 468 U.S. at 719. Similarly, the *Kyllo* Court's conclusion that thermal imaging of a residence is a search because it reveals confidential information about the interior seems rooted in an assumption that technology must be regulated when it jeopardizes the values sheltered by the Fourth Amendment. These two decisions do reflect an understanding of the relationship between technology and the reach of the Fourth Amendment similar to the one I proffer. I am not sure, however, that the Supreme Court would subscribe to my expansive statement of the underlying premise. The opinions in *Karo* and *Kyllo* are clearly limited to invasions of home interior privacy. *See supra* notes 168-73, 196-201 and accompanying text.

means that are governed by the Fourth Amendment.[429] Several facets of this standard merit comment and explanation.

The proposed standard rests squarely on the premise about Fourth Amendment purposes and values endorsed in *Katz* and reinforced in subsequent opinions–*i.e.*, that the goal of the Framers was to preserve an interest in privacy.[430] More specifically, it accepts the conclusion that the Framers were primarily concerned with informational privacy–*i.e.*, with safeguarding the entitlement to keep matters about our lives secret from the government.[431] This seems to me a

[429] The proposed standard certainly bears similarities to the narrower standard adopted by the *Kyllo* Court for technological invasions of home privacy. *See Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical `intrusion into a constitutionally protected area,' constitutes a search–at least where . . . the technology in question is not in general public use.") (citation omitted); *id.* at 40 ("Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a `search' and is presumptively unreasonable without a warrant."). There is reason to believe that the Court's doctrine may have been inspired by the suggestion made in the *amicus curiae* brief I prepared in *Kyllo*. *See* Brief Amicus Curiae of the National Association of Criminal Defense Lawyers and the American Civil Liberties Union at 27, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508) ("At a minimum, the Fourth Amendment is implicated whenever a device enables officials to breach protected interests in secrecy and confidentiality by learning concealed information that previously could have been learned only by means of physical entry into a home or other enclosed space."); *id.* at 5-6 ("At a minimum, a technological advance that is an effective substitute for physical intrusion and poses the same threats to privacy should be governed by the Fourth Amendment. A new device must be constrained by the Constitution whenever it enables officials to learn any confidential information that previously could have been learned only by . . . physical intrusion."). The standards proposed in the brief and here are both broader than that adopted by the Court insofar as neither is restricted to home interior contexts. In addition, the *Kyllo* brief argued that "[a]t a minimum" the Fourth Amendment should govern the situations described by the standard proposed, and the standard put forward in this article calls for constitutional control "at least" in the situations it encompasses. Neither is intended as an *exclusive* threshold test. Both contemplate the possibility of additional situations in which government conduct may qualify as searches if Fourth Amendment values are threatened. It is arguable that the *Kyllo* standard itself is not an exclusive threshold standard for home interior contexts–*i.e.*, that conduct not satisfying the majority's standard could still qualify as a Fourth Amendment search.

[430] *See* Rakas v. Illinois, 439 U.S. 128, 160 (1978) (White, J., dissenting) (asserting that the "primary object of the Fourth Amendment" safeguard against unreasonable *searches* "[is] . . . the protection of privacy" (quoting Cardwell v. Lewis, 417 U.S. 583, 589 (1974) (plurality opinion) (alteration in original)).

[431] *See* Tomkovicz, *supra* note 19, at 665-66. This is not to say that the guarantee against unreasonable searches protects *only* confidentiality interests. I have already noted that there may be other "privacy" interests–such as the

plausible understanding of the ambitions behind constraining physical intrusions into homes and other domains.[432]

In addition, while I believe that the reasonable expectation of privacy doctrine has many flaws, deficiencies and inadequacies,[433] the proposed standard can coexist peacefully with that doctrine. It is not a rival or competitor, but a supplement, *i.e.*, an effort to furnish more specific guidance for the resolution of issues raised by technological developments.

Next, the proposal provides for the regulation of devices that heighten perceptive abilities (*e.g.*, listening devices) as well as those that make ordinary human perceptive abilities more effective (*e.g.*, airplanes). In terms of jeopardy to secrecy, I see no difference between keener senses and improved vantage points for normal senses. Both sorts of enhancement can increase access to otherwise inaccessible information about our lives.

It merits mention that the proposed formulation contains no limitation based on the character of the location or area targeted. Homes are not singled out for special protection. Other concealed spaces receive constitutional shelter. Even public locales are candidates for coverage. Location *alone* does not factor into the analysis.[434]

Unlike the current doctrine, the standard contains no restriction based on the content of the confidential details rendered accessible. Before the advent of technologies capable of discerning only confidential facts that might be deemed insignificant or illegitimate, those facts were protected by the Fourth Amendment. I have seen no evidence that the Framers meant to exclude such information from the

interest in the integrity and dignity of one's person and the interest in quiet repose–that were the objects of Fourth Amendment protection. The proposal in this article focuses on the protection of the core interest in informational privacy. In recognition of the possibility that other interests merit Fourth Amendment protection, the proposal specifies that technological exploitation qualifies as a search *at least* in the circumstances described. Fourth Amendment application in additional, appropriate situations is not precluded.

