THE FOURTH AMENDMENT IN AN ERA OF UBIQUITOUS TECHNOLOGY

Susan W. Brenner[*]

I. PRIVACY

We must think through the way technology changes what is private, and develop new concepts of reasonable privacy that preserve liberty and are workable in a networked world.[1]

The pre-eminent guarantee of personal privacy for those of us in the United States is the Fourth Amendment to the United States Constitution. As most everyone knows, the Fourth Amendment protects us from "unreasonable" searches and seizures. Searches infringe upon privacy; seizures impact on other interests, notably the interest in the possession and use of property.[2]

---

[*] NCR Distinguished Professor of Law and Technology, University of Dayton School of Law.

[1] Elon University/Pew Internet & American Life Project, Imagining the Internet: Predictions Database, Fall 2004 at http://www.elon.edu/predictions/ q12.aspx (last visited Aug. 2005). In 2004, the Pew Internet & American Life Project surveyed "1,286 network-technology stakeholders" to elicit their views as to how the Internet "will change our lives between 2004 and 2014." Id. The comment quoted in the text above was one respondent's reaction to this question:

> As computing devices become embedded in everything from clothes to appliances to cars to phones, these networked devices will allow greater surveillance by governments and businesses. By 2014, there will be increasing numbers of arrests based on this kind of surveillance by democratic governments as well as by authoritarian regimes.

Id.

[2] See, e.g., United States v. Karo, 468 U.S. 705, 728 (1984) (Stevens, J., concurring in part and dissenting in part).

Privacy evolved as a "bricks and mortar" concept.[3] When the Fourth Amendment was added to the Constitution, the real-world was the only world; technology had not yet given us the ability to transcend the strictures of the real-world in various ways.[4] We now have that ability: We can substitute the virtual realities provided by computer technology for the physical world; we can communicate with almost anyone from almost anywhere; and we use technologies to make our lives easier, to earn our living and to amuse us.

Technology is not a new phenomenon; ancient inventors produced complex mechanisms and understood a great deal about the physical forces underlying modern technology.[5] What is new is the way we approach technology: Ancient inventions were regarded as curiosities and often remained little more than toys;[6] this tendency to ignore or resist new technologies, which was the product of various social and cultural forces, persisted for centuries.[7] The resistance began to decline

[3] The phrase "bricks-and-mortar" "[d]escribes a site that has a physical presence in the real world (as opposed to a virtual presence in the online world)". WordSpy, Definition of bricks-and-mortar, at http://www.wordspy.com/words/bricks-and-mortar.asp (last visited Aug. 2005).

[4] N B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 79-105 (1937).

[5] See, e.g., The Antikythera Mechanism: The Clockwork Computer, THE ECONOMIST (Sept. 19, 2002), at http://www.economist.com/displaystory.cfm?story_id=1337165 (last visited Aug. 2005); Ancient Greek Scientists: Hero of Alexandria, Technology Museum of Thessaloniki, at http://www.tmth.edu.gr/en/aet/5/55.html (last visited Aug. 2005) (hero invented the steam engine, among other things, in the first century B.C.); see also RUDI VOLTI, SOCIETY AND TECHNOLOGICAL CHANGE 35-44, 54-56 (4th ed. 2001).

[6] See, e.g., A. WOLF, A HISTORY OF SCIENCE, TECHNOLOGY AND PHILOSOPHY IN THE 16TH AND 17TH CENTURIES 543 (1935); see also WILLIAM FIELDING OGBURN, TECHNOLIGICAL TRENDS AND NATIONAL POLICY, INCLUDING THE SOCIAL IMPLICATIONS OF NEW INVENTIONS 51 (1937).

[7] See, e.g., OGBURN, supra note 6, at 66 ("resistance to technological change has been so much a part of the texture of the historical process, that it cannot be ignored when the future of technology is charted"). See id. at 39-66 (describing historical resistance to different technologies).

in the nineteenth century because of the implementation of technologies—including the telegraph, electricity, the telephone, and the automobile—that would proliferate and permeate the fabric of society.[8] The success of these and subsequent technologies produced a cultural climate which embraced new technology.[9] Our receptivity to technology accelerates the processes of invention and implementation which, in turn, influence how we live; we move further and further away from the "bricks and mortar" reality that produced the Fourth Amendment.[10]

And that brings us to the question at hand: Can the Fourth Amendment's privacy guarantees be adapted to deal with a world in which technology is increasingly pervasive—a world of ubiquitous technology?[11]

---

[8] But see id. at 43-45, 49-51 and 53 (early resistance to these technologies).

