Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search

Stephen E Henderson

Available at: https://works.bepress.com/stephen_henderson/4/
Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search

by Stephen E. Henderson*

I. INTRODUCTION

In late 2002 the Pentagon's Defense Advanced Research Projects Agency ("DARPA") launched an ill-named, if not entirely ill-advised, data-mining initiative as part of its response to the terrorist attacks of September 11, 2001. Under the direction of Vice Admiral John M. Poindexter, infamous for his role in Iran-Contra,1 DARPA dubbed the program "Total Information Awareness" ("TIA"). The goal was to amalgamate a mammoth database of existing commercial and governmental information, from Internet mail and calling records to banking transactions and travel documents, which would be analyzed by a to-be developed computer system capable of spotting suspicious behavior.2

* Associate Professor, Widener University School of Law. University of California at Davis (B.S., 1995); Yale Law School (J.D., 1999). I wish to thank Harold Krent, Andrew Leipold, Alan Garfield, and Orin Kerr for their helpful comments on earlier drafts, and Henry Perritt for his general encouragement of related work during my time at Chicago-Kent.

1. Admiral Poindexter was National Security Advisor to President Reagan during Iran-Contra, in which the proceeds of arms sales to Iran were used to covertly support the contras of Nicaragua despite a Congressional directive via the Boland Amendment that federal funds not be used for that purpose. See The Iran-Contra Report: Chronology: After 13 years of Hide-and-Seek, A Bitter Chapter of U.S. History Ends, N.Y. TIMES, Jan. 19, 1994, at A8.

As the brainchild of an office whose motto was "Scientia Est Potentia" ("Knowledge is Power"), the Orwellian connotations of TIA did not go unheeded. In the words of critic William Safire,

Every purchase you make with a credit card, every magazine subscription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database." To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you—passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance—and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen.

As a result of such libertarian concern and aggravated by the choice of Admiral Poindexter to lead the program, Congress ultimately legislated not only TIA's demise, but that of the entire office that spawned the initiative. This will not be the last word, however. Even

3. See William Safire, You Are a Suspect, N.Y. TIMES, Nov. 14, 2002, at A35. DARPA formed the Information Awareness Office ("IAO") to develop new surveillance technologies in response to the attacks of 9/11. See Markoff, Threats, supra note 2. The choice of the ominous moniker "Total Information Awareness" demonstrates a rather remarkable failure to learn from the FBI's decision to dub its electronic surveillance capability "Carnivore." Although allegedly named to demonstrate its selectivity because a carnivore eats only the meat, the name was, unsurprisingly, a public-relations disaster. Following significant and sustained civil libertarian interest and ire, the FBI finally changed the name to the admirably bland DCS-1000 ("digital collection system"). See John Schwartz, Bin Laden Inquiry Was Hindered by F.B.I. E-Mail Tapping, N.Y. TIMES, May 29, 2002, at A16. DARPA similarly belatedly changed the name of its program to "Terrorism Information Awareness," as well as removed an emblem for IAO that featured "a human eye, embedded in the peak of a pyramid, scanning the globe." Ariana Eunjung Cha, Pentagon Details New Surveillance System, WASHINGTON POST, May 21, 2003, at A6; John Markoff, Poindexter's Still a Technocrat, Still a Lightning Rod, N.Y. TIMES, Jan. 20, 2003, at C1.


now much of the TIA framework continues under other names in other agencies, and private entities are hard at work gathering data for similar private initiatives.\(^6\) In the words of Admiral Poindexter, "It's very important that this research be continued. I think it eventually will be. I'm an optimist."\(^7\)

While databases such as TIA are only one of many significant threats to privacy and information security in the twenty-first century,\(^8\) the concept of TIA (merely collecting what was voluntarily provided to third parties) and the strident and swift political response (against a database in which we would all be included) have lessons for how we should think about the Fourth Amendment\(^9\) in a world of amazing but intrusive technology. The Fourth Amendment's prohibition against unreasonable searches and seizures\(^10\) is only relevant to certain activity. When

---


9. U.S. CONST. amend. IV.

10. The Fourth Amendment provides that

(It)he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.
employers and other private individuals conduct surveillance, or ask us to trade our privacy for a perk, the Fourth Amendment is not implicated. If the government desires to commit a similar intrusion into our privacy, but we consent, the Amendment provides no restraint. But even outside these longstanding limitations, a real risk exists that Supreme Court jurisprudence defining a "search" may render the Amendment increasingly irrelevant.

The Fourth Amendment is only implicated when the government invades our "reasonable expectation of privacy." According to the Supreme Court, we retain no reasonable expectation of privacy in what we knowingly expose to the public. As technology dictates that more and more information regarding our personal lives is available to anyone equipped to receive it, and as social norms dictate that more and more information is provided to third parties, this restriction threatens to render the Fourth Amendment a practical nullity. The current definition of what constitutes a Fourth Amendment search was crafted in light of one developing technology, the telephone networks. Now is the time to craft a definition that accommodates the amazing but intrusive technologies of the twenty-first century.

This Article will first review the genesis of the "reasonable expectation of privacy" ("REP") requirement, both to establish the governing legal

11. See, e.g., Bedell, Got the Funny Feeling, supra note 8; Your Staff are the Weakest Link, COMPUTING, May 6, 2004, available at 2004 WL 62911377 (describing non-scientific study in which approximately three-quarters of those asked were willing to provide their passwords for a chocolate bar); Mike Musgrove, Search Is On for Gmail Names, WASHINGTON POST, May 21, 2004, at E1 (describing widespread willingness to pay for a desirable address on a forthcoming free e-mail service despite its content being monitored for advertising purposes); Tom W. Bell, Internet Privacy and Self-Regulation: Lessons from the Porn Wars, 65 CATO INSTITUTE BRIEFING PAPER, Aug. 9, 2001, at 3 (describing the disconnect between Internet users alleged concern for privacy and their actions); Go on, Watch me: People are Voluntarily Surrendering Their Privacy, ECONOMIST, Aug. 17, 2003, at 12.


This Court has also consistently construed this [Fourth Amendment] protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.

Id. (internal quotation marks omitted).

13. See Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). "It is . . . well settled that one of the specifically established exceptions to the requirements of [the Fourth Amendment] is a search that is conducted pursuant to consent." Id. (citing Davis v. United States, 328 U.S. 582, 593-94 (1946)).

14. Id. at 277.

15. See Section III, infra.
framework and to demonstrate how changing technology has altered our conception of the Fourth Amendment search in the past. This includes the “third party cases,” in which the Supreme Court articulated and developed the doctrine that one retains no reasonable expectation of privacy in information provided to a third party.

This Article then examines a pressing and undecided issue that helps to frame the need for doctrinal clarification, namely whether there is a reasonable expectation of privacy in electronic mail in unencrypted and encrypted form. This analysis and an examination of several developed and developing technologies, make clear that the “third party doctrine” must be strictly construed if the Fourth Amendment is to meaningfully limit government intrusions. “Knowing exposure” should not remove information from the protection of the Fourth Amendment, but rather only affirmative desire that content be utilized by a third party. This will avoid the dangerous incentive effect in which those very searches receiving little to no Fourth Amendment protection are also becoming cheaper to perform.

With the reasonable expectation of privacy doctrine so limited, or even jettisoned altogether in favor of a dictionary definition of “search,” courts can properly turn their focus to what intrusions are “reasonable.” This Article concludes by examining three potential guideposts in this determination: government need, political process checks, and use limitations.

II. FROM OLMSTEAD TO KATZ—THE GENESIS OF THE “REASONABLE EXPECTATION OF PRIVACY”

Olmstead v. United States16 came before the Supreme Court during Prohibition in 1928. Although Prohibition itself was relatively short-lived, at least as a national policy,17 the issue confronted by the Court remains contentious—how should the Fourth Amendment’s prohibition against “unreasonable searches and seizures” be applied to novel technologies not available to, and perhaps not even conceivable to, the Framers.18

17. Prohibition, ushered in by the Eighteenth Amendment to the Constitution (1919), was repealed by the Twenty-First Amendment in 1933. Some states, however, maintained their prohibition laws until the 1960s. See “Prohibition,” WEBSTER’S INTERNATIONAL ENCYCLOPEDIA (1999).
18. For an excellent discussion of this general topic, see Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY L.J. 869 (1996). That the Supreme Court only addressed the issue of wiretapping telephone conversations in 1928, some 50 years after the invention of the telephone, makes it unsurprising that the application of the Fourth
The criminal scheme in Olmstead was of "amazing magnitude," involving the importation and sale of liquor on a massive scale.\(^{19}\) Over seventy individuals were indicted, including Roy Olmstead, who acted as "general manager" and received half of the operation's profits. An operation of this scale required ample means of communication, which were provided via telephone. Three lines led into the organization's main office, at which someone was always present to take orders, and Olmstead and his co-conspirators also placed and received calls from their respective residences.\(^{20}\)

Federal agents obtained much of their evidence from this relatively state-of-the-art communications system. The agents tapped the lines running from the residences and the main office.\(^{21}\) While these taps could have been conducted within the boundaries of defendants' property, none of them were. The residential taps were made in the streets near the homes, and the taps for the office lines were made in a basement in which defendants had no property interest.\(^{22}\)

Based on the Fourth Amendment language protecting "[t]he right of the people to be secure in their persons, houses, papers, and effects,"\(^{23}\) the Court stated "[t]he amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects."\(^{24}\) This language easily encompasses some modes of communication, such as

Amendment to many current technologies remains undecided. The wheels of justice often turn slowly, which some have argued is reason to turn to Congress rather than judicial interpretation of the Constitution when technology interacts with privacy. \textit{See} Orin S. Kerr, \textit{The Fourth Amendment in New Technologies: Constitutional Myths & the Case for Restraint}, 102 Mich. L. Rev. 801-88 (2004). Ultimately, however, it is the duty of the courts to say what the law is, especially when it comes to interpreting the Constitution.

19. 277 U.S. at 455-56.

It involved the employment of not less than 50 persons, of two sea-going vessels for the transportation of liquor to British Columbia, of smaller vessels for coastwise transportation to the state of Washington, the purchase and use of a branch beyond the suburban limits of Seattle, with a large underground cache for storage and a number of smaller caches in that city, the maintenance of a central office manned with operators, and the employment of executives, salesman, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney. In a bad month sales amounted to $176,000; the aggregate for a year must have exceeded $2,000,000.

\textit{Id.} at 456. It enjoyed the assistance of some members of the Seattle police. \textit{Id.} at 457.


21. \textit{Id.} Monitoring of these phone lines was extensive. It extended over a period of nearly five months, and agents' typewritten record of the substance of monitored conversations reached 775 pages in length. \textit{Id.} at 471 (Brandeis, J., dissenting).

22. \textit{Id.} at 457.

23. U.S. CONST. amend. IV.

as a letter sent via the United States Post Office because "[t]he letter is a paper, an effect." In the opinion of the Court, however, it was equally clear that this language did not encompass the mode of communication at issue, namely the transmission of the human voice via an analog electronic signal. The Court stated, "The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only." The outcome may have been different had the tapping of the phone lines been accomplished via entry onto the defendants' property, and hence threatened the security of their "houses." Here, there was no such entry, and according to the Court,

[t]he language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched . . . . [Conversations] passing over [telephone wires] are not within the protection of the Fourth Amendment.

Thus, the Court adopted what has come to be termed the "property-based" or "trespass-based" conception of the Fourth Amendment: if there was no encroachment on a defendant's property interest, there could be no violation of the Fourth Amendment.

Fearing that the Court had overlooked the necessity of adapting constitutional guarantees to a changing world, Justice Brandeis, in dissent, presciently worried that "[w]ays may some day be developed by

25. Id. (discussing Ex Parte Jackson, 96 U.S. 727 (1877), which held that the Fourth Amendment protects sealed letters released to the United States Postal Service for delivery).
26. Id. at 465.
27. Id. at 464.
28. See id. (emphasizing that "[t]here was no entry of the houses or offices of the defendants"). Even had there been some trespass, Olmstead may not have prevailed, however, based on the Court's characterization of an earlier decision as holding that despite a trespass, there was no search when government agents merely utilize their sense of hearing. Id. at 465 (describing Hester v. United States, 265 U.S. 57, 58 (1924)).
29. Id. at 465-66.
30. Id. at 466.

Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his 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.