[432] Over eighty years before the *Katz* revolution, in its first significant Fourth Amendment threshold decision, the Court recognized "the privacies of life" as an object of that provision's protective scheme. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

[433] See Tomkovicz, *supra* note 19, at 678-90, for criticisms of the reasonable expectation of privacy doctrine.

[434] That is not to say that location is irrelevant. The site of a particular activity or object that is the target of technological surveillance may well affect whether the information acquired is otherwise accessible by unregulated human senses.

shelter provided by that guarantee.[435] While I would incorporate an appropriate limitation if persuasive evidence were forthcoming, at present I would not suspend the protection that existed at the time the Constitution was adopted.

Perhaps one of the more significant features is the proposal's regulation of devices in two distinguishable instances. Technological developments are brought under Fourth Amendment control when the information they render accessible would only have been accessible by means that would clearly have triggered Fourth Amendment scrutiny–*i.e.*, when the technology is a substitute for a physical intrusion or any other constitutionally-regulated action.[436] My proposal also calls for the regulation of devices that make it possible for the government to learn information that it could not have learned at all–*i.e.*, information that would have remained confidential, but is now capable of revelation and acquisition by technological means. The use of sensitive microphones to overhear whispered conversations in public places illustrates the latter situation. Prior to the development of electronic eavesdropping technology, such conversations could not have been learned at all. Human limitations rendered their content inaccessible, thus confidential.[437] I have concluded that such privacies–those that could not have been breached at all–are sufficiently like those enclosed by breachable physical barriers to deserve protection.

Situations in which there is a risk of perception of matters by unregulated, unaided human senses raise an extremely difficult issue: Should technological devices be free of constitutional control whenever there is *some chance* that the matters perceived *could* also have been perceived by using ordinary senses and abilities in ways that would not

---

[435] For discussion and analysis of this issue, see *supra* notes 261-81 and accompanying text.

[436] The holdings in *Katz*, *Karo* and *Kyllo* all fall within this category, I believe. In all three cases, the Court found that official uses of technological devices had crossed the threshold because the technologies afforded access to information that could otherwise have been obtained only by conduct that would have triggered Fourth Amendment control–*i.e.*, by physical intrusions into homes or a telephone booth. *See supra* notes 98-114, 168-73, 196-201 and accompanying text.

[437] For a discussion of how the use of electronic tracking beepers to monitor public travels arguably enables officials to learn information that otherwise would be inaccessible to human faculties, see *supra* notes 218-19 and accompanying text.

trigger Fourth Amendment regulation. I have opted for a standard that includes not only situations where it is certain that matters would be inaccessible to unregulated ordinary senses but also situations in which it is "highly likely" that information would have been imperceptible by constitutionally unregulated means. My choice is based on the premise that the Framers would not have found a forfeiture or surrender of all interests in confidentiality in every situation where there is *any risk* that unregulated human perception could gain access to information. It rests on the conclusion that there is constitutionally cognizable damage to privacy when technological sense enhancements dramatically increase the government's opportunities to learn information that ordinary human abilities would have a very small possibility of learning. If the risk of acquisition by unregulated means is sufficiently small, mechanisms that make acquisition certain or probable seem to pose genuine danger to interests in confidentiality. This conclusion requires prescription of the degree of risk of ordinary sense perception that is too small to support a loss of privacy protection against technological means. For the time being, I have incorporated the relatively imprecise phrase "highly likely." According to the proposal, when it is "highly likely" that the matters perceived would not be accessible to unregulated human perception, the chance of ordinary perception is not large enough to permit technology to go uncontrolled.[438]

The proposal is intended to address situations where ordinary senses undoubtedly *could* gain access to the information learned by technological means, but generally are not used by the public to gain such access. It is designed to regulate technology in those situations *only if* the use of ordinary senses to perceive the information would be constitutionally regulated. The proposed standard dictates this result by *not* including uses of technology when it is certain or there is a sizeable risk that the information acquired by the mechanism would have been perceptible or

[438] I admit that there is considerable ambiguity in the phrase "highly likely." Those terms do not identify the level of likelihood with any precision. Consequently, the magnitude of the chance of ordinary perception that occasions a forfeiture of protection against technological means is uncertain. As is often the case with legal standards that address questions of risk, greater specificity and precision in this area do not seem possible. Ultimately, we must trust judges to apply general standards to the best of their abilities. I have no particular attachment to the phrase "highly likely" and would be pleased if a better alternative were offered.

accessible by means *not governed* by the Fourth Amendment. Thus, in deciding whether technology crosses the Fourth Amendment threshold, the critical question is whether the employment of ordinary human faculties would be subject to constitutional control.[439]