[9] See, e.g., STEVEN JOHNSON, INTERFACE CULTURE: HOW NEW TECHNOLOGY TRANSFORMS THE WAY WE CREATE AND COMMUNICATE 1-10 (1st ed. 1997); see also VOLTI, supra note 5, at 35-53, 266-68.

[10] See Section I.A., infra.

[11] The phrases "ubiquitous technology" and "ubiquitous computing" are used interchangeably to refer to technologies that are woven into the fabric of everyday life. See, e.g., Niall Winters, Personal Privacy and Popular Ubiquitous Technology, UbiConf 2004, at http://www.uclic.ucl.ac.uk/projects/ubiconf/materials/Papers/Niall%20Winters.pdf. (last visited Aug. 2005). John Blau notes:

> Ubiquitous computing involves having computing devices essentially everywhere in the home, office or public area, as well as easy, natural ways for people to interact with them. Wireless technologies, sensors, radio frequency identification (RFID) tags and machine-to-machine communications will play a big role in this new area of computing.

John Blau, German Group Studies Ubiquitous Computing, Data Privacy, Network World, Dec. 22, 2004, at http://www.nwfusion.com/news/2004/1222germagroup.html (last visited Aug. 2005). This article focuses on "communicative" technologies instead of, say, industrial or agricultural technologies. Its concern is with technologies that can be used to generate information, collect information and/or share information. See Section II., infra. The Fourth Amendment is, of course, concerned with channeling how law enforcement finds, through searches, and obtains, through seizures, varieties of

To answer that question, we must do several things: The first is to identify the basic conceptions of privacy which existed in Twentieth Century American law: the Fourth Amendment standard and a tort standard derived from the work of Louis Brandeis and Charles Warren. The two sections immediately below undertake this analysis,[12] the purpose of which is to provide a benchmark—to let us understand how our approach to privacy evolved to accommodate technologies. The next step is to adapt that approach to accommodate Twenty-first century technologies. Section II of the article reviews existing and projected technologies and explains why the approach which evolved is inadequate. Section III considers how we can adapt our approach to deal with the era of ubiquitous technology. Finally, Section IV offers a brief conclusion.

A. Fourth Amendment

> *The . . . constitutional prohibition against unreasonable searches and seizures, has its source in that principle of the common law which finds expression in the maxim that `every man's house is his castle.' English history discloses [that the] . . . constitutional provisions . . . had their origin `in the . . . unwarrantable intrusion of executive agents into the houses . . . of individuals . . . .''*[13]

The Fourth Amendment is predicated on a spatial conception of privacy.[14] It is intended to protect the sanctity of pri-

information. See Section I.A., infra.

[12] See infra §§ I(A) and I(B),

[13] United States v. Three Tons of Coal, 28 F. Cas. 149, 151 (E.D. Wis. 1875). English law, of course, was not alone in providing special protection for the home. See LASSON, supra note 4, at 13-20.

[14] See Olmstead v. United States, 277 U.S. 438, 463 (1928) ("The well-known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects.").

vate property from intrusions by public officials[15] which derives from English common law.

Early common law punished "those who invaded a neighbor's premises."[16] In fact, by the Twelfth-century, housebreaking had become one of the "more serious crimes in medieval England" and by the Sixteenth-century English law had developed specific prohibitions against housebreaking, burglary and trespass.[17] These laws were only concerned with trespasses by private persons because official searches were almost unheard of until the Fifteenth century.[18] In the latter half of the Fifteenth century, however, the King and Parliament began authorizing trade guilds to "enter and search the workmanship of all manner of persons" to enforce guild regulations.[19] Roughly a century later, the Court of the Star Chamber, charged with licensing books and regulating printing "decreed that the wardens of the Stationers' Company . . . should have authority to open all packs and trunks of papers and books brought into the country, to search in any warehouse, shop, or any other place where they suspected a violation of the laws of printing to be taking place [and] to seize the books printed contrary to law".[20] Other courts followed suit, issuing edicts authorizing similar searches directed at those suspected

---

15 See Boyd v. United States, 116 U.S. 616, 627 (1886).

16 See William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 32 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with author).