Id.
which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."\(^{31}\) Although some of Justice Brandeis's concerns were perhaps unrealistic,\(^ {32}\) technological developments since 1928 have given continued credence to his basic assertion that "[d]iscovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."\(^ {33}\)

Despite Justice Brandeis's impassioned and eloquent dissent,\(^ {34}\) the property-based conception advanced in \textit{Olmstead} remained persuasive to a majority of the Court. The contours of that doctrine are demonstrated by two subsequent decisions. In \textit{Goldman v. United States},\(^ {35}\) federal agents had access to the office space adjoining the office of one of the defendants.\(^ {36}\) In order to overhear conversations occurring within the defendant's office, agents entered his office without his knowledge and installed a listening device that was wired into the adjacent space through the connecting wall. When that device failed to operate, however, the agents instead relied on a "detectaphone," a device that, when placed on the agent's side of the wall, was able to detect and

\begin{footnotes}
\item[31.] \textit{Id.} at 474 (Brandeis, J., dissenting). Justices Holmes, Butler, and Stone also dissented. \textit{See id.} at 469 (Holmes, J., dissenting); \textit{id.} at 485 (Butler, J., dissenting); \textit{id.} at 488 (Stone, J., dissenting). Chief Justice Taft delivered the majority opinion.
\item[32.] Justice Brandeis posited that "[a]dvances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." \textit{Id.} at 474 (Brandeis, J., dissenting).
\item[33.] \textit{Id.} at 473 (Brandeis, J., dissenting).
\item[34.] His dissent includes this famous passage:

\begin{quote}
[It] is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.
\end{quote}

\textit{Id.} at 479 (Brandeis, J., dissenting). Justice Brandeis concluded with these words: Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means—to declare that the government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.
\item[35.] \textit{Id.} at 485 (Brandeis, J., dissenting).
\item[36.] 316 U.S. 129 (1942).
\item[36.] \textit{id.} at 131. The three defendants were attorneys convicted for conspiring to defraud creditors in a bankruptcy proceeding. \textit{id.} at 130-31.
\end{footnotes}
amplify the sound waves resulting from the conversation taking place in the adjoining room.\textsuperscript{37}

Based on the reasoning from \textit{Olmstead}, the use of the listening device might have violated the Fourth Amendment because it had been installed via a trespass. The Court, however, did not have to reach this issue because the device was inoperable and, therefore, never used. As to the detectaphone, there was no trespass to any protected space, and there was no examination of any person, paper, or effect. Hence no search occurred for purposes of the Fourth Amendment.\textsuperscript{38}

In \textit{Silverman v. United States},\textsuperscript{39} the police again eavesdropped through a party wall. This time, however, they used a "spike mike," a microphone which penetrated a few inches through the wall and came to rest against the ducting of the defendant's home.\textsuperscript{40} Although the court below had followed \textit{Goldman}, refusing to draw a distinction based on such a minute intrusion, the Supreme Court was not similarly persuaded.\textsuperscript{41} The Court stated the "decision here . . . is based upon the reality of an actual intrusion into a constitutionally protected area . . . . We find no occasion to re-examine \\textit{Goldman} here, but we decline to go beyond it, by even a fraction of an inch."\textsuperscript{42}

While \textit{Silverman} was in one sense a straightforward application of the property-based conception, it was also a departure from \textit{Olmstead}'s insistence that the examination of a tangible object was required to constitute a search.\textsuperscript{43} The arbitrariness of the Court's remaining bright-line rule did not go unnoticed. Justice Douglas, in concurrence, questioned the results of \textit{Goldman} and \textit{Silverman} when "the invasion of

\begin{footnotes}
\item[37] Id. at 131.
\item[38] Id. at 134-36. The Court had no desire to reconsider \textit{Olmstead}:
That case was the subject of prolonged consideration by this [C]ourt. The views of the [C]ourt, and of the dissenting justices, were expressed clearly and at length.
To rehearse and reappraise the arguments pro and con, and the conflicting views exhibited in the opinions, would serve no good purpose. Nothing now can be profitably added to what was there said.
\textit{Id.} at 135-36. Two justices in dissent agreed with this premise. Justice Murphy added a substantive dissent largely mirroring that of Justice Brandeis in \textit{Olmstead}. See id. at 136-42 (Murphy, J., dissenting). See id. at 136 (Stone, C.J. and Frankfurter, J., dissenting).
\item[40] Id. at 506-07. The defendants were operating an illegal gambling operation. \textit{Id.} at 506.
\item[41] Id. at 512.
\item[42] Id.
\end{footnotes}
privacy is as great in one case as in the other." Six years later in *Katz v. United States*, Olmstead's conception would suffer its final demise.

In *Katz* law enforcement once again sought to use technology to obtain evidence, this time by placing an electronic listening device, or "bug," on the outside of a public telephone booth. The Ninth Circuit, following *Olmstead, Goldman*, and *Silverman*, concluded that no Fourth Amendment violation occurred because "there was no physical entrance into the area occupied by [Katz]." Even such an intrusion would be of no import if a public telephone booth was not a protected space. Therefore, the first of Katz's questions presented before the Supreme Court asked whether a public telephone booth is a constitutionally protected area. The Court "decline[d] to adopt this formulation," speaking as if Katz should have known better: "In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"

Magnanimously, the Court was able to disregard the "misleading way the issues [had] been formulated," explaining that "this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places." Surely this would have come as a surprise to Olmstead and Goldman, but the Court held that those cases were no longer good law: "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."

---

46. *Id.* at 348. Like in *Silverman*, Katz was engaged in illegal gambling, here in violation of the federal Wire Wager Act, 18 U.S.C. § 1084 (1961). *Id.*
47. *Katz v. United States*, 369 F.2d 130, 134 (9th Cir. 1966).
48. *Id.* at 133.
50. *Id.* at 351.
51. *Id.* at 353. The Court asserted that "the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Id.* There was intervening precedent, such as the decision of *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967), which stated "[t]he premise that property interests control the right of the Government to search and seize has been discredited." *Id.* But that language was used in a different context, the seizure of mere evidence, and the decision was handed down only months before *Katz* was argued. It was certainly not unexpected, and seemingly not unreasonable, for Katz to have relied on the directly analogous precedent of *Goldman* and *Silverman*, despite the Court's implications to the contrary. And as Justice Harlan explained in his concurring opinion, the *place* intruded upon is still very relevant: "As the
Unfortunately, the Court did not clearly articulate a new test to replace the property-based conception, stating only that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." Thus, the test for what constitutes a Fourth Amendment "search" instead comes from Justice Harlan's concurrence: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Because the first requirement is often difficult to determine and is subject to government manipulation—for example a law enforcement announcement that all homes will hereafter be subject to random inspections—the second requirement has become determinative.

Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

Justice Harlan succinctly noted that "[Goldman's] limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion." *Id.* at 362.

52. *Katz*, 389 U.S. at 353. The Court did go on to hold that the search and seizure were unconstitutional absent judicial authorization. *See id.* at 354-59.

53. *Id.* at 361 (Harlan, J., concurring). Despite the majority's failure to clearly articulate a new test, both elements of this test can be found in its opinion. *See Smith v. Maryland*, 442 U.S. 735, 740 (1979)

"(The first question) is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy—whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve (something) as private.' The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is 'justifiable' under the circumstances").

*Id.* (internal citations omitted).

54. *See Smith*, 442 U.S. at 740 n.5; *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974). The Court seems to indiscriminately waffle between phrasing the requirement a "reasonable" expectation of privacy and a "legitimate" expectation of privacy, leaving uncertain whether the test is meant to be empirical, as suggested by the former term, or normative, as suggested by the latter. *See, e.g.*, *Smith*, 442 U.S. at 740, 743-44 (using both terms interchangeably). *See also California v. Ciraolo*, 476 U.S. 207, 219 n.4 (1986).

In Justice Harlan's classic description, an actual expectation of privacy is entitled to Fourth Amendment protection if it is an expectation that society recognizes as "reasonable." Since *Katz*, our decisions also have described constitutionally
Thus in 1928 when the Supreme Court first encountered the relatively novel technology of telephone wiretapping, it held the practice did not constitute a Fourth Amendment search. At that time approximately forty-one percent of U.S. households were equipped with telephone service. But by 1967, when eighty-seven percent of households were so equipped, the Court, influenced by the increasing prevalence and importance of the telephone in society, reversed course:

[A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

That technology should inform what constitutes a Fourth Amendment search is therefore not novel. The remaining question, which is a hard one, is precisely what that effect should be.

III. THE "THIRD PARTY DOCTRINE"

In order to understand how the reasonable expectation of privacy ("REP") criterion of Katz applies to modern technology, it is necessary to examine a second line of cases in which the Supreme Court developed what can be termed the "third party doctrine." The first of these cases, Hoffa v. United States, was decided a year before Katz.
Notorious labor leader James ("Jimmy") Hoffa and his co-defendants were convicted for their attempts to bribe members of a criminal jury. Perhaps the most damning testimony was that of Edward Partin, a fellow Teamster who testified to his conversations with Hoffa and a co-defendant and who had acted as an informant to the government while events were unfolding.

Partin's assistance was not motivated by altruism; he was facing state and federal indictments of his own, and he had been in contact with federal agents prior to his initial meeting with Hoffa. Following his service, Partin's wife received $1200 in government funds and the pending criminal charges against him were never pursued. The Court accepted that Partin was a government agent prior to his first meeting with Hoffa and that he was compensated for that service. Hoffa argued that the use of such a "secret informer" violated the Fourth Amendment.

The Court held otherwise: "Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it . . . . [N]o right protected by the Fourth Amendment was violated in [this] case." Although Hoffa was decided before Katz, and therefore, before the REP test definitively replaced the property-based conception, the Court reiterated the doctrine in United States v. White, a similar "false friend" case. Thus, despite

61. The jury was empanelled to decide whether James Hoffa had violated the Taft-Hartley Act. The case ended in a hung jury. Hoffa, 385 U.S. at 294.
62. Id. at 295.
63. Id. at 297-98. At least some of these pending charges were serious, including embezzlement, kidnapping, and manslaughter. See id. at 317-18 (Warren, C.J., dissenting). In Chief Justice Warren's opinion, the payments were made to his wife in order to obfuscate their true source. See id. at 319 (Warren, C.J., dissenting).
64. Id. at 299. The government claimed the payment was merely reimbursement for Partin's out-of-pocket costs, and the failure to pursue charges against Partin had no necessary relation to his assistance. Id. at 298. Although the lower courts found ample support for these contentions, the Supreme Court chose to presume Partin was a government mole, presumably because that was the best scenario for the defendants, but it still proved unavailing. See id.
65. Id. at 295. Hoffa also alleged violations of his Fifth and Sixth Amendment rights. Id. at 295, 309-10.
66. Id. at 302-03.
67. 401 U.S. 745 (1971). Although there was no majority opinion in White, the Court determined there is no Fourth Amendment violation when an informant wears a wire that
obtaining the same information that might otherwise be obtained via a bug, which would constitute a Fourth Amendment search according to *Katz*, there is no protection from false friends.\(^{68}\)

The third party doctrine was further elucidated in *United States v. Miller*\(^{69}\) and *Smith v. Maryland*.\(^{70}\) Recognizing the desirability of banking records for government investigations, the Bank Secrecy Act of 1970\(^{71}\) required banks to maintain records of customer transactions.\(^{72}\) When federal agents obtained Mitchell Miller's records via grand jury subpoena, Miller moved to suppress the evidence for violation of his Fourth Amendment rights.\(^{73}\) Despite the fact that banks were required to preserve this information, and that Miller had no choice but to surrender the information to the bank in order to transact business there, the Court found the third party doctrine controlling: "[Miller] had no protectable Fourth Amendment interest in the . . . documents."\(^{74}\) As in *Hoffa* and *White*, a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."\(^{75}\)

In *Smith* the Court returned to the telephone network. When the victim of a robbery began to receive obscene and harassing phone calls, apparently from the perpetrator, police requested that the telephone company place a pen register on the suspect's home phone line. That device recorded all phone numbers dialed from the defendant's residence, contemporaneously transmits his conversations to agents. *See id.* at 746-47, 754. Arguably the Court also reaffirmed the "false friend" doctrine in *Katz* itself: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S. at 351 (internal citations omitted).

70. 442 U.S. 735 (1979).
73. *Id.* at 437. The government used the bank records in its prosecution against Miller for failure to pay required taxes on the manufacture of alcohol. *Id.* at 436.
74. *Id.* at 437.
75. *Id.* at 443. The Court went on to reiterate that

[...]this Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

*Id.* (citing, inter alia, *White* and *Hoffa*).
thus, verifying that he was the caller of interest.\textsuperscript{76} The Court held that a caller has no reasonable expectation of privacy in the numbers dialed from his or her home telephone, and therefore, that no Fourth Amendment search had taken place.\textsuperscript{77} According to the Court, any subjective expectation of privacy would be unreasonable because a telephone customer, like anyone else, "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."\textsuperscript{78}

IV. \textsc{Electronic Mail}

Electronic mail ("e-mail") has rapidly become a familiar form of communication for business and pleasure, despite its potential insecurities.\textsuperscript{79} While as recently as the year 2000 only approximately forty-six percent of adult Americans were online, today at least sixty-three percent are online.\textsuperscript{80} Although not yet as universal as the telephone in

\begin{footnotes}
\footnotetext{76}{Smith, 442 U.S. at 737.}
\footnotetext{77}{Id. at 743-45. The Court also concluded it was unlikely that the defendant had any subjective expectation of privacy in the information, given that customers know phone company equipment requires the number to route the call, that the phone company makes a record of at least some numbers dialed (toll calls), and because most customers know that the phone company can generally assist in tracing obscene or harassing callers. Id. at 742-43.}
\footnotetext{78}{Id. at 743-44. For more contemporary variations on this theme, see Michael Moss \& Ford Fessenden, \textit{America Under Surveillance: Privacy and Security: New Tools for Domestic Spying, and Qualms}, N.Y. TIMES, Dec. 10, 2002, at A1 (describing FBI efforts to identify every person who had taken diving lessons in the previous three years via dive shop records after becoming concerned that terrorists might attack using scuba gear); Philip Shenon \& John Scwartz, \textit{JetBlue Target of Inquiries By 2 Agencies}, N.Y. TIMES, Sept. 23, 2003, at C1 (describing JetBlue Airways' revelation that it had provided travel records on passengers to a Pentagon contractor). For other examples of what is deemed "voluntarily turn[ed] over" see United States v. Dionisio, 410 U.S. 1, 14-15 (1973) (holding taking of voice exemplar does not constitute a search; stating same for facial characteristics and handwriting); United States v. Mara, 410 U.S. 19, 22 (1973) (handwriting exemplar).}
\footnotetext{79}{See Katie Hafner, \textit{Billions Served Daily, and Counting}, N.Y. TIMES, Dec. 6, 2001, at G1 (according to one estimate 9.8 billion e-mails are sent each day); Steve Lohr, \textit{Off the Shelf: A Management Revolution Still in the Making}, N.Y. TIMES, Mar. 17, 2002, § 3, at 5 (noting that "the average American office worker receives [thirty-six] email messages a day, seven times more than voicemail").}
\end{footnotes}
1967, e-mail is becoming universal at a much more rapid pace. In the words of Chief Justice Rehnquist,

'[t]echnology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.'

Despite this well-known threat, most courts have yet to determine whether the sender of e-mail retains a reasonable expectation of privacy in the contents of the message. An examination of how the REP doctrine applies to e-mail demonstrates an ambiguity in the third party doctrine that has significant ramifications for technologically-enhanced searches.

A. The Technology of E-mail

For our purposes, a rather rudimentary understanding of e-mail will suffice. Say Bob, who has an account with the Internet Service Provider ("ISP") Earthlink and the e-mail address bob@earthlink.net, wants to send a message to Alice, who has an account with AT&T and the e-mail address alice@att.net. Bob will first draft the message with his e-mail client of choice (e.g., Microsoft Outlook or Eudora), which will then "send" the message. Because the Internet is a packet-switched network, Bob's message will be divided up into multiple packets if it is lengthy. This does not fundamentally alter our analysis, however, so we will presume Bob's e-mail will travel as a single packet. Just as with postal mail, Bob's message could not reach Alice if her address were

81. It was not until 1945 that forty-six percent of American households were equipped with telephone service. U.S. Census Bureau, Statistical Abstract, supra note 58.