Finally, the proposed standard does not include an exception for mechanisms "in general public use." I remain ambivalent about the merits of such an exception. For those persuaded by the arguments in favor of the exception,[440] something along the following lines could be appended to the end of the proposal: "Exploitation of a device is not a search, however, when the device at issue has been widely used by members of the public to enhance perception and acquire information under circumstances that demonstrate societal acceptance of the resulting losses of privacy." As the earlier discussion of the merits of the current "in general public use" exception suggests, such an exception could be defensible *only* if a device has actually been generally used by the public to perceive the information accessed by technological means, if society has had time and opportunity to react to the perils from widespread public use, and if society has evinced a lack of concern with the fact that matters that were once confidential and inaccessible are now being learned by fellow citizens. Only in the undoubtedly rare situations where these criteria are satisfied would it make constitutional sense to

[439] The investigatory conduct addressed in *Bond v. United States*, 529 U.S. 334 (2000)–the use of the sense of touch to ascertain the configuration of the contents of a soft-sided bag–provides a useful illustration. *Bond*, 529 U.S. at 336. According to the *Bond* Court, whether the use of touch in this way is controlled by the Fourth Amendment depends upon the extent and manner of use. *Id.* at 338-39. Official employment of the sense of touch is subject to Fourth Amendment control *if* the tactile manipulation performed exceeds that ordinarily engaged in by members of the public. Under the proposed standard, a technological tool that could discern the shape of contents would constitute a search if the tactile manipulation necessary to learn the same information would be intrusive enough to trigger Fourth Amendment control, but not if the use of touch to access the same details would be unconstrained.

Beeper-aided tracking provides another example. Suppose that the public *could* use ordinary senses and abilities to track all public movements on a journey, but does not generally use unaided faculties to monitor others' movements. The use of an electronic beeper to monitor those movements will be constitutionally regulated *if* the use of unenhanced faculties to track the same movements would be regulated. If the use of ordinary senses and abilities would not be controlled and technology provides access to no more than what those senses could access–technology will not be regulated.

[440] For a discussion of this issue, see *supra* notes 324-66 and accompanying text.

invoke an "in general public use" exception. Consequently, language used to capture such an exception must be carefully phrased to encompass only those rare situations.

At the outset of this project, I was optimistic that I might arrive at a clear, simple, manageable standard for resolving threshold technology questions. The standard I have proposed is somewhat opaque, fairly complex and potentially unwieldy. While not desirable, these characteristics have been necessitated by the intricacies and subtleties of the issues that arise when addressing the relationship between technology and the threshold of the Fourth Amendment. While a simpler standard might be superficially appealing, it could not perform the heavy lifting required. One alternative might have been to abandon the quest for a governing doctrinal standard as an unproductive exercise in futility. I continue to believe, however, that the effort to provide general, consistent guidance is a worthy endeavor. My proposal undoubtedly has flaws, deficiencies, and ample room for improvement. I offer it as a first step toward a more principled regime for resolving threshold technology issues and invite others to assist in its development and refinement.

V. CONCLUSION

For a number of reasons, discernment of the relationship between technology and the threshold of the Fourth Amendment is an exceedingly difficult undertaking. The novel, sometimes ingenious, devices that give rise to constitutional questions were unknown to and unanticipated by those who drafted the Constitution. The conduct these mechanisms make possible often bears little or no ostensible resemblance to the physical intrusions that troubled our ancestors. Nonetheless, the dramatic increases in human capacities they afford can threaten the very same privacy interests that are violated by physical intrusions. Moreover, technological tools sometimes pose novel threats to privacy by enabling officials to gain access to potentially confidential information that was wholly unreachable in an earlier age. Official exploitations of technology challenge us to make difficult distinctions between tools that imperil Fourth Amendment values–those that cloak "old grievance[s]" in "insidious disguises"[441]—and tools that do not implicate the protections of that guarantee. The objective of this article has

[441] Boyd v. United States, 116 U.S. 616, 630 (1886).

been to furnish a principled basis for making these critical distinctions.

The Supreme Court's holdings in threshold technology cases have sometimes been rooted in logically defensible premises that can promote principled decisionmaking. On other occasions, however, they have been based on unsupported and questionable assumptions. The most glaring deficiencies in the Court's opinions have been failures to examine and respond to the subtle, unique and important questions raised by technological enhancements of human potential. Too often, the Court has remained on the surface, ignoring the troublesome intricacies that lie beneath. The analyses and suggestions in this article have been intended to expose the neglected complexities and to prompt the sorts of in-depth analyses necessary for constitutionally legitimate resolutions. While the answers provided here may not be correct, the often unaddressed questions that have been highlighted are significant.

In the years to come, as in years past, technology, terrorism and other powerful forces will bring pressure to bend constitutional rules and restrict fundamental freedoms. These forces have the power to shred the fabric of the Fourth Amendment. The inquiries pursued in this article and in this groundbreaking symposium can yield answers that are faithful to our constitutional heritage and can lead to solutions that will help preserve the delicate, enviable balance between security and freedom that is the very essence of our nation.