17 Id. at 31-35.

18 Id. at 36, 75. A law enacted in 1335 required innkeepers near ports to search guests for counterfeit money; the innkeepers kept a portion of whatever they found and turned the rest over to "official searchers" who took the rest and monitored the innkeepers' discharge of this obligation. See LASSON, supra note 4, at 23.

19 See LASSON, supra note 4, at 24.

20 Id. at 25. The Stationers' Company was a guild of printers charged with enforcing the Star Chamber's restrictions on printing. See, e.g., TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 25 (1969).

of libel, heresy and political dissent.[21] This led to the evolution of the general warrant, which was issued with no proof of individualized suspicion and in which no "names are specified . . . and . . . a discretionary power given to messengers to search wherever their suspicions may chance to fall."[22] As arbitrary searches became more common, "Englishmen began to insist that their houses were castles for the paradoxical reason that the castle-like security that those houses had afforded from intrusion was vanishing."[23]

In several decisions issued in the mid-eighteenth century, English courts held that homes were protected from arbitrary action by government officials.[24] Most of these decisions grew out of an investigation into seditious libel: Ordered to find the author of a recently-published letter, officers acting under the authority of a general warrant searched five houses and made a number of arrests.[25] Those persons whose homes were searched sued the officers who conducted the searches for trespass, and the government "undertook the responsibility of defending all actions arising from the warrant and the payment of all judgments."[26] To the delight of the British public,

---

[21] See LASSON, supra note 4, at 25-27.

> No limitations seem to have been observed in giving messengers powers of search and arrest in ferreting out offenders and evidence. Persons and places were not necessarily specified, seizure of papers and effects was indiscriminate, everything was left to the discretion of the bearer of the warrant.

Id. at 26; see also Cuddihy, supra note 16, at 100-19.

[22] LASSON, supra note Error! Bookmark not defined., at 45 (quoting Wilkes v. Wood, 98 Eng. Rep. 489 (C.D. 1763)).

[23] Cuddihy, supra note Error! Bookmark not defined., at 128; see also LASSON, supra note Error! Bookmark not defined., at 30-45.

[24] See Money v. Leach, 97 Eng. Rep. 1050 (K.B. 1765); Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765); Wilkes, 98 Eng. Rep. at 489; Huckle v. Money, 95 Eng. Rep. 768 (K.B. 1763).

[25] See Cuddihy, supra note Error! Bookmark not defined., at 886-94; see also LASSON, supra note Error! Bookmark not defined., at 43-45.

[26] LASSON, supra note Error! Bookmark not defined., at 45.

the plaintiffs won, and their verdicts were upheld on appeal.[27] Encouraged by their success, John Entick, the victim of a similar search, sued the officers who searched his home for trespass and won a verdict of £300.[28] The Court of Common Pleas upheld his verdict:

> [O]ur law holds the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave. [If] he does, he is a trespasser. . . . The defendants have no right to avail themselves of the usage of these warrants. . . . [W]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society.

The effect of these decisions was to apply the same standard to public and private actors: In either instance, a trespasser could be held civilly liable for entering another's property "without lawful authority".[30] The primary difference was that a public actor could rely upon a warrant, as well as upon a property owner's consent, as authorization for an entry.[31]

---

[27] Id. at 44-46.

[28] Id. at 47; see also Entick, 95 Eng. Rep. at 808:

> The plaintiff . . . declare[d] that the defendants [Nathan Carrington and three others, messengers in ordinary to the King] with force and arms broke and entered his dwelling-house . . . , continued there four hours without his consent and against his will, all that time disturbed him in the peaceable possession thereof, broke open the doors to the rooms, and the locks, . . . broke open the boxes, chests, drawers, etc., of the plaintiff in his house, . . . searched and examined all the rooms . . . in his dwelling . . . and all the boxes . . .; read over, pried into, and examined all the private papers . . . of the plaintiff there found, whereby the secret affairs, etc., of the plaintiff became wrongfully discovered and made public. . . to the damage of the plaintiff, 2,000 pounds.