83. For a complete description of the technology of e-mail see JAMES F. Kurose & KEITH W. Ross, COMPUTER NETWORKING: A TOP-DOWN APPROACH FEATURING THE INTERNET 106-24 (2001).

84. Perhaps a more technically proper term for "email client" is "user agent." See id. at 107-08.

85. See id. at 18-20.

86. This would always be true in a message-switched network. See id. at 20-21. While it is theoretically possible that different packets (portions) of the same message will travel different routes to their ultimate destination, as a practical matter this is unlikely, and either way it is not crucial to our analysis. See id. at 275. Each packet contains the information necessary to route it to its ultimate destination, where the entire message will be reassembled. See id. at 24.
not included. Therefore, Bob’s computer will append the required addressing information to his message.87

The manner in which Bob’s message will travel to the mail server at his ISP depends on the technology he uses to access the Internet. If he uses a dial-up connection over the plain old telephone system (“POTS”), his modem will convert the digital voltage states of his computer to an analog-encoded digital signal that can travel over the telephone line.88 If Bob uses DSL, his more sophisticated modem will do the same.89 If he uses a cable broadband connection, Bob’s cable modem will route the signal to the local head end, from where it will travel to the mail server.90 If he is at an office with a local area network (“LAN”), an Ethernet modem will probably send the data on its way.91 Regardless of the technology, the result is the same—Bob’s message will make its way to Earthlink’s mail server.

That server will send the message on its way to AT&T’s mail server; from there it will be up to AT&T to deliver the content to Alice.92 The Internet is a vast network of networks, each linked via some means of communication, be it copper wire, fiber optic cable, or radio transmission.93 Earthlink’s server will not have a direct connection to AT&T. Instead, Earthlink will send the message to an intermediate system that puts the message “closer” to its destination; that system will send the message to another intermediate system “closer” to its destination, and this process will continue until the message ultimately reaches the mail server owned by AT&T.94 The routing algorithms that determine the path Bob’s message will take through the “Internet cloud” are fascinating and complicated, but beyond our scope.95 But the message will take some sequence of “hops” from one system to the next until it reaches AT&T.

So who has access to Bob’s message? Obviously Bob’s ISP, Earthlink, and Alice’s ISP, AT&T, have access. But these are not all; every system through which Bob’s message travels could access its content. Bob has

87. See id. at 24.
88. Id. at 30-31.
89. Id. at 31-32.
90. Id. at 32-33.
91. Id. at 33-34.
92. The Simple Mail Transfer Protocol (SMTP) will be used to communicate the message between the mail servers, while either the Post Office Protocol—Version 3 (POP3) or the Internet Mail Access Protocol (IMAP) will be used to retrieve the message from AT&T’s mail server. See id. at 109-11, 118-22.
93. See id. at 1-4, 34-38.
94. See id. at 3.
95. See id. at 321-31.
absolutely no way of knowing which systems these will be or who will own them. In fact, because routing is dependent upon current traffic, nobody could know which systems these will be. Bob only knows that his message will ultimately make its way to AT&T, from whom Alice will obtain it.

B. Reasonable Expectation of Privacy

According to the third party doctrine, Bob has voluntarily given his message to any number of persons, and therefore could be said to have no reasonable expectation of privacy ("REP") in that message. If so, the government could access the e-mail without Fourth Amendment restriction not only from Earthlink or AT&T, but also from any intermediate system through which the message passed that happened to retain a copy. Although this leaves absolutely no Fourth Amendment protection for a critical means of communication, such a holding would not be without precedent.

While there is scant law on the Fourth Amendment's application to e-mail, the military courts have considered the issue on several occasions. In *United States v. Maxwell*, an Air Force officer was convicted by general court-martial based on the content of e-mails he sent to and received from other AOL users. The U.S. Court of Appeals for the Armed Forces held that Maxwell possessed a REP in e-mail messages on the AOL system, but only because the messages never left AOL's proprietary network and AOL contractually guaranteed their privacy. In the words of the court, "AOL differs from other systems, specifically the Internet... [T]he Internet has a less secure e-mail...

---

96. One plausible reason for the paucity of law is the statutory protection provided to electronic communications, including e-mail, under the Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000), and under the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2000). Because suppression of evidence is not a remedy under either Act, however, it remains surprising that more defendants do not invoke the Fourth Amendment. See 18 U.S.C. § 2515 (1968) (providing exclusionary remedy only for wire or oral communications); 18 U.S.C. §§ 2707 (2002), 2708 (1986) (not providing for suppression). An impetus for statutory protection was a Department of Justice opinion that one may not have a reasonable expectation of privacy in e-mail. See S. Rep. 99-541, 3-4; 1986 U.S.C.C.A.N. 3555, 3557-58. Because of the storing and forwarding technology of e-mail, however, it may not receive any meaningful protection under the Wiretap Act. See United States v. Councilman, 373 F.3d 197, 201-04 (1st Cir. 2004) (holding any e-mail in "electronic storage" as defined by the Stored Communications Act is not governed by the Wiretap Act).
98. Id. at 410, 417.
99. Id. at 417.
system, in which messages must pass through a series of computers in order to reach the intended recipient.”

In United States v. Monroe, Staff Sergeant Monroe used an e-mail account provided by the military. When personnel charged with administering that network perused his e-mail, Monroe alleged a violation of the Fourth Amendment. The same military court found no REP: "Based on the totality of the circumstances, we conclude that Monroe had no reasonable expectation of privacy in his e-mail messages or e-mail box at least from the personnel charged with maintaining the [network]." In United States v. Geter, a lower military court followed Maxwell and Monroe and found no REP.

In both Monroe and Geter, the service provider, the United States government, actively denied any expectation of privacy for reasons of military order. But the reasoning of Maxwell is not so limited, nor did the court in Geter so limit its holding. The defendant in Geter argued that e-mail should be treated analogously to postal mail, thus urging the court to follow the longstanding Supreme Court precedent that the sender of postal mail retains a reasonable expectation of privacy in the contents of a sealed mailing. The court rejected the proffered analogy based on the following circumstance. When Geter’s message was sent via electronic mail a copy was retained despite the transmission having been completed, and only that copy was accessed.

The court could just as easily have cited the fact that those transmitting e-mail along its path need not tear open a physical envelope to read

100. Id. Whether the court had a solid understanding of the technology is questionable, but the implications for e-mails that do traverse the Internet is clear.


102. Id. at 327-28.

103. Id. at 330. Monroe had knowingly received pornography, including several depictions of child pornography and several depictions that were obscene. See id. at 329.


105. Id. at *3. Geter, a member of the United States Marine Corps, had used his government e-mail account to send messages in furtherance of a conspiracy to distribute controlled substances. Id. at *1.

106. In Monroe defendant encountered a banner upon every login: “USERS LOGGING INTO THIS SYSTEM CONSENT TO MONITORING BY THE HOSTADM.” Monroe, 52 M.J. at 328. At least one other court has held similarly with respect to the content of a police department network. See generally Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

107. Geter, 2003 WL 21254249, at *5. The Supreme Court concluded a reasonable expectation of privacy existed in sealed postal mail in Ex parte Jackson, 96 U.S. 727, 733 (1877).


109. See id.
its contents. Perhaps this distinction is what lead the Eighth Circuit to state that "[w]hile it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution." But surely such a technological fortuity should not govern the Fourth Amendment. In his dissent in *Olmstead*, Justice Brandeis argued that telephone calls should be treated like postal mail, an argument the Court has come to accept. Brandeis’s argument applies just as forcefully to e-mail:

In Ex parte Jackson it was held that a sealed letter intrusted to the mail is protected by the [Fourth] Amendment. ... There is, in essence, no difference between the sealed letter and the private telephone message. As [was] said below: “True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference.”

Instead, what is relevant is whether the information was voluntarily provided to a third party for that party’s use, distinguishing between couriers of information—whatever the format—and recipients of information. In *Smith* the Supreme Court held there was no REP in the numbers dialed on a telephone because “[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.” In other words the telephone company must know the number dialed in order to complete the requested communication. Because the telephone company has no similar need to know the contents of that communication, the sender retains a REP in those contents despite the fact that they are every bit as much voluntarily conveyed to the phone company.

110. United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002). Regarding the court’s reference to statutory protection, see supra note 101. The court in *Bach* declined to decide whether there is a reasonable expectation of privacy in e-mail because it was not determinative. *See id.* at 1066.

111. *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting).


113. *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting) (internal citation omitted).


115. The contents of a communication are conveyed to the telephone company, and telephone companies are statutorily authorized to review those contents in order to protect their rights and property. *See* 18 U.S.C. § 2511(2)(a)(i) (2000).

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic
Similarly, in *Miller* the Court explained that

these are the business records of the banks . . . . [B]anks are not neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance. The records of [Miller's] accounts, like all of the records [which are required to be kept pursuant to the Bank Secrecy Act] pertain to transactions to which the bank was itself a party . . . . All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.\(^{116}\)

The many systems that may route an e-mail along its path, including the sender's and recipient's ISPs, are not parties to the substantive communication and do not have any similar stake in that substance. Instead, like the United States Post Office, they merely require the addressing information necessary to forward the message closer to its destination.

Therefore, as with postal mail and telephone conversations, the sender of e-mail retains no REP in the addressing components, but should retain a REP in the contents.\(^{117}\) However, no court has so held, and

---

communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

*See*, e.g., United States v. Pervaz, 118 F.3d 1, 5 (1997) (cellular provider relied upon § 2511(2)(a)(i) to monitor conversations on cloned cellular phones).

\(^{116}\) *Miller*, 425 U.S. at 440-42 (internal quotation marks and citations omitted).

\(^{117}\) For an early consideration of this distinction, see Chris J. Katopis, *"Searching" Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L. & TECH. J. 175, 196-203 (1995). The Fourth Circuit, in an unpublished opinion, has recognized that the addressing components of e-mail are analogous to the number dialed on a telephone and, therefore, receive no Fourth Amendment protection under the REP test. *See* United States v. Hambrick, 2000 WL 1062039, *4 (4th Cir. 2000) (unpublished) ("In this case, as in *Miller*, there is no legitimate expectation of privacy in information voluntarily conveyed to a third party and exposed to their employees in the ordinary course of business."); *Id.* (internal quotation marks omitted). *See also* Maxwell, 45 M.J. at 418. The Wisconsin Supreme Court recently determined there was a reasonable expectation of privacy in remotely stored files, an encouraging, though somewhat clumsily articulated, holding. *See In re John Doe Proceeding*, 680 N.W.2d 792, 805 (Wisc. 2004).

There may also be "external" justifications for providing Fourth Amendment protection to e-mail, such as its significance in the discourse of society (thus implicating the First Amendment). Such external arguments will not be pursued in this Article. Likewise, even if courts acknowledge a reasonable expectation of privacy in sent e-mail, Fourth
the Supreme Court has never explained when information voluntarily conveyed to a third party "counts" (i.e., one retains no REP, as in Smith and Miller) and when it does not (i.e., one retains a REP, as in Katz).\textsuperscript{118}

V. UBQUITOUS VOLUNTARY DISCLOSURE

A. Packet-switched Telephone

Although a nuanced interpretation of "voluntary disclosure" will therefore provide Fourth Amendment protection to electronic mail (we can term this a "limited third party doctrine"), a consideration of encrypted e-mail will help introduce the true magnitude of this third party issue. First, however, it is useful to note a technological fortuity that could lead courts to the right result—namely that the sender of e-mail retains a REP in the contents of the message—but for the wrong reason. The result would be welcome, but a failure to recognize the necessary doctrinal change will leave privacy at the mercy of developing technology.

Unlike the Internet, traditional telephone networks are circuit switched. When Bob places a telephone call to Alice, the resources necessary to communicate their words are reserved for the duration of the call.\textsuperscript{119} While this can be frustrating—Bob might get the recording "all circuits are busy now" if he tries to call on Christmas morning or Mother's Day—once the connection is established, Bob and Alice know they will be able to complete their conversation, no matter how monotonous and lengthy. Even when Alice temporarily puts down the receiver to look for a document or to let in the dog, the resources they occupy are unavailable to others. With a circuit-switched system, a fixed number of lines running under the Atlantic ocean necessarily means that only a fixed number of New Yorkers can communicate with their London counterparts at any one time, even if all those users are silent for significant periods.\textsuperscript{120}

---

\textsuperscript{118} Amendment doctrine may allow law enforcement to obtain such content via a mere subpoena not requiring notice to the sender. This would offer relatively little protection. See, e.g., United States v. Barr, 605 F. Supp. 114 (S.D.N.Y. 1985). While this is a significant issue, it too is beyond the scope of this paper.

\textsuperscript{119} Although the holding in \textit{Katz} itself dictates that the restrictive view should be adopted, it is not clear whether the Supreme Court will do so. \textit{See infra} Section V.G.

\textsuperscript{120} The lines are multiplexed, so more than one conversation is conveyed on each physical link. But for our purposes, this is an unnecessary complication. For a description of multiplexing see id. at 15-18.
The Internet's packet-switched architecture means that those sending Internet communications will not hear "all circuits are busy now," but it also means there is no guarantee when, if ever, a given packet of information will reach its intended destination. Today one can subscribe to a Voice over Internet Protocol ("VoIP") service, in which all telephone calls are, at least in part, packet switched. Moreover, telecommunications providers have begun to route at least portions of traditional landline telephone conversations via packet switching because it avoids wasting resources during silent periods.

Any content communicated over a packet-switched network experiences store and forward delay as it routes through the network, and the owner of any intermediate system through which the packet traverses has control over the storage of that content. Therefore, the content can be retrieved in later than real-time. If courts were to find no REP in the contents of e-mail because it is necessarily conveyed to others, they would either have to find likewise for the contents of modern telephone conversations, an unlikely result, or create an anomaly whereby digitized voice content passing through precisely the same systems retains a REP that e-mail content does not.

B. Encryption

In order to better understand the consequences of a third party doctrine, let us return to Bob and Alice. Bob again wants to send an e-mail to Alice, but this time he wants to take advantage of encryption's ability to guarantee confidentiality, making the message unintelligible.

121. If the reader wonders how e-mail or other data transfer can then function at all reliably, it is because it depends upon a protocol known as TCP (Transmission Control Protocol) that provides reliable data transfer by resending lost packets. See id. at 11-12. If an application instead requires rapid communication but can absorb some data loss, such as viewing a live sporting event online, a different protocol termed UDP (User Datagram Protocol) is used. See id. at 12-13.

122. Id. at 18-20; Voice-Over-Internet Protocol, at http://www.fcc.gov/voip; The Quiet Iconoclast-Face Value, ECONOMIST, July 3, 2004, at 54 (describing "Skype" Internet telephony service); James Fellows, In Internet Calling: Skype is Living Up to Hype, NEW YORK TIMES, Sept. 5, 2004.

123. KUROSE & ROSS, COMPUTER NETWORKING, supra note 83, at 20. The provider must still limit the number of simultaneous callers, however, to approximate the performance guarantee of a circuit.

124. Architectures in which content is necessarily provided to third parties will become more and more common. For example, airlines currently forbid the use of mobile phones, not because they are a safety hazard, but because their use would wreak havoc on the telephone networks as the plane quickly moved from one base station to the next. The solution is to have all content channeled through the airline. Cleared for Take-off? Mobile Phones on Planes, ECONOMIST, Apr. 3, 2004 (available at 2004 WL 62017484).
to anyone other than his intended recipient.\textsuperscript{125} If Bob and Alice select a secure implementation of a strong cryptographic algorithm and are careful to maintain the secrecy of the encryption password or “key,” not even the wealthiest and most able of adversaries will be able to comprehend the message.\textsuperscript{126}

When Bob writes his e-mail, it is in plaintext—anyone can read it, presuming they understand the language in which it is written. When he encrypts the message it becomes ciphertext, which, again presuming a strong algorithm and implementation, is absolute gibberish. A third party cannot glean any of the plaintext from the ciphertext without decrypting the message, which requires knowledge of the encryption passphrase or key.\textsuperscript{127} Bob has wisely used technology to guarantee his privacy vis-à-vis Alice where the law is unsettled. Neither his ISP nor Alice’s ISP, nor any of the many intermediate systems the message might traverse on its way to Alice’s ISP, nor anyone obtaining the ciphertext from any of those sources, will be able to read the contents of the message.

So far so good. But it is also possible, indeed perhaps plausible for encryption neophytes, that Bob and Alice might use an algorithm or implementation that is crackable.\textsuperscript{128} In that case the government could obtain the ciphertext from the ISP and then decipher the plaintext without the encryption key. Thus, it is necessary to ask whether, even if e-mail did not generally retain a REP, would encrypted e-mail retain such an expectation?

The answer should be an emphatic yes. According to Supreme Court precedent, one retains a reasonable expectation of privacy in anything placed inside a closed container.\textsuperscript{129} Moreover, this REP receives significant protection. Absent an exception, police with probable cause may not open a closed container; they may only seize the container and

\begin{itemize}
\item \textsuperscript{125} Confidentiality is one of the three critical functions that cryptography, or encryption, can provide. It can also provide integrity (permitting the recipient to detect tampering) and authenticity (permitting the recipient to verify the source of the message). \textit{See} BRUCE SCHNEIER, \textit{SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD} 86, 93 (2000).
\item \textsuperscript{126} Obviously a great number of assumptions go into any statement that alleges a scientific conclusion without delving into the science itself. For purposes of this paper, however, it is not necessary to understand the fascinating mathematics of encryption. For an excellent description of modern cryptography understandable to a lay person, see \textit{id.} at 85-119. For a lucid description of the mathematics of encryption, see generally BRUCE SCHNEIER, \textit{APPLIED CRYPTOGRAPHY} (1996).
\item \textsuperscript{127} \textit{See} SCHNEIER, \textit{SECRETS & LIES}, \textit{supra} note 125, at 86-87.
\item \textsuperscript{128} \textit{See id.} at 102-06.
\item \textsuperscript{129} United States v. Ross, 456 U.S. 798, 812 (1982).
\end{itemize}
seek a warrant to permit its opening. Further, the law is no respecter of containers. When it comes to the Fourth Amendment, a pauper's paper bag is as worthy as a king's triple-locked chest. So, if Bob decided to personally walk a printout of his message to Alice, whether he chose to enclose the message in a brown paper bag, an attaché case, or ciphertext, he should retain a REP in its contents.

Does the result change when Bob gives that closed container to another party for temporary safekeeping, here his ISP? While the law in this area is not without ambiguity, courts have held that a person providing a closed container to another for temporary safekeeping can retain a REP in the contents of that container. And with regard to


The exceptions include customs searches (see Jacobsen, 466 U.S. at 114 n.8; Ross, 456 U.S. at 823), a search not exceeding the scope of a prior search by a non-governmental actor (see Jacobsen, 466 U.S. at 115-16), a search incident to a lawful arrest (see Ross, 456 U.S. at 823), and when the container is located within an automobile (see Ross, 456 U.S. at 823). See also WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 5.5 (2004) (describing five additional categories).

131. Ross, 456 U.S. at 822-23 ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."). The Court explained that a constitutional distinction between "worthy" and "unworthy" containers would be improper. Even though such a distinction perhaps could evolve in a series of cases in which paper bags, locked trunks, lunch buckets, and orange crates were placed on one side of the line or the other, the central purpose of the Fourth Amendment forecloses such a distinction. For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

132. Thus, in holding unconstitutional the search of a bag deposited with a grocery store clerk, the District of Columbia Circuit stated that the implications of the government's argument that he retained no reasonable expectation of privacy are most disturbing. In a variety of circumstances, we are all forced to surrender our possessions temporarily to the custody of others. We leave our bags with clerks at stores, museums, and restaurants; we check our
letters and packages sent via either postal mail or private courier, the most analogous to e-mail, the Supreme Court has so held. Thus, if police were to obtain the container (an encrypted e-mail) from the bailee (Bob's ISP or other intermediary), they would not have the authority to peruse its contents.

Yet a knowledgeable commentator, Orin Kerr, has arrived at a contrary conclusion, namely that encryption does not create a REP. While I believe there are subtle errors in Professor Kerr's legal analysis, for our purposes we need only focus on Kerr's clever...
hypothetical: The infamous Lex Luthor, of Superman fame, prints an advertisement in the newspaper offering a trade. If $100 million is wired to his bank account, he will provide the key that will decrypt the enclosed message describing where and when he plans some "diabolical entertainment." An enterprising police officer instead scrutinizes the encrypted message over breakfast—no doubt consisting of donuts—and realizes Luthor used only a simple substitution cipher, with B substituting for A, C substituting for B, etc. He quickly unscrambles the message and averts disaster at no cost to the taxpayer other than his salaried pay.136

Averting disaster is good, but also putting away the would-be perpetrator is even better. Kerr is unwilling to accept that Luthor would be able to suppress the evidence found as a result of the officer’s decryption, a result he feels should follow if encryption creates a REP.137 First, it does not seem clear that this result would follow. If a convicted kidnapper confronts an officer on the street, holds up a briefcase, and states, “I’ve kidnapped another little girl, and her name and address just happen to be in this briefcase, too bad you can’t open it!”, it seems obvious the officer can seize the briefcase based on probable cause (a confession) and open it immediately on account of exigent circumstances. A court authorizing such conduct ex-post would not be denying that the briefcase created a REP in its contents, but rather would be making the unremarkable declaration that the search was reasonable under the circumstances and, hence, constitutional. A court could likewise ratify the officer’s conduct in the Luthor hypothetical without denying the container, namely encryption, its due.

Of course Luthor thoughtfully provided until noon the next day for officers to obtain and wire the $100 million; perhaps there was no exigency. But this is akin to our kidnapper holding up the briefcase and

agent listening to a recording of the conversations from translating them to English. The discussion of Kerr’s Luthor hypothetical, infra, describes the relevance of defendants having adopted a “code” known by hundreds of millions of people. Last, Kerr cites Commonwealth v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991), in which the Pennsylvania Supreme Court allowed police to use evidence obtained via a warrant search of defendant’s computer that was marked for deletion but not yet overwritten. That police may, pursuant to a warrant, search within any particularly described location that may contain items subject to seizure is well settled (see Ross, 456 U.S. at 820), but it has no bearing on whether police may search that same location without a warrant as Kerr argues. Somewhat different responses to Professor Kerr are made by Sean J. Edgett, Student Note, Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy, 30 PEPP. L. REV. 339 (2003).

137. Id. at 519-20.
instead stating, "I'm going to kidnap another little girl tomorrow, and her name and address just happen to be in this briefcase." Even if there were insufficient exigency, and therefore, the officer would be authorized only to seize the briefcase and seek a warrant permitting it to be searched, this does not indicate that the briefcase is now a "better" container, creating "more" of a REP. It merely recognizes that the same privacy invasion that is reasonable in one circumstance is not reasonable in another. So too with Luthor's encryption.

But the cipher chosen by Luthor is childish, on par with Pig-Latin. Could it really be necessary that an officer obtain a warrant before utilizing his or her ordinary intelligence to decipher the message? The Supreme Court has answered sensibly in the negative. While the Court has refused to create a jurisprudence of "worthy" and "unworthy" containers, Luthor's simple substitution cipher is akin to our kidnapper holding up a transparent bag, perhaps a Ziploc. In the words of the Court, "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view." A Ziploc bag provides a wonderful seal, but it doesn't conceal its contents from an officer possessing ordinary eyesight. Likewise, a substitution cipher does not conceal a message from an officer possessing ordinary intelligence. In both instances the content is in "plain view."

Even with these limitations, Kerr's Luthor hypothetical is insightful because it presents an interesting question: Is it simply too bizarre to accept a Fourth Amendment that might restrict police from using information provided to them? If Luthor had chosen a stronger cryptographic algorithm, the officer would not have been able to decrypt the message without the aid of technology. Would it be strange to deny the officer the use of that technology absent a warrant, or is this the Fourth Amendment we have had all along? Should the ability to "see through" a closed briefcase via x-rays or other electromagnetic waves

138. While substitution ciphers are common fodder for newspaper puzzle pages and are easy to solve for some, they are much more complicated than Luthor's because they do not merely shift every letter by one.

139. Id. at 522-23.

140. See LAFAVE, SEARCH AND SEIZURE, supra note 130, at § 5.5(f) (describing containers that permit an observer to view or infer their contents). The reader should be careful not to conflate the discussion here with situations in which the content is not affirmatively provided to the party from which it is obtained by the government. See Section III, supra, discussing unencrypted e-mail. Professor Kerr had no reason to address this situation.

141. It is not at all unfamiliar in criminal jurisprudence that we might deny police, or at least prosecutors, use of information police obtain (think of Miranda), but here police are being provided the information.
mean police have carte blanche authority to do so without Fourth Amendment restraint? In order to answer these questions it is helpful to review some modern technologies.

C. Millimeter Waves

Although most of us are unaware of it, our bodies are constantly radiating energy. In fact all objects above a temperature of absolute zero emit electromagnetic radiation. Thus, the paper on which these words are printed emits radiation, as does the chair on which you may be sitting. We cannot see this radiation unless it is within the visible spectrum, meaning within those wavelengths of electromagnetic energy that are detectable by the human eye.

While this may seem an idle scientific curiosity, it becomes extremely relevant if you want to know what someone is carrying on his or her person. It just so happens that the human body is more emissive in the millimeter wave spectrum than most other objects, including guns, knives, or particulates such as cocaine. And just as visible light transmits through glass, millimeter waves transmit through clothing. Thus, enterprising scientists are developing handheld devices

---

142. See Nat'l Inst. of Justice, Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection, NIJ Guide 602-00, at 16 (2001), available at www.nlectc.org. This is not the "zero" we typically relate to temperature in the United States, which would be zero degrees Fahrenheit. Absolute zero is zero Kelvin, which is equivalent to negative 460 degrees Fahrenheit or negative 273 degrees Celsius. See id.; Edwin R. Jones & Richard L. Childers, Contemporary College Physics 348 (3d ed. 2001).

143. See Jones & Childers, supra note 142, at 685-87. It is a familiar concept that electromagnetic radiation exists that is not visible to our eye—we all know that ultraviolet rays emitted by the sun can burn our skin. Yet unlike radiation in the visible spectrum, ultraviolet rays are almost completely reflected by glass, and thus, one cannot get a sunburn (or tan) through an automobile windshield.

Bodies at moderate temperature generally emit mostly in the infrared spectrum, which is a longer wavelength than visible light, and only as a body is heated does it emit more and more into the visible spectrum. Thus, a heated object appears red, a hotter object appears yellow, and an even hotter object appears blue, because the eye "sees" the wavelengths in the visible spectrum as moving from red to yellow to blue. See id. at 762-63, 862-63.


145. Nigel Hawkes & Oliver Wright, The Machine That Leaves You No Place to Hide, The Times (London), Nov. 8, 2003, at 11. Another spectrum of wavelengths we commonly encounter that transmit through objects are radio waves; if they did not, it would be
that display an image of an individual and any items that individual is carrying.\textsuperscript{146}

Such a device is entirely passive, meaning it emits no radiation as would a typical x-ray device.\textsuperscript{147} It is in essence a video camera, only one that is interested in millimeter waves rather than those in the visible spectrum. Hence, the device merely receives what is "voluntarily provided" and displays that information in a convenient format.\textsuperscript{148}

D. Off-the-window Eavesdropping

When a person speaks, those of us blessed with hearing can hear that speech because we have a membrane in our ears that is sensitive to sound waves.\textsuperscript{149} Sound waves propagate through the air carrying energy.\textsuperscript{150} When a wave encounters a solid object, energy will continue into the solid and cause the solid to vibrate. The magnitude of such vibrations is of course small for ordinary sound volumes, and the vibrations cannot be detected by the human eye.\textsuperscript{151} If that solid is a

impossible to listen to a radio located entirely inside a home or receive a call on the cellular telephone in your pocket.