Id.

[29] Entick, 95 Eng. Rep. at 818.

[30] WILLIAM BLACKSTONE, III, COMMENTARIES ON THE LAWS OF ENGLAND 209 (1870).

[31] As one scholar noted, a warrant "would act as a sort of declaratory

During this era, American colonists were waging their own war against writs of assistance, a variant of the general warrant.[32] Although their legal challenge to the writs failed,[33] the resentment generated was a driving factor for the Revolution and, later, in the adoption of the Bill of Rights.[34] The Fourth Amendment was therefore a product of the same concerns that resulted in the law of trespass' being applied to public actors: "to guard individuals against improper intrusion into their buildings where they had the exclusive right of possession".[35] It was intended to secure spatial privacy—to restrict law enforcement's ability to break down doors and rummage through rooms, boxes, chests, drawers, etc.[36] Like its English analogue, the Fourth Amendment was intended to preserve privacy by discouraging law enforcement trespasses,[37] and that conception of privacy prevailed unchallenged until the second decade of the Twentieth century when the Supreme Court heard its first wiretap case.

There were only a few Fourth Amendment cases in the Nine-

judgment . . . . A lawful warrant . . . would compel a . . . directed verdict for the defendant government official in any subsequent lawsuit for damages." Akhil Reed Amar, The Bill of Rights As A Constitution, 100 YALE L.J. 1131, 1178-79 (1991); see also Patcher v. Sprague, 1807 WL 931 (N.Y. 1807) (valid warrant is a defense to an action for trespass).

[32] See LASSON, supra note Error! Bookmark not defined., at 53 (with a writ of assistance one could "search any house, shop, warehouse, etc.; break open doors, chests, packages . . . and remove any prohibited or uncustomed goods or merchandise").

[33] Id. at 51-61.

[34] Id. at 79-82; see also Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978).

[35] Jones v. Gibson, 1818 WL 488 *5 (N.H. 1818).

[36] See supra note Error! Bookmark not defined..

[37] See, e.g., Humes v. Taber, 1850 WL 1823 *6 (R.I. 1850) (warrant no defense to an action in trespass against a sheriff who searched the wrong house); Jones, 1818 WL at *5 (action in trespass against an "inspector of revenue" for seizing goods without a warrant); Patcher v. Sprague, 1807 WL 931 (N.Y. 1807) (valid warrant is a defense to an action for trespass).

teenth century and perhaps the best known is *Boyd v. United States*. *Boyd* involved the "compulsory production of a man's private papers," which the Court found to be the "equivalent" of a search and seizure.[38] The Court struck down the practice in an opinion which cited *Entick* and seemed to fuse the Fifth Amendment's privilege against self-incrimination with the Fourth Amendment's prohibition against "unreasonable searches and seizures."[39] The opinion quotes *Entick* extensively for the proposition that an unauthorized violation one's "papers" is a trespass.[40] The focus was on spatial privacy—on the government's "*going*" or "*seeing*" something it should not—even though the "intrusion" was accomplished indirectly.[41]

---

[38] Boyd, 116 U.S. at 622. A court order was used to require "the claimants" in the case to surrender an invoice concerning the purchase of 29 cases of plate glass. Id. at 617-18. Order issued as part of an investigation into whether "the claimants" had unlawfully avoided paying duties on the glass. Id.

[39] Id. at 632-35.

[40] Id. at 626-30.

[41] See supra note Error! Bookmark not defined.. The Supreme Court cited Boyd's Fourth Amendment-Fifth Amendment fusion analysis in several cases, none of which involved the traditional Fourth Amendment scenario in which the government searches for and seizes evidence. See Bram v. United States, 168 U.S. 532, 544 (1897) (coerced confession case); Stone v. United States, 167 U.S. 178, 188 (1897) (action to recover damages for trees unlawfully cut on federally-owned land); Brown v. Walker, 161 U.S. 591, 635-36 (1896) (grand jury witness' appeal of contempt citation for refusing to answer questions put to him); Counselman v. Hitchcock, 142 U.S. 547, 580-81 (1892) (grand jury witness' appeal of contempt citation for refusing to answer questions put to him), overruled in part by Kastigar v. United States, 406 U.S. 441 (1972). See generally United States v. Zucker, 161 U.S. 475, 478 (1896). Many of these cases, along with some lower federal court decisions from this era, involved compelling testimony from witnesses. See, e.g., In re Jefferson, 96 F. 826, 828 (D. Wash. 1899) (compelling witness to testify against her husband would violate Fourth Amendment). David Steinburg writes:

> Federalism may in part explain the lack of early decisions interpreting the Fourth Amendment. In the eighteenth century and the nineteenth century, the Bill of Rights-including the Fourth Amendment-only applied to the federal government. During this same time period, most criminal laws were enacted by the states, not the federal government. Criminal prosecutions almost

1. Letters

The most relevant Nineteenth-century Supreme Court decision is *Ex parte Jackson*,[42] which was an appeal from a conviction for sending "a circular concerning a lottery" through the U.S. Mail.[43] In *Jackson*, the Court held that Congress had the power to prohibit mail from being used to deliver certain types of material as long as the restrictions were enforced in accordance with rights of:

> far greater importance than the transportation of the mail. . . . [A] distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, . . . and other printed matter, purposely left in a condition to be examined. Letters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon . . . oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. . . . [A]ll regulations adopted as to mail matter . . . must be in subordination to the great principle

always took place in the state courts, where the Fourth Amendment did not apply.

David E. Steinberg, The Original Understanding of Unreasonable Searches and Seizures, 56 FLA. L. REV. 1051, 1072-73 (2004) (footnotes omitted); see, e.g., Miller v. Texas, 153 U.S. 535, 538 (1894).

[42] 96 U.S. 727 (1877).

[43] Id.

> embodied in the fourth amendment of the Constitution.[44]

To the modern eye, *Jackson* seems to extract a concept of "portable privacy" from the notion of spatial privacy upon which the Fourth Amendment was predicated. Sealed letters and packages carry with them the privacy accorded the premises from which they originated; violating that privacy is a trespass which must be authorized by a warrant.[45] This appears to extend the original Fourth Amendment understanding of privacy as "privacy of place," to transcend the bricks-and-mortar approach meant to limit law enforcement intrusions into "private" physical spaces. To us, *Jackson* seems to anticipate *Katz*,[46] the Twentieth-century decision in which the Court expanded the Fourth Amendment to privacy beyond "space."[47]

It is doubtful that the *Jackson* Court viewed its holding in that light. It is more probable that the Court simply believed it was extending spatial privacy to "papers" which were in transit from one person to another—that were moving from one "private" space to another. Viewed in this light, the decision is but an application of the concern with spatial privacy and with the confidentiality of private "papers" that appears in *Entick* and the other English trespass decisions.[48] This interpretation is also supported by *Boyd*'s concern with non-traditional trespass into the privacy of one's "papers."[49]

But certain aspects of *Jackson* are still relevant to this discussion. For one thing, while *Jackson* did not specifically involve technology, it did provide the factual predicate for the holding. The colonial era postal service was ad hoc, notoriously

---

[44] Id. at 728 (emphasis added).

[45] See supra notes 37, 44 and accompanying text.

[46] 389 U.S. 347 (1967).

[47] Katz is discussed infra. See infra notes 117-127 and accompanying text.

[48] See supra note Error! Bookmark not defined..

[49] See supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text.

unreliable and offered no guarantees that what was sent would not be read by government authorities, postal employees or anyone who happened to have access.[50] The situation did not seem to improve much after the Revolution, with the establishment of a formal postal service.[51] In a letter to the Marquis de Lafayette, soon-to-be President George Washington observed that sending a letter through the post office meant that his words "should become known to all the world."[52] By the nineteenth century, postal employees were at least trying to maintain the "secrecy" of communications sent through the mail.[53] Interestingly, as Smith notes:

> [the] greatest protection for postal secrecy came not from a law or regulation, but from a physical innovation. In the mid-1800s adhesive envelopes were introduced, providing for the first time an easy means for sealing one's personal writings before entrusting them to the postal service.[54]

The self-sealing adhesive envelope was much more effective than its precursor, the wax-sealed envelope.[55] Thus, the *Jack-*

---

[50] See ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 23-26, 49-52 (2000). Colonists who were concerned about prying by Crown authorities developed codes to encrypt their letters. Id. at 24-26.