\textsuperscript{147} See GUIDE TO THE TECHNOLOGIES, supra note 142, at 17, 31, 43-44; Butterfield, supra note 144.

\textsuperscript{148} Just as one could avoid providing information to Internet third-parties by foregoing the use of e-mail, one could avoid providing information to those equipped with millimeter wave detectors by shielding his or her body from such emissions. Once a person is made aware of the relevant science, any decision not to counter that science can be deemed "voluntary."

\textsuperscript{149} See LAURALEE SHERWOOD, HUMAN PHYSIOLOGY: FROM CELLS TO SYSTEMS 216 (5th ed. 2004).

\textsuperscript{150} Sound, including the human voice, is a longitudinal wave, meaning it is a series of compressions and expansions of air molecules that propagates through the air (visualize a slinky, stretched at one end and then released). It is termed a longitudinal wave to distinguish it from a transverse wave, which would result if one end of a rope were pulled up and then back down. See JONES & CHILDERS, supra note 142, at 406-13.

\textsuperscript{151} See id. at 412-13; SHERWOOD, supra note 149, at 215. That solids will vibrate from sound waves is a phenomenon most of us will recognize from our involuntary experiences with extremely loud car stereos.
window, however, and if a laser beam is directed at that window, the beam will be modulated by those vibrations. That modulation will contain the same information one's ear would obtain inside the room; hence, a person located outside the room or building can hear the conversation.  

Although such a device is not entirely passive (the laser itself propagates energy, a small portion of which will travel into the window), it creates only the most negligible of disturbances to an outside window where it merely receives information "voluntarily provided" and conveys that information in an audible format.

E. TEMPEST

TEMPEST is the military's term for van Eck radiation, which is the radiation unintentionally leaked by all electronic equipment. While this is ordinarily a mere nuisance (perhaps a hairdryer or blender disrupting television reception), computers are subject to this leakage like all other electronic devices. A computer's monitor is particularly leaky, but hard drives, cables, printers, and all other peripherals also leak radiation.  

In concept such a device is not new: "It is said that certain types of electronic rays beamed at walls or glass windows are capable of catching voice vibrations as they are bounced off the surfaces." Berger v. State of New York, 388 U.S. 41, 47 (1967).

152. Maggie Farley, Speak Into My Attaché Case: At the U.N., Few Conversations are Safe From Listening Devices, L.A. TIMES, Apr. 1, 2004, at A1 (noting the technology and alleging, according to an unnamed former CIA official, that it is utilized at the U.N. in New York); Eric Hanson, Deadly finale at Mount Carmel: Agents had Array of Electronic Bugs, HOUSTON CHRONICLE, Apr. 22, 1993, at A12 (describing technology and supposing, according to a private expert in counter-surveillance techniques, that it was used at the Branch Davidian compound in Waco). In order to discern the conversation, the eavesdropper must be able to filter out ambient noise, such as that from birds chirping or cars driving nearby. George J. Church, The Art of High-Tech Snooping: How Nigh-invisible Devices Can Get Under an Embassy's Skin, TIME, Apr. 20, 1987, at 22. A countermeasure is available via devices that vibrate widows with white noise—unless the would-be-eavesdropper has access to that white noise as well, he or she will be unable to filter it from the desired conversation. See id.; Andrew Baxter, Inside Track: Good Vibrations for Everyday Objects, FINANCIAL TIMES, Oct. 11, 2000, at 17 (noting use of the defense at a bank).


154. SCHNEIER, SECRETS & LIES, supra note 125, at 220. It is possible to shield such devices, essentially by creating a Faraday cage of conducting materials around the device, but doing so is costly. Id.; Church, supra note 152. For a provider of such solutions see
This leaked radiation can be detected, and the information a device is processing can sometimes be extracted. Thus, Peter Wright claims that MI5 was able to obtain the plaintext of French communications despite being unable to break its diplomatic cipher, and television "police" in Britain are able to catch scofflaws of their infamous television license. And it is possible, given appropriate environmental conditions and suitable equipment, to view the contents of a computer monitor from down the street. Such equipment, like a millimeter wave video camera, is entirely passive. The device merely receives what is "voluntarily provided" and displays that information in a convenient format.

F. Distributive Effect

Millimeter wave detectors, off-the-window eavesdropping, and TEMPEST receivers are all sophisticated, but they are within the reach of current technology. Thus, police equipped with modern technology are "voluntarily provided" with substantial information previously protected by the Fourth Amendment, first under the property-based conception and then, when new technologies made that inadequate, under the reasonable expectation of privacy conception. If courts do not adopt the limited third party doctrine, the use of such devices may dramatically increase.

At least two factors influence the prevalence of a policing technique. First, there are costs independent of legal regulation. For example, neither the use of undercover agents nor stakeouts are restricted by the Fourth Amendment, but both activities are very expensive in terms of police time. Further, undercover agents are often at significant risk


155. Peter Wright, Spycatcher: The Candid Autobiography of a Senior Intelligence Officer (1986). Encrypting data does not itself defend against TEMPEST because it is a "side-channel attack"—the plaintext can leak right along with the encrypted text. See Schneier, Secrets & Lies, supra note 125, at 220.


157. Schneier, Secrets & Lies, supra note 125, at 220. The leaked radiation not only travels through the air; it can also travel over power or telephone lines, or can be retransmitted via cell phone or radio. Id. An extensive amount of information on TEMPEST is available at Joel McNamara, The Complete, Unofficial TEMPEST Information Page, at http://www.eskimo.com/~joelm/tempest.html.

158. As to undercover agents, see the discussion of the false friend cases (Hoffa and White), supra notes 59-68. As to stakeouts, see the discussion of tracking automobiles (Knotts and Karo), infra.
of harm. Therefore, we can presume police will be judicious in their use of these techniques.  

As William Stuntz has forcefully argued, a second factor is legal regulation.  

"[L]egal regulation acts as a tax, a mechanism for making some activities more expensive relative to their substitutes."  

Because we have a multi-tiered Fourth Amendment in which some activities are strictly regulated (e.g., the search of a home) and others receive no restriction (e.g., those deemed not a search), resource-constrained police are likely to engage in less of the former and more of the latter.  

If courts were to reject the limited third party doctrine and opt for a broad conception of voluntary disclosure, these two factors would combine to dramatically skew police resources.  

Unlike the use of undercover agents or stakeouts, the cost of using devices like those described above is negligible. While the cost of the equipment may currently be high, it will decrease dramatically over time and is a one-time sunk cost. Technologically-enhanced searches thus have a natural efficiency, tending to lower the cost of obtaining a given quantum of information. While ideally the Fourth Amendment would right this balance, under a broad conception of voluntary disclosure, the opposite will occur.  

Rather than obtaining the probable cause necessary to search a person, police could use a passive millimeter wave detector. Rather than obtaining a warrant authorizing a bug, police could use off-the-  

---  

160. Id. at 1274.  
161. Id.  
162. See id. at 1275-76. Professor Stuntz examines this distribution effect in detail as it relates to drug crime and demonstrates that "policing urban crack markets is cheaper than policing suburban markets in cocaine powder, and Fourth Amendment law makes that cost gap substantially larger than it otherwise might be." Id. at 1285. This leads him to argue that we should rethink our conception of the privacy interest protected by the Fourth Amendment. See id. at 1289.  
163. Legislatures could of course regulate or prohibit such activity. It is the responsibility of courts to interpret the Fourth Amendment, however, and there are reasons of permanence to prefer rights be protected by the Constitution rather than merely by legislation. For a view that favors Congressional action in this arena over judicial interpretation, however, see Kerr, The Fourth Amendment in Cyberspace, supra note 134.  
164. Police can conduct a protective "pat down" merely upon the dual reasonable suspicion that a crime has been committed and that the suspect is armed, but a full search requires probable cause. See Terry v. Ohio, 392 U.S. 1, 9 (1968).
Rather than obtaining a warrant to install a keystroke recorder on a computer, police could obtain its real-time operations via a TEMPEST receiver. In all three instances, the technologically-enhanced search, absent Fourth Amendment restriction, is likely to be far cheaper than the Fourth Amendment restricted alternative.

G. Kyllo

The Supreme Court has yet to adopt the limited third party doctrine and has at times seemed entirely indifferent to the intrusive capability of modern technology. When law enforcement was able to track a vehicle only via an electronic tracking device, the Court brushed aside the contention that the technology could be relevant and stated that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them."

Yet the Court's opinion in Kyllo v. United States, while far from a model of judicial clarity, demonstrates that at least some of the

165. While the Fourth Amendment would term the required judicial authorization a "warrant" no matter what specific requirements were necessary to render the search reasonable, the Wiretap Act requires what is often termed a "Title III order" after Title III of the Omnibus Crime Control and Safe Streets Act of 1968, codified as amended at 18 U.S.C. §§ 2510-2522 (2000).

166. If the computer was located in the home, the Supreme Court's decision in Kyllo would impose a Fourth Amendment restraint because Kyllo implicitly adopts the limited third party doctrine in the home context. See infra Part V(G).

167. United States v. Knotts, 460 U.S. 276, 282 (1983). Knotts is discussed in more detail infra Part VI(B). The Court's precise language ends with "such enhancement as science and technology afforded them in this case," which could serve as a limiting principle, but the Court made no effort to articulate what that limitation might be. See id. Three Justices, in concurrence, similarly truncated the majority's language. Id. at 288 (Stevens, J., concurring). The Court went on to conclude that "[i]nsofar as respondent's complaint appears to be simply that scientific devices such as the [electronic] beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now." Id. at 284.

A majority of the Court was similarly unphased by the use of technology in a series of cases in which the Court held that airplane and helicopter flyovers did not constitute searches. See Florida v. Riley, 488 U.S. 445, 451-52 (1989) (concerning naked-eye observation from helicopter circling at 400 feet); California v. Ciraolo, 476 U.S. 207 (1986) (concerning naked-eye observation from airplane flying at 1,000 feet); Dow Chemical Co. v. United States, 476 U.S. 227, 229, 239 (1986) (concerning aerial photography from airplane at 1,200 feet using $22,000 camera). All three cases split the Court five to four, however.

Justices have begun to advert to the danger of increasingly intrusive technology. The indoor growth of marijuana typically requires high-intensity lamps, which emit infrared radiation. This radiation can be detected and displayed by a video camera attuned to those wavelengths of electromagnetic energy.\(^\text{169}\) When a federal agent suspected that Danny Kyllo was growing marijuana in his home, the agent, from the vantage point of his patrol car positioned on the public street, used such an imager to measure and display the relative amounts of radiation emanating from the home.\(^\text{170}\) In the words of the district court, the imager was "a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house."\(^\text{171}\) The question for the Court was whether this constituted a Fourth Amendment search.\(^\text{172}\)

The radiation emanating from Kyllo's home, whether from high-intensity lamps or leakage from his computer, was available to anyone equipped to receive it, and Kyllo could have blocked it. He did not, however, affirmatively provide the information to others \textit{intending} that it be used. Thus, the limited third party doctrine would not foreclose the possibility that the agent's use of the thermal imager constituted a Fourth Amendment search,\(^\text{173}\) while a broad interpretation of the doctrine would require a holding of no search.

Unfortunately, the Court's opinion, penned by Justice Scalia for a five-member majority,\(^\text{174}\) failed to address the third party doctrine. Instead, it focused on the constitutional space involved in this intrusion, the home, and the special place it holds in Fourth Amendment jurisprudence.\(^\text{175}\) However, the Court's holding that the thermal scan did

---

\(^{169}\) Such a device operates just like the millimeter wave camera described in Section V(C).

\(^{170}\) \textit{Kyllo}, 533 U.S. at 29-30.

\(^{171}\) \textit{Id.} at 30.

\(^{172}\) When the scan detected high levels of infrared radiation consistent with an indoor growing operation, agents used this information, informants' tips, and utility bills to obtain a search warrant. Inside they found more than 100 marijuana plants. \textit{Id.}

\(^{173}\) Under current doctrine it would still be necessary to consider whether Kyllo had a reasonable expectation of privacy. For a discussion of the wisdom of this requirement see \textit{infra} Section VI.A.

\(^{174}\) Joining Justice Scalia were Justices Souter, Thomas, Ginsburg, and Breyer, not a typical five-member voting block of the Court.

\(^{175}\) After quoting the text of the Fourth Amendment, the Court began its analysis by asserting that "[a]l the very core of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" \textit{Kyllo}, 533 U.S. at 31 (quoting \textit{Silverman v. United States}, 365 U.S. 505, 511 (1961)). Rather than discussing technologically-enhanced searches in general, the Court limited its analysis to those impacting the home:
constitute a search is consistent with the limited third party doctrine.\textsuperscript{176} And the opinion contains encouraging words regarding the relevance of technology:

The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy . . . . While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.\textsuperscript{177}

However, the majority's failure to address the third party doctrine renders the entire opinion of questionable significance outside the context of the home.

The four-member dissent, penned by Justice Stevens, squarely frames the issue the majority neglected: "'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.' That is the principle implicated here."\textsuperscript{178} That is precisely the principle implicated, and the dissent would have done well had it examined that issue carefully. Instead, the dissent erroneously concluded that there was no search because the surveillance was "off-the-wall" rather than "through-the-wall."\textsuperscript{179}

This distinction, which implicitly adopts a broad interpretation of the third party doctrine, seems to conflict with \textit{Katz} itself. After all, the bug in \textit{Katz} was placed on the outside of the public telephone booth, the seeming equivalent of the off-the-window eavesdropping described in

\textsuperscript{176} Id. at 33 (internal citations omitted); See id. at 37-38 (further discussing the unique context of the home). The Court concluded that "the Fourth Amendment draws a firm line at the entrance to the house. That line, we think, must be not only firm but also bright." Id. at 40 (internal citation and quotation marks omitted).

\textsuperscript{177} Id. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'").

\textsuperscript{178} Id. at 34, 36. The court cited several systems designed to "see" through walls. Id. at 36 n.3.

\textsuperscript{179} Id. at 42 (quoting \textit{Katz}, 389 U.S. 347, 351) (Stevens, Rehnquist, O'Connor, Kennedy, JJ., dissenting).

\textsuperscript{179} Id. at 41 (Stevens, Rehnquist, O'Connor, Kennedy, JJ., dissenting).
Section IV(D). But the dissent believed it could distinguish the holdings because

(i) In *Katz*, the electronic listening device attached to the outside of the phone booth allowed the officers to pick up the content of the conversation inside the booth, making them the functional equivalent of intruders because they gathered information that was otherwise available only to someone inside the private area; it would be as if, in this case, the thermal imager presented a view of the heat-generating activity inside petitioner's home. By contrast, the thermal imager here disclosed only the relative amounts of heat radiating from the house; it would be as if, in *Katz*, the listening device disclosed only the relative volume of sound leaving the booth, which presumably was discernible in the public domain . . . . The use of the latter device [i.e., one disclosing only volume] would be constitutional given *Smith v. Maryland*, which upheld the use of pen registers to record numbers dialed on a phone because, unlike "the listening device employed in *Katz* . . . pen registers do not acquire the contents of communications."180

This attempt to distinguish *Katz* demonstrates a complete failure to appreciate the third party doctrine, apparently believing those cases relied on some talismanic distinction between "content" and "non-content" information.181

Thus, *Kyllo* is a mixed bag. Five members of the Court seem to appreciate technology's relevance to what constitutes a Fourth Amendment search, which is encouraging even though it is questionable what they would hold outside the context of the home. But while their holding is consistent with the limited third party doctrine, they failed to

180. Id. at 49-50, 50 n.6 (alteration in original) (internal citation omitted) (Stevens, Rehnquist, O'Connor, Kennedy, JJ., dissenting).

181. Precisely what information would constitute "content" outside the context of human speech is left unclear, but apparently the following would not:

[P]ublic officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gasses, airborne particulates, or radioactive emissions, any of which could identify hazards to the community. In my judgment, monitoring such emissions with "sense-enhancing technology," and drawing useful conclusions from such monitoring, is an entirely reasonable public service.

Id. at 45 (internal citation omitted) (Stevens, Rehnquist, O'Connor, Kennedy, JJ., dissenting). Of course whether such conduct is "reasonable" is an entirely separate question from whether it constitutes a search, but Justice Stevens seems to use the two interchangeably.
recognize that issue. Even more discouraging is that four members of the Court would vote to the contrary.\textsuperscript{182}

VI. WHAT IS \textit{REASONABLE}?

Sections III and IV demonstrate that the REP test and a limited third party doctrine provide Fourth Amendment protection for many technologically-enhanced searches. This is important because courts tend to favor clarifications and minor adjustments, and this is one that realistically can and should be made. But this is not to say that either doctrine is sensible. Before turning to how courts should interpret reasonableness in the context of technologically-enhanced intrusions, it is helpful to briefly reconsider why we have the REP test.

A. REP Redux

For those concerned about privacy vis-à-vis the government, once technology allowed intrusion without physical encroachment \textit{Katz's} test was a great improvement over \textit{Olmstead's} property-based conception. But the language of the Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."\textsuperscript{183} While neither the term "search" nor "seizure" is defined by the Constitution, they are (and were, at the time of the founding) ordinary, commonplace words.\textsuperscript{184} Should they not bear that ordinary meaning? The Supreme Court's definition of "seizure" seems to follow this logical mold: a seizure occurs when there is "some meaningful interference with an individual's possessor interests in . . . property."\textsuperscript{185} So while \textit{Katz's}

\begin{itemize}
\item \textsuperscript{182} Moreover, the federal circuits that had considered the issue had uniformly sided with the \textit{Kyllo} dissenters. See id. at 46 n.4.
\item \textsuperscript{183} U.S. CONST. amend. IV.
\item \textsuperscript{184} When the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief." N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989).
\item \textsuperscript{185} United States v. Jacobsen, 466 U.S. 109, 113 (1984). A contemporary dictionary gives its first definition of "search" as: "To make a thorough examination of; look over carefully in order to find something; explore." \textit{AMERICAN HERITAGE COLLEGE DICTIONARY} (1997).
\end{itemize}
conception was an improvement upon *Olmstead*, we are left to wonder why either Court thought it necessary to artificially limit the meaning of "search."

The Court in *Olmstead* implied that its limitation on "search" was necessary to avoid a dramatic result. According to the Court, a beneficent desire to give the Fourth Amendment a liberal construction to "effect the purpose of the framers of the Constitution in the interest of liberty . . . cannot justify enlargement of the language employed 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." Even if both hearing and sight constitute a "search," it does not follow that they are necessarily unreasonable and, hence, forbidden.

But *Olmstead* was decided in an era in which the Court tenaciously hung to the mantra that warrantless searches were presumptively unconstitutional. Indeed in *Katz*, when adopting the REP definition, the Court emphatically stated:

> Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions. 187

Therefore, if a warrantless intrusion were to be deemed constitutional, it must either fall within one of those "few . . . exceptions" or not be a search at all.

The Court's recent jurisprudence instead recognizes that finding the Fourth Amendment to be implicated does not forbid anything; its command is only that any search or seizure be reasonable. 188 Thus, in describing the transition from *Olmstead*'s property-based conception as it relates to visual observation of a home, the Court in *Kyllo* stated:

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

---

187. *Katz*, 389 U.S. at 357 (internal quotation marks and citations omitted).
188. See, e.g., *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002) ("We must therefore review the School District's Policy for 'reasonableness,' which is the touchstone of the constitutionality of a governmental search.").
somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.\textsuperscript{189}

Thus, the Court, while not yet ready to jettison the REP “two step,” recognizes its redundancy. By smuggling the term “reasonable” into REP, the Court’s current jurisprudence merely splits into two artificial steps what could be handled as one. If there is no reasonable expectation of privacy, it would seem to necessarily follow that the intrusion was a reasonable one.\textsuperscript{190} Thus, I add my voice to those of Professors Akhil Amar and Vikram Amar, who eloquently and convincingly made the case for jettisoning the REP test in favor of a dictionary definition of search.\textsuperscript{191} What is important for purposes of this paper, however, is merely to recognize that with or without a REP requirement, some form of third party doctrine could be a part of reasonableness, and, with or without a REP requirement, the real work is done by that reasonableness determination.

B. The Third Party Doctrine Redux

The third party doctrine is objectionable even if limited as recommended. First, it treats privacy as an indivisible commodity—once information is given to any one party for any one purpose, it is treated as if it were given to every person for any possible purpose as far as the Fourth Amendment is concerned. This powerful critique was first made by Justice Marshall, dissenting in \textit{Smith}.\textsuperscript{192} Second, perhaps a subset of

\begin{footnotes}
\item[189.] \textit{Kyllo}, 533 U.S. at 32.
\item[190.] Before writing for the Court in \textit{Kyllo}, Justice Scalia had raised this issue directly in a concurrence joined by Justice Thomas: “[C]ase law . . . leaps to apply the fuzzy standard of ‘legitimate expectation of privacy’—a consideration that is often relevant to whether a search or seizure covered by the Fourth Amendment is ‘unreasonable’—to the threshold question whether a search or seizure covered by the Fourth Amendment has occurred.” \textit{Minnesota v. Carter}, 525 U.S. 83, 91-92 (1998).
\item[192.] 442 U.S. at 749 (Marshall, Brennan, JJ., dissenting). \textit{See also} Lewis R. Katz, \textit{In Search of a Fourth Amendment for the Twenty-First Century}, 65 IND. L.J. 549, 564-66 (1990). This critique is certainly applicable to modern technologies. For example, many drivers in the Northeast take advantage of the E-ZPass, an electronic tag placed inside a vehicle that makes it unnecessary to stop at toll booths. \textit{See E-ZPass Information, How It Works}, at http://www.ezpass.com/static/info/howit.shtml. That those drivers willingly convey their identity and location to toll collectors does not mean they should be held to provide it to anyone setting up an antenna to capture that information, including police. Similarly those using cell-phones convey their location to their cellular providers. \textit{See}
the more serious first critique, application of the doctrine is sometimes ambiguous.

Consider the tracking of automobiles. In United States v. Knotts, officers suspected the defendants were manufacturing illicit drugs. When one of the defendants purchased a drum of chloroform, officers followed his vehicle, but they twice lost visual surveillance. They were nonetheless able to continue tracking the vehicle because they had placed an electronic transmitter, or "beeper," in the drum. But this too proved difficult and officers lost its signal. Only when a helicopter was able to relocate the then-stationary transmitter were police led to the drum's ultimate destination, a secluded cabin. The defendants alleged that this tracking violated the Fourth Amendment.

Relying on the third party doctrine, the Supreme Court held that

[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Thus, "there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment." Under a broad conception of the third party doctrine, this holding seems correct. However, under a limited conception, the proper result is not immediately apparent. On the one hand, a driver intentionally


194. Id. at 278. One termination of visual surveillance was a tactical decision based on defendant's initiation of evasive maneuvers. Id.; United States v. Knotts, 662 F.2d 515, 516 (8th Cir. 1981).
195. Knotts, 460 U.S. at 278. "A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." Id. at 277. The chemical vendor had consented to its installation. Id. at 278.
196. Id. at 278. When officers searched the cabin pursuant to a search warrant, they found a fully operable drug laboratory consisting of over $10,000 in equipment and chemicals in sufficient quantities to produce fourteen pounds of pure amphetamine. Id. at 279.
197. Id. at 281-82.
198. Id. at 285. The following year the Court held that monitoring such a beeper located within a residence does constitute a search. See United States v. Karo, 468 U.S. 705, 714 (1984).
conveys his or her position to pedestrians and other drivers to avoid an accident. On the other hand, most drivers would not think they were conveying their entire driving route to bystanders, though they surely recognize the possibility that another vehicle will travel the same route and thereby gather that information. That probability, however, decreases as the route becomes more lengthy or complex. And unless the driver consents to electronic surveillance, the presumption that he or she intends to convey a driving route that is not amenable to visual surveillance, as in *Knotts*, is especially dubious.

A similar ambiguity arises in the context of “data mining.” While, as noted above, the third party doctrine has always been subject to critique for adopting an indivisible conception of privacy, it becomes especially suspect when one considers the extraordinary databases under construction today. Whether one should be considered to have affirmatively given information to a third party for use when that information is incorporated into a database of entirely unforeseeable scope and intent is not clear.

As a final example, consider the Supreme Court’s strange jurisprudence of flyovers and baggage squeezes. Relying on the third party doctrine, the Court has held that all three of the following do not constitute a search: (1) observation of a fenced residential backyard from the vantage point of a chartered airplane flying at 1000 feet; (2) aerial photography of an industrial manufacturing complex via a $22,000 mapping camera at 1200 feet; and (3)

---

199. One might consent to such surveillance for reasons of personal security or convenience. See, e.g., http://www.onstar.com (describing OnStar service available in some vehicles that offers, *inter alia*, roadside assistance and vehicle tracking). The Ninth Circuit has held, however, that the government violates the Wiretap Act if it renders such a system inoperable in order to eavesdrop. See *In re Application of the United States*, 349 F.3d 1132, 1146 (2003).


“We what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”... Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, we readily conclude that respondent’s expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor.


[The] industrial complex... is open to the view and observation of persons in aircraft lawfully in the public airspace immediately above or sufficiently near the area for the reach of cameras. We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by
observation of a greenhouse in a residential backyard from a helicopter hovering at 400 feet. Yet when the Court was called upon to determine whether a border patrol agent's physical squeeze of a bus passenger's carry-on bag constituted a search, the Court held in the affirmative.

The flyover holdings are correct under a broad conception of the third party doctrine, but they seem contrary to the limited doctrine. In all three cases, the target of the surveillance took significant precautions to prevent observation. What is most relevant here, however, is a comparison of the holdings. Given the Court's decision that there is no REP in a fenced backyard because that information is knowingly conveyed to anyone flying overhead, how could there be a REP in information obtained by squeezing a soft canvas bag placed in a shared carry-on compartment? In a "world of travel that is somewhat less gentle than it used to be," surely passengers realize their bags will be handled by others. Nonetheless, according to the Court, "[p]hysically invasive inspection is simply more intrusive than purely visual inspection." When the item physically inspected is a soft-cover carry-on, and the item visually inspected is located within a securely fenced backyard, this proposition is questionable. But an all or nothing third party doctrine is prone to creating these types of arbitrary distinctions.

As with the REP, courts would do better to consider such "degrees" of providing information to others as a factor in the reasonableness inquiry rather than as an independent determinative test.

As with the REP, courts would do better to consider such "degrees" of providing information to others as a factor in the reasonableness inquiry rather than as an independent determinative test.

---


204. Bond v. United States, 529 U.S. 334 (2000). The agent felt a "brick-like" object, after which he requested and obtained consent to search the bag. Id. at 336.

205. In Ciraolo the homeowner surrounded his yard with a 6-foot outer fence and a 10-foot inner fence. 476 U.S. at 209. Dow Chemical Company spent millions of dollars each year on elaborate security precautions. Dow Chemical, 476 U.S. at 241-42 (Powell, J., dissenting in part). The homeowner in Riley surrounded his greenhouse with trees and shrubs and placed a wire fence surrounding the greenhouse and his home. 488 U.S. at 448.

206. Bond, 529 U.S. at 340 (Breyer, J., dissenting).

207. Id. at 337.
C. Reasonableness

As a unanimous Supreme Court stated in 2001,

[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests."

That comparison, however, need not be conducted in every case. In the context of the home, for example, the Court has consistently held that warrantless searches are presumptively unconstitutional. A government wishing to justify such an intrusion must proffer an adequate rationale, such as exigent circumstances, consent, or the homeowner's status as a probationer. Only upon such a showing need a court balance the competing interests.

While the Supreme Court has appropriately recognized a wide range of factors relevant to this calculus, the Court is inconsistent in their application. Moreover, advancing technology may require that we rethink what factors are relevant and which way various factors cut.