[51] Id. at 49-50.

[52] Id. at 50.

[53] Id. at 51-52.

> During the Nineteenth Century, it was the task of the Post Office to wipe out a tradition dating back to pre-Revolutionary times that intercepting mail and reading it was not especially uncommon—and to replace it with a new respect for confidential treatment of letters in transit. At mid-century, the task was not yet complete.

Id. at 54-55.

[54] Id. at 56.

[55] An 1873 New York Times editorial noted that a letter "`sealed with its red wafer, and into which the prying eyes of the village postmistress so often peeped, was soon superseded by the envelope, which secured the inviolability of the

son Court's distinction between sealed mail and other material was made possible by an innovation in communications technology.

Another pertinent aspect of *Jackson* was its focus on the privacy of communications. The mode of communication at issue in *Jackson* was not new but an innovation made it reasonable, for the first time, to expect that the contents of letters and parcels could be protected from "snoops and other members of the public."[56] Whatever its import for Fourth Amendment jurisprudence, this development is significant because it parallels issues which were arising regarding contemporaneous technology, and anticipating issues which would develop regarding evolving technology.

2. Telegraphy

In 1844, Samuel Morse sent the first public telegram using technology he developed in 1836.[57] After Morse formed his telegraph company, Western Union, in 1845, the growth of "the telegraph network was . . . explosive."[58] As lines were strung around the world, telegraphy "revolutionized business practice, gave rise to new forms of crime, and inundated its users with information."[59] For practical reasons, telegraphy did not give rise to the privacy issues that had arisen with regard to materials sent through the mail. Unlike the postal system, telegraphy was a proprietary communication system where the contents of communications were revealed to agents of the telegraph company, who translated the messages into Morse Code and transmitted them to another agent, who translated them back from Morse Code and then delivered them to the recipient.[60] The lack of an analogue to the sealed envelope meant it was not reasonable for those who employed telegraphy to claim that the privacy of their communications had been compromised by "insiders"—Western Union employees.[61]

---

contents from all eyes but those for which they were intended." Id. at 56.

[56] California v. Greenwood, 486 U.S. 35, 40 (1988).

[57] SMITH, supra note Error! Bookmark not defined., at 66; see also

There were, however, efforts to prevent the disclosure of telegram contents to "outsiders." Some states made it a crime for a telegraph company or its employees to disclose the contents to anyone but the authorized recipient.[62] Some also adopt-

TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS vii (1998).

[58] Id. at 56-91.

[59] Id. at vii.

[60] Id. at 63-65.

> Whatever personal information or sentiments were included in the message truly left the control of the originator. Further, unlike the situation with the U.S. Mail, an employee handling telegraph traffic could easily read messages without risking leaving the traces of an unopened envelope. There was no physical evidence of an interception. And, unlike the postal service, the telegraph system permitted the retention of every message.

SMITH, supra note Error! Bookmark not defined., at 66; see also Arthur W. Grumbine, The Era of Morse Telegraphy: Part 1, at http://www.faradic.net/~gsraven/telegraph_tales/grumbine/ grumbine_1.html (last visited Aug. 2005) ("[Telegraphy] was no different from opening everybody's mail and reading every word of it; then sending the contents across country by a peculiar code system invented by Samuel F. B. Morse").

[61] It would seem, of course, that messages could be encrypted to preserve the privacy of their contents, but this did not become a common practice:

> When it was first introduced, many people anticipated that telegraphic transmission would be far more secure than the Postal Office had been and that it would provide "impenetrable secrecy," because the messages were coded, or could be coded. But coding was not used for most business and personal correspondence. (The main reason was that a sender could recover damages caused by errors in transmission by the telegraph company but when it transmitted encoded messages its liability was significantly lower).

SMITH, supra note Error! Bookmark not defined., at 67. See, e.g., Primrose v. W. Union Tel. Co., 154 U.S. 1, 4-5 (1894) (suit seeking damages for mistake made in transmitting coded telegraphic message); Postal Tel.-Cable Co. v. Louisville Cotton Oil Co., 122 S.W. 852, 852-53 (Ky. Ct. App. 1909) (suit for damages resulting from failure to deliver coded telegraphic message). Criminals sometimes encrypted messages used to facilitate criminal activity. See, e.g., State v. Chapman, 1871 WL 3337, at *5 (Nev. 1871) (accomplice sent a "cipher telegram" advising robbers when a large shipment of coins would be arriving).