208. United States v. Knights, 534 U.S. 112, 118-19 (2001). The Court went on to explain that "[a]lthough the Fourth Amendment ordinarily requires the degree of probability embodied in the term 'probable cause,' a lesser degree satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable." Id. at 121. See also Soldal v. Cook County, 506 U.S. 56, 71 (1992) ("Reasonableness is . . . the ultimate standard under the Fourth Amendment . . . . As is true in other circumstances, the reasonableness determination will reflect a careful balancing of governmental and private interests.") (internal citations and quotation marks omitted); Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("The Fourth Amendment'[s] . . . 'central requirement' is one of reasonableness."); Atwater v. City of Lago Vista, 523 U.S. 318, 361 (2001) (terming the balance of interests is the "bedrock" principle of Fourth Amendment jurisprudence) (O'Connor, J., dissenting).

209. Kirk v. Louisiana, 536 U.S. 635, 636 (2002) (per curiam) ("absent exigent circumstances, the firm line at the entrance to the house . . . may not reasonably be crossed without a warrant") (internal quotation marks omitted) (citing Payton v. New York, 445 U.S. 573, 590 (1980)).


211. See McArthur, 531 U.S. at 331.

(In the circumstances of the case before us, we cannot say that the warrantless seizure was per se unreasonable. It involves a plausible claim of . . . "exigent circumstances." . . . Consequently, rather than employing a per se rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.).
This analysis becomes even more important if the Court were to adopt a dictionary definition of "search" because intrusions that formerly had no Fourth Amendment restriction would now be subject to the same reasonableness criterion.

1. Government Need. Reasonableness requires a court to compare the intrusion upon privacy with the government need. One element of government need could be termed "fungibility." If the same information is available via other less intrusive means, the greater intrusion is likely to be unreasonable. Thus, the fact that a low-cost, technologically-enhanced search can obtain needed information should not itself be sufficient to render that search constitutional.

Another logical element of government need is the magnitude of the crime at issue. Imagine two police officers, Officer Paul and Officer Parks. Officer Paul has probable cause to believe a given intrusion will locate evidence relevant to a murder investigation. Officer Parks has probable cause to believe the same intrusion will locate evidence that the suspect is indeed a user of marijuana. Surely the intrusion by Officer Parks is less likely to be reasonable, and the Supreme Court has recognized this. The recognition has only been on the periphery, however, when the crime is especially minor or especially dangerous.

In Welsh v. Wisconsin, police received a report that an erratically driven car had swerved off the road into an open field. When inspection of the now abandoned car revealed that it was registered to Edward Welsh and that he lived within walking distance, officers traveled to his residence. Without obtaining a warrant or consent, police entered the home and proceeded upstairs to Welsh's bedroom where they found him lying in bed. Welsh was arrested for driving while under the influence of an intoxicant. Under the laws of Wisconsin at the time, the offense was a nonjailable violation with a maximum fine of $200.

213. Id. at 742. The sole witness pulled off the road behind the erratically-driven vehicle, and thus, was available for police questioning when they arrived upon the scene. Id.
214. Id. at 742-43, 743 n.1, 746. Although Welsh's stepdaughter opened the door to their home, the trial court made no finding regarding consent. Therefore, the Court presumed an absence of consent for purposes of its opinion. Welsh was actually subject to a criminal misdemeanor charge with a maximum penalty of up to one year in jail and a fine of $500 because he had previously been convicted of the same offense within the previous five years. Id. at 746. The officers entering his home were unaware of his record, however, and therefore, the Court proceeded as if only the nonjailable civil violation were at issue. Id. at 746 n.6.
Welsh challenged the entry into his home, and the Court phrased the question presented as follows: "[W]hether, and if so under what circumstances, the Fourth Amendment prohibits the police from making a warrantless night entry of a person's home in order to arrest him for a nonjailable traffic offense."215 In other words, when the magnitude of intrusion is large (entrance into a home) and the magnitude of the underlying crime is small (deemed by the legislature to be a nonjailable civil forfeiture offense), can that intrusion be reasonable?

The Court began with its holding in Payton v. New York216: "[W]e decided in Payton . . . that warrantless felony arrests in the home are prohibited by the Fourth Amendment, absent probable cause and exigent circumstances."217 Whether the officers had probable cause was not before the Court.218 The Court accepted the State's asserted exigency, namely the necessity of determining Welsh's blood-alcohol level before it naturally decreased with the passage of time.219 Thus, the question before the Court was the scope of Payton—is the government need for a non-felony arrest sufficient to render reasonable a warrantless entry into a home based upon probable cause and the exigency of loss of evidence?

In an unfortunate twist, however, the Court held that the magnitude of the crime rendered the exigency insufficient,220 and thus the Court had "no occasion to consider whether the Fourth Amendment may impose an absolute ban on warrantless home arrests for certain minor offenses."221 According to the Court, when the underlying offense is minor, even the destruction of evidence does not present an exigency sufficient to justify a warrantless intrusion into the home.222 Although

---

215. Id. at 742.
217. Welsh, 466 U.S. at 749.
218. Id. at 748 n.9.
219. Id. at 753-54. The Court had previously recognized the exigency of loss of evidence via the temporal decrease in blood-alcohol content. See Schmerber v. California, 384 U.S. 757, 770-71 (1966) (allowing warrantless blood test for alcohol).
220. Welsh, 466 U.S. at 754.
221. Id. at 749 n.11.
222. Id. at 750-54. The Court adopted the explanation of Justice Jackson in a 1948 concurrence:

Even if one were to conclude that urgent circumstances might justify a forced entry without a warrant, no such emergency was present in this case. This method of law enforcement displays a shocking lack of all sense of proportion. Whether there is reasonable necessity for a search without waiting to obtain a warrant certainly depends somewhat upon the gravity of the offense thought to be in progress as well as the hazards of the method of attempting to reach it . . . . It is to me a shocking proposition that private homes, even quarters in a tenement, may be indiscriminately invaded at the discretion of any suspicious
the Court's decision to frame the inquiry as one of insufficient exigency is unnecessarily confusing, the upshot is unchanged—one factor in determining the reasonableness of an intrusion is the magnitude of the underlying crime. Thus, the Court opined that it was "difficult to conceive of a warrantless home arrest that would not be unreasonable under the Fourth Amendment when the underlying offense is extremely minor." The Court has similarly recognized that suspicion of a particularly serious crime may render reasonable an intrusion that would otherwise be unreasonable. In Florida v. J.L., a unanimous Court determined the frisk of a youth based upon an anonymous tip that the youth was carrying a gun was unconstitutional. But the Court warned against interpreting its holding as a per se bar.

The facts of this case do not require us to speculate about the circumstances under which the danger alleged in an anonymous tip might be so great as to justify a search even without a showing of [informant] reliability. We do not say, for example, that a report of a person carrying a bomb need bear the indicia of reliability we demand for a report of a person carrying a firearm before the police can constitutionally conduct a frisk.

Courts should more regularly consider the magnitude of the underlying crime as part of the reasonableness inquiry. Technology will
permit searches that may seem less intrusive but that obtain the same quantum of information—perhaps a scan by a passive millimeter wave camera rather than a full-body pat-down, or a single search of an extensive database rather than a significant background investigation. Including the magnitude of the alleged crime in the analysis may prevent courts from too freely authorizing intrusive conduct.\(^\text{228}\)

2. Political Process Checks. A fascinating tale of technological sleuthing helps demonstrate the role political process checks could play in the reasonableness inquiry. On March 21, 2003, Michael Little was driving his truck under an overpass in Surrey, England, when a brick hurled from above crashed through his windshield and into his chest. Although he managed to maneuver his 44-ton truck to the shoulder, he died of a heart attack before a police patrol located him three hours later. Such a random and senseless crime is difficult to solve, but police received a break when they discovered the perpetrator's blood on the brick, from which they were able to extract his DNA. When they ran a fingerprint of that DNA through Britain's database of criminal offenders, however, there were no matches.\(^\text{229}\)

The perpetrator, a teenager named Craig Harman, had enjoyed a night of drinking with friends. When he came upon a Renault Clio parked in a driveway, he broke the windshield as part of a fruitless

---

\(^228\) The usual way in which judges interpreting the Fourth Amendment take account of the fact that searches vary in the degree to which they invade personal privacy is by requiring a higher degree of probable cause (to believe that the search will yield incriminating evidence), and by being more insistent that a warrant be obtained if at all feasible, the more intrusive the search is. But maybe in dealing with so intrusive a technique as television surveillance, other methods of control as well, such as banning the technique outright from use in the home in connection with minor crimes, will be required, in order to strike a proper balance between public safety and personal privacy.

United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984) (internal citations omitted).

William Stuntz has proffered that "where the search tactic is both secret and potentially invasive, it should probably be limited to the investigation of violent felonies." William J. Stuntz, Local Policing After Terror, 111 YALE L.J. 2137, 2184 (2002). Professor Stuntz has convincingly critiqued what he terms the "transsubstantive" Fourth Amendment. See William J. Stuntz, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment, 114 HARV. L. REV. 874 (2001).

effort to steal the vehicle. In so doing, he cut his hand. When he and a friend later picked up bricks, Harman’s blood transferred to the brick that would shortly thereafter crash into Little’s windshield.\textsuperscript{230}

Having no other leads,\textsuperscript{231} police turned to Britain’s Forensic Science Service. Running Harman’s DNA fingerprint through their system resulted in a list of persons who shared eleven or more genetic markers with the perpetrator. Narrowing that list by geography left a man who shared sixteen markers with the perpetrator. That person was Craig Harman’s brother.\textsuperscript{232} Craig pleaded guilty to manslaughter when a sample of his DNA was a perfect match for that found on the brick.\textsuperscript{233}

Thus, technologically-enhanced sleuthing found a killer, albeit an unintentional one, who will now spend six years in prison.\textsuperscript{234} Britain leads the world in this use of “familial DNA” because it has the first and most expansive DNA database in the world.\textsuperscript{235} That database will soon grow even faster. Not only will police continue to take and preserve samples from anyone charged with a crime, but they will now take and preserve samples from mere arrestees.\textsuperscript{236}

While it may be normatively justifiable to construct a database solely of those convicted of crimes based on known rates of recidivism and the forfeiture of rights, no similar justification exists for retaining samples from mere arrestees. Moreover, notions of common fairness dictate that a better system would utilize an all-inclusive database to which everyone was required to contribute. If such a system were proposed, it would

\textsuperscript{230} Sue Clough, \textit{World first for police as relative’s DNA traps lorry driver’s killer}, \textsc{Daily Telegraph} (London), Apr. 20, 2004, at 6; \textit{Killer caught by relative’s DNA}, BBC News, Apr. 19, 2004, at http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/3640119.stm. Harman’s target was a sports car that was fortunately able to swerve out of the brick’s path. Bird, \textit{supra} note 237.

\textsuperscript{231} Six months of investigation and a £25,000 reward had not lead to the killer. Bird, \textit{supra} note 229.

\textsuperscript{232} “[T]wo people chosen at random are likely to share six or seven markers, but 11 or more suggests a blood relative.” \textit{The Sins of the Rathers—DNA Fingerprinting}, \textsc{Economist}, Apr. 24, 2004, at 60.

\textsuperscript{233} Bird, \textit{supra} note 229. Scientists estimated the probability of the blood on the brick not coming from Craig Harman at one in a billion. \textit{Id.}

\textsuperscript{234} \textit{Id.}

\textsuperscript{235} Falloon, \textit{supra} note 229. Police have solved at least two other murders using the technique, including one for which three persons had been falsely convicted of the crime. \textit{See} Bird, \textit{supra} note 229.

\textsuperscript{236} Falloon, \textit{supra} note 229. At least four states, Texas, Louisiana, Virginia, and California now require DNA samples be taken from certain arrestees, and Congress is considering a similar measure. \textit{See} Mark Hansen, \textit{DNA Dragnet}, 90 \textsc{ABA J.} 37, 43 (May 2004); Eric Slater, \textit{State Lends a Strong Hand to Crime-Fighting with DNA}, \textsc{L.A. Times}, Nov. 4, 2004, at A1. In such jurisdictions, uniform applicability is certainly preferable in order to avoid racial or other profiling and sham arrests designed to gather DNA samples.
benefit from the spirited dialogue that would no doubt result from any program in which those in power must participate. Further, if it were nonetheless implemented, it would enjoy a democratic legitimacy. Its use would then be relatively uncontroversial, unlike current DNA dragnets in which there are allegations of police threatening and berating individuals into giving “voluntary” DNA samples.\footnote{237}

The same is true if local police decide to conduct thermal scans of homes or millimeter wave scans of persons in a public place. If police provide advanced notice of their intentions and apply the technique in a broad and uniform manner, concerned citizens with the resources to resist such a program are likely to seek political redress. In the words of William Stuntz, “spreading the cost of policing through a larger slice of the population ... reduces the odds of voters demanding harsh and intrusive police tactics secure in the knowledge that those tactics will be applied to others.”\footnote{238} We witnessed this phenomenon in the demise of the Pentagon’s proposed Total Information Awareness project: it had uniform applicability, individuals thereby subjected to the program cried foul, and Congress terminated the program.\footnote{239}

A court’s determination of whether an intrusion is reasonable should include these factors of public vetting and broad applicability. If “expectations of privacy ... must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society,”\footnote{240} surely those “understandings” include proposals that have been publicly vetted and, ideally, democratically enacted. While a dislike of general warrants, and therefore, a preference for individualized suspicion, is rooted in our Fourth Amendment jurisprudence,\footnote{241} in some contexts broad applicability may be preferable.

During the 1980s the public schools in Vernonia, Oregon, witnessed a dramatic increase in disciplinary actions and other disruptions, which school officials attributed to an endemic drug culture led by student athletes. When various initiatives failed to alleviate the problem, the school district considered implementing a drug testing program and held

\footnotesize{237. See Hansen, \textit{DNA Dragnet}, supra note 236, at 38; Pam Bullock, \textit{To Try to Net a Killer, Police Ask a Small Town’s Men for DNA}, \textit{NEW YORK TIMES}, Jan. 10, 2005.}

\footnotesize{238. Stuntz, \textit{Local Policing}, supra note 228, at 2166.}

\footnotesize{239. A system for prescreening airline passengers dubbed CAPPs II recently suffered a similar fate, despite government spending of over $100 million on its planning. \textit{See} Mimi Hall & Barbara DeLollis, \textit{Plan to Collect Flier Data Canceled}, \textit{USA TODAY}, July 15, 2004, at 1A.}


a parent "input night" to discuss requiring mandatory drug testing for all students participating in interscholastic athletics. The parents in attendance were unanimously in favor, and a drug testing program was implemented beginning in the fall of 1989. When seventh-grader James Acton was denied the chance to play football based on his refusal to submit to testing, his family sued, alleging a violation of the Fourth Amendment.

In Vernonia School District 47J v. Acton, the Court held the policy was constitutional. The Court found several reasons to favor a suspicionless, uniform regime, including the accusatory nature of suspicion-based testing and the risk of invidious discrimination in selecting test subjects. The Court stated, "In many respects, we think, testing based on 'suspicion' of drug use would not be better, but worse." Thus, the Court has recognized that there are contexts in which broad, uniform application is more reasonable than that based upon individualized suspicion.

With regard to the public vetting of the school district policy, the Court had this to say:

We may note that the primary guardians of Vernonia’s schoolchildren appear to agree. The record shows no objection to this districtwide program by any parents other than the couple before us here—even though, as we have described, a public meeting was held to obtain

---

242. Id. at 648-50. The policy included both a mandatory test at the beginning of the season and random testing thereafter. See id. at 650.
243. Id. at 651.
245. Id. at 664-65.
246. Id. at 667.
247. Id. at 664. The Court's other reasons for favoring uniform testing were the likelihood of lawsuits alleging discriminatory treatment under a suspicion-based regime and a hesitancy to add another non-instructional duty for teachers. Id. at 663-64.
248. Three Justices strongly disagreed:

In justifying this result, the Court dispenses with a requirement of individualized suspicion on considered policy grounds. First, it explains that precisely because every student athlete is being tested, there is no concern that school officials might act arbitrarily in choosing whom to test. Second, a broad-based search regime, the Court reasons, dilutes the accusatory nature of the search. In making these policy arguments, of course, the Court sidesteps powerful, countervailing privacy concerns. Blanket searches, because they can involve thousands or millions of searches, pose a greater threat to liberty than do suspicion-based ones, which affect one person at a time.

Id. at 667 (O'Connor, Stevens, Souter, JJ., dissenting) (internal quotation marks omitted). An exhaustive analysis of how and when broad applicability is superior to individualized suspicion, which will have to await another paper, must take into account the many arguments of Justice O'Connor. See id. at 667-84.
parents' views. We find insufficient basis to contradict the judgment of Vernonia's parents, its school board, and the District Court, as to what was reasonably in the interest of these children under the circumstances.249

The Court reiterated these principles in a more recent decision holding constitutional a drug testing policy adopted by a school district in Tecumseh, Oklahoma, which required drug testing not only for student athletes but for all those participating in competitive extracurricular activities.250 Justice Breyer's concurring opinion strongly advocates public vetting:

When trying to resolve this kind of close question involving the interpretation of constitutional values, I believe it important that the school board provided an opportunity for the airing of these differences at public meetings designed to give the entire community "the opportunity to be able to participate" in developing the drug policy. The board used this democratic, participatory process to uncover and to resolve differences, giving weight to the fact that the process, in this instance, revealed little, if any, objection to the proposed testing program.251

While the Court has therefore recognized democratic vetting and broad application as favoring reasonableness in the "special needs" context of the public school,252 it has been less amenable to the concept in the realm of ordinary crime control. Despite previously allowing uniform automobile checkpoints to be used for intercepting illegal aliens253 and combating drunk driving (and implying they could be used for verifying license and registration254), in Indianapolis v. Edmond,256

249. Id. at 665.
251. Id. at 841. Justice Breyer also joined the majority opinion, and believed his concurrence was "consistent with the Court's opinion." Id. at 839.
252. See id. at 829-30. The Court uses the term "special needs" to refer to those situations in which there is a purpose "other than the normal need for law enforcement," such as highway safety or keeping school children off of drugs. See Ferguson v. City of Charleston, 532 U.S. 67, 74 n.7 (2001).
255. Delaware v. Prouse, 440 U.S. 648, 663 (1979) (holding unconstitutional a discretionary license and registration stop but implying a uniform roadblock for the same purpose would be constitutional). See Indianapolis v. Edmond, 531 U.S. 32, 37-38 (2000) ("[I]n Delaware v. Prouse we suggested that a similar type of roadblock with the purpose of verifying drivers' licenses and vehicle registrations would be permissible.") (internal citation omitted). Thus, once again a system of uniform applicability can sometimes be
the Court struck down a program of uniform checkpoints designed to interdict drugs.\textsuperscript{257} The Court "decline[d] to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes."\textsuperscript{258} As DNA databanks, data mining, thermal scans, and other technologies develop, the Supreme Court would be wise to reconsider this limitation. Whether the government need is crime control or automobile safety, those intrusions that are uniformly applied and publicly vetted are more likely to be reasonable.

3. Use Limitations. We have already discussed the limited third party doctrine, which in effect requires police to avert their "technologically-enhanced" eyes from information otherwise provided. The Supreme Court has also recognized that the programmatic purpose of a search may determine its constitutionality, meaning that for searches not based upon individualized suspicion and probable cause, the constitutionality of the search may depend upon its purpose.\textsuperscript{259}

One such search with which we are all familiar is the searching of carry-on baggage of those boarding an airplane. In the words of Judge Kozinski, writing for the Ninth Circuit, "[w]hile narrowly defined searches for guns and explosives are constitutional as justified by the need for air traffic safety, a generalized law enforcement search of all passengers as a condition for boarding a commercial aircraft would plainly be unconstitutional."\textsuperscript{260} Therefore, an airport screener's search violated the Fourth Amendment when, pursuant to a policy guaranteeing a $250 bounty, he informed the Customs Service that a certain

more reasonable. Justice Rehnquist humorously referred to this as a jurisprudence of "misery loves company." \textit{Prouse}, 440 U.S. at 664 (Rehnquist, J., dissenting).

\textsuperscript{256} 531 U.S. at 32 (2000).

\textsuperscript{257} \textit{Id.} at 44.

\textsuperscript{258} \textit{Id.} Readers familiar with \textit{Dow Chemical Co. v. United States}, 476 U.S. at 276 (discussed \textit{supra} note 202) may think the five-member majority's refusal to rely on trade secret law, which has been publicly vetted and democratically adopted, to similarly reflect a hesitancy to consider political process checks in the reasonableness determination. The majority in \textit{Dow Chemical}, however, did not reject this principle but instead rejected reliance on trade secret law because it was substantively irrelevant given the facts \textit{sub judice} (trade secret law does not forbid all photography—for example it has nothing to say about a non-competitor taking photographs for personal enjoyment). \textit{See Dow Chemical}, 476 U.S. at 239 n.6. Moreover the four dissenters relied on that law. \textit{See id.} at 248-249 (Powell, J., dissenting in part).

\textsuperscript{259} \textit{See Edmond}, 531 U.S. at 45-46 ("[P]rogrammatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion.").

\textsuperscript{260} United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1243 (9th Cir. 1989).
passenger was carrying a large amount of currency.\textsuperscript{261} The Ninth Circuit was not willing, however, to restrict the use of information obtained in airport searches that were not tainted by such improper motivation:

Nothing we say today precludes [screeners] from reporting information pertaining to criminal activity, as would any citizen. We see the matter as materially different where the communication is undertaken pursuant to an established relationship, fostered by official policy, even more so where the communication is nurtured by the payment of monetary rewards. The line we draw is a fine one but, we believe, one that has constitutional significance.\textsuperscript{262}

That line is not, however, mandated by the Fourth Amendment. As Harold Krent has argued, "the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information."\textsuperscript{263} Thus, if police wish to conduct a technologically-enhanced search, the proposed uses of information so obtained should factor into the reasonableness inquiry.

In accepting Vernonia's drug testing policy, the Court first recognized that

\textit{[t]he other privacy-invasive aspect of urinalysis is, of course, the information it discloses concerning the state of the subject's body, and the materials he has ingested. In this regard it is significant that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic.}\textsuperscript{264}

But it is not only relevant what information the government obtains, but also what the government does with that information. In Vernonia "the results of the tests [were] disclosed only to a limited class of school personnel who ha[d] a need to know; and they [were] not turned over to law enforcement authorities or used for any internal disciplinary function . . . . Accordingly, . . . [the Court determined] the invasion of privacy [was] not significant."\textsuperscript{265}

Likewise, in accepting Tecumseh's policy, the Court considered relevant that

\begin{itemize}
  \item \textsuperscript{261} Id. at 1241, 1248.
  \item \textsuperscript{262} Id. at 1247 n.7.
  \item \textsuperscript{263} Harold J. Krent, \textit{Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment}, 74 TEX. L. REV. 49, 51 (1995).
  \item \textsuperscript{264} The first privacy-invasive aspect being collection of the sample. \textit{See Vernonia}, 515 U.S. at 658.
  \item \textsuperscript{265} Id. at 658-60.
\end{itemize}
[t]he Policy clearly requires that the test results be kept in confidential files separate from a student's other educational records and released to school personnel only on a "need to know" basis . . . . Moreover, the test results are not turned over to any law enforcement authority. Nor do the test results here lead to the imposition of discipline or have any academic consequences . . . . Given the minimally intrusive nature of the sample collection and the limited uses to which the test results are put, we conclude that the invasion of students' privacy is not significant.266

The Court has similarly determined an intrusion was unreasonable because its fruits were used for criminal prosecution. In Ferguson v. City of Charleston,267 a public hospital, in conjunction with local prosecutors and police, designed a program to test expectant mothers for drug use.268 If a woman tested positive, she would be threatened with prosecution in order to "provide the necessary 'leverage' to make the [p]olicy effective."269 Despite the Court's past acceptance of suspicionless drug testing and traffic checkpoints, the Court held the program unconstitutional because the search results were conveyed to law enforcement.270

Justice Scalia, in a dissent joined by Chief Justice Rehnquist and Justice Thomas, critiqued this consideration of the use of a search's fruits.271 But as technologically-enhanced intrusions become more

266. Earls, 536 U.S. at 833-34.
268. Id. at 70-73. Although it was the hospital that initially contacted the local prosecutor, the prosecutor played the central role in developing the policy. See id. at 71.
269. Id. at 72 (quoting brief for City of Charleston). According to the initial policy, a patient testing positive after labor should be arrested. The policy was modified to provide an opportunity to avoid arrest by consenting to substance abuse treatment whether the drug use was detected during the pregnancy or following labor. Id.
270. Id. at 82-84. At least the program would be unconstitutional absent informed consent, which was not decided below; the Court remanded for consideration of this issue. See id. at 73-76, 77 n.11. In the words of the concurrence, "[t]he traditional warrant and probable-cause requirements are waived in our previous cases on the explicit assumption that the evidence obtained in the search is not intended to be used for law enforcement purposes." Id. at 88 (Kennedy, J., concurring). The previous cases were Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 633-34 (1989) (allowing drug testing for railway employees involved in train accidents); Nat'l Treasury Employees v. Von Raab, 489 U.S. 656, 679 (1989) (allowing drug testing for U.S. Customs Service employees seeking promotion to certain positions); Vernonia, 515 U.S. at 646 (allowing drug testing for student athletes) (discussed supra note 248); and Chandler v. Miller, 520 U.S. 305, 322-23 (1997) (striking down drug testing for candidates for state office).
271. Id. at 92 (Scalia, J., dissenting). Justice Scalia's strident argument in dissent made his authorship of Kyllo somewhat surprising:
commonplace and more invasive, this distinction could play an important role in determining Fourth Amendment reasonableness. While an intrusion is nonetheless made—a search takes place and the information is obtained—the ideal balance in a dangerous world may require a "Chinese wall" between those who engage in certain surveillance and routine law enforcement. While our privacy is surely invaded by government agents scanning persons or homes to prevent a terrorist attack or to protect a passing dignitary, it nonetheless might be more reasonable if they agree not to share that information with those pursuing ordinary law enforcement ends.\textsuperscript{272}

VII. NOTHING NEW UNDER THE SUN?

As Lawrence Lessig has developed, there are both legal and technological constraints on government action.\textsuperscript{273} The framers of the Constitution only had to be concerned with those intrusions that were technologically convenient in their day, and thus, the Supreme Court first interpreted the command of the Fourth Amendment to be tied to trespass. But fortunately the constitutional command chosen by the framers—that people be free from unreasonable searches—is a flexible one that allows courts to continue to protect privacy as we transition into a world in which no intrusion is technologically inconvenient.

The REP test must be limited to reign in its third party doctrine. Without external restraint, technology will lead to an expectation of no privacy, and police practice will incorporate that technology to create a reality of no privacy. Although legislation is always welcome in this area, and is crucial when it comes to protecting our privacy vis-à-vis each other,\textsuperscript{274} it is the responsibility of the courts to define our rights guaranteed by the Fourth Amendment in a deliberate fashion. Restricting the third party doctrine to information deliberately conveyed

\textsuperscript{272} Of course what uses are reasonable will have to depend on what information is discovered, thus, tying into the recognition that the magnitude of the underlying crime is also relevant to reasonableness. Police discovering a kidnapping victim could not be required to ignore that discovery under any rational or respectable system.

\textsuperscript{273} Lessig, Reading the Constitution, supra note 18, at 870.

\textsuperscript{274} The Fourth Amendment does not restrict non-government actors.
in order that its content be used is a necessary step in preventing the Fourth Amendment from becoming irrelevant.

The aims of the Fourth Amendment would be even better served if the Supreme Court would jettison its outmoded REP criterion and return to the text of the Amendment, considering only whether a search is reasonable under the circumstances. While a broad consideration of those circumstances, including magnitude of crime, political process checks, and use controls, may sometimes lead away from historical concerns such as the fear of general warrants, the command of the Fourth Amendment is better served by adapting to changing circumstances than tenaciously hanging onto the past. Just like time, technology waits for no one, and the Fourth Amendment must once again heed its call.

275. Moreover, such inclusion will provide courts with criteria to determine reasonableness when they might otherwise struggle to understand a given technology. See Orin S. Kerr, The Fourth Amendment in New Technologies: Constitutional Myths and The Case for Caution, 102 Mich. L. Rev. 799 (2004) (contrasting a court's relatively limited ability to educate itself about a given technology with that of a legislature).