[62] See MINN. GEN. STAT. § 6782 (1894) (cited in Peterson v. W. Union

ed statutes creating a cause of action for those whose messages went awry or were otherwise made public.[63] Some observers were concerned about the possibility that Western Union would disclose the contents of messages to authorities. This became a reality in 1877, when a Congressional committee, investigating the validity of votes cast in certain states, sought access to telegrams as evidence.[64]

> Western Union President William Orton ordered [his employees] not to respond. He accused Congress of requiring his employees `to become spies and . . . informers against the customers who have reposed in us the gravest confidence concerning both their official and their private affairs.' . . . With Democrats supporting disclosure and Republicans supporting confidentiality, the Western Union manager was found in contempt of Congress . . . arrested by a deputy sergeant of arms on Capitol Hill and detained.[65]

Telegraph Co., 77 N.W. 985, 987 (Minn. 1899); 13 WAGNER'S STATUTES § 51 (cited in Ex parte Brown, 1880 WL 423, at *4 (Mo. 1880)); see also Little Rock & Fort Smith Tel. Co. v. Davis, 1883 WL 1201, at * 3 (Ark. 1883) (noting state statutes imposing civil liability and criminal penalties) (citing SCOTT & JARNAGAN, LAW OF TELEGRAPHS §§ 419-46). The efficacy of these laws, which were enacted in "a bare majority" of states," is uncertain. See, e.g., SMITH, supra note Error! Bookmark not defined., at 68. A New York Times editorial from 1866 claimed that violations of these laws were hard to detect and that Western Union employees were subject to "`strong temptations'" to ignore them. Id. (quoting The New York Times, December 31, 1866, at 4).

63 See VA. CODE ANN. § 2900 (Michie 1900):

> [T]elegraph companies shall be liable for special damages occasioned in . . . delivering dispatches, or for the disclosure of the contents of any private dispatch to any person other than to him to whom it was addressed, the amount of these damages to be determined by the jury upon the facts in each case. Grief and mental anguish occasioned to the plaintiff may be considered by the jury in the determination of the quantum of damages.

(quoted in Connelly v. W. Union Tel. Co., 40 S.E. 618, 622 (Va. 1902)); see also IND. REV. STAT. § 5513 (1894) (cited in W. Union Tel. Co. v. Bierhaus, 36 N.E. 161, 162 (Ind. Ct. App. 1894)).

64 See SMITH, supra note Error! Bookmark not defined., at 68.

65 Id. at 68-69; see also ERNEST J. EBERLING, CONGRESSIONAL INVESTIGA-

Orton eventually gave in; Western Union delivered "30,000 political telegrams . . . to the House Committee on Privileges and Elections in the winter of 1877."[66]

The messages, however, were never used in the investigation,[67] but the episode sparked a debate about the confidentiality of telegrams. Congressman James Garfield argued for legislation guaranteeing confidentiality, but other members of Congress believed that the "`security of society'" was more important than confidentiality.[68] Over the next few years, Congress debated whether telegrams "should be compared to Post Office material and therefore kept confidential" or "should be available by subpoena."[69] For the public, confidentiality "was a double-edged sword: a requirement of non-disclosure or of instant destruction of messages would protect privacy but also allow the company to escape liability for errors", since the evidence would have been destroyed.[70] Western Union responded by reducing the retention time for copies of messages, and in 1880 a House Committee "reported out favorably a bill . . . to protect telegrams to the very same extent as sealed letters in the Post Office."[71] The House did not act on the bill and the proposal died, in part because of events occurring elsewhere.[72] In 1880, Jay Gould, "perhaps the most hated capitalist of America's

TIONS: A STUDY OF THE ORIGIN AND DEVELOPMENT OF THE POWER OF CONGRESS TO INVESTIGATE AND PUNISH FOR CONTEMPT 231-46 (1928). See generally United States v. Babcock, 24 F. Cas. 908 (C.C. Mo. 1876) (ruling on Orton's motion to vacate subpoena requiring production of the telegrams).

66 SMITH, supra note Error! Bookmark not defined., at 69.

67 Id.

68 Id. A Kentucky Congressman said Garfield had a "`newfangled sentimentality'" about the confidentiality of telegrams. Id.

69 Id.

70 Id.

71 Id. at 70.

72 Id.

Gilded Age," acquired Western Union.[73] The public's distrust of Gould led to demands that the government take over Western Union, both to prevent price gouging and to protect the privacy of telegraphic messages.[74] The debate over government acquisition of Western Union continued for years and finally ended when Jay Gould died in 1892;[75] by then, the public's reliance on telegraphy was being replaced by a new technology—the telephone.[76]

When Gould died, the Bell Telephone Company had been in existence for fifteen years.[77] "Boston and New York were talking to Chicago, Milwaukee, Pittsburg, and Washington.

---

[73] Id.

[74] Id. at 70-71.

[75] Id. at 71.

[76] Ronnie J. Phillips, Digital Technology and Institutional Change from the Gilded Age to Modern Times: The Impact of the Telegraph and the Internet, 34 J. OF ECON. ISSUES 267, 276-77 (2000), at http://diglib.lib.utk.edu/utj/jei/34/jei-34-2-3.pdf (last visited Aug. 2005).

> It was a competing technology that ultimately destroyed the Western Union monopoly. With the greatly increased demand for the telegraph in the period after the Civil War, the search began for the creation of a "harmonic telegraph" that would enable the simultaneous transmission of multiple messages. In the 1890s, Alexander Graham Bell was teaching deaf mutes in Boston. Two local wealthy businessmen, who each had a deaf child, were impressed by Bell's personality and decided to back him in the race to beat Western Union in the development of a practical harmonic telegraph. While working on the harmonic telegraph, Bell discovered by accident the principles of the telephone. The new technology was demonstrated at the Centennial Exposition of 1876 in Philadelphia.
>
> After a patent dispute with Bell Telephone, in November 1879 Western Union formally contracted to relinquish the rights to the new telephone technology to Bell, under the assumption that the new technology would not challenge the telegraph. Bell Telephone, formed in May 1877, was an immediate success. . . . [W]ithin three years there were 30,000 phones in use around the world. In 1886, there were more than 250,000 phones in use worldwide. By the turn of the century, the telegraph had seen its heyday.

Id.

[77] See supra note Error! Bookmark not defined..

One-half of the people of the United States were within talking distance of each other."[78] It had been transmitting a million messages a day since 1888, install its first million telephones in 1898, and would string its first million miles of wire in 1900.[79] "A new generation had grown up, without the prejudices of its fathers. People had grown away from the telegraphic habit of thought, which was that wire communications were expensive luxuries for the few."[80]

3. Telephony

Telephones were less expensive to use than telegraphy, and they held out the possibility of providing more confidentiality because one could communicate directly, instead of relying on telegraph agents to code, transmit, and de-code the contents of the communication.[81] However, the early telephone system was not actually secure because it was not a truly automated system:

> One "party line" would serve four or more customers. Simply by picking up the telephone, . . . customers could hear the conversation of another if the line were in use. . . . [T]his was common because a party-line customer would have no other way of knowing whether the line was free . . . except to pick up the phone and listen. There was no dial tone in those days; . . . operators would direct the call manually at a switchboard. In small towns, you could simply ask the operator for the name of the person you wanted to reach. . . . If the operator had . . . tried to place a call to the same person and gotten no answer, she might tell the caller that

---

[78] HERBERT N. CASSON, THE HISTORY OF THE TELEPHONE 183 (1910); see also supra note Error! Bookmark not defined..

[79] CASSON, supra note 78, at 182.

[80] Id. at 178; see also JOHN W. OLIVER, HISTORY OF AMERICAN TECHNOLOGY 440 (1956) ("The telephone, unlike the telegraph . . ., was the instrument of, and for, the people. It served individuals of limited means as efficiently as the man of wealth.").

[81] See supra note Error! Bookmark not defined. and accompanying text.

> the person wasn't home . . . [O]perators knew who was talking with whom, if not the content of the conversation.[82]

The lack of privacy led a Kansas City undertaker named Almon Strowger to invent an "automatic telephone switching system that dispensed with operators."[83] Strowger patented his device in 1882; it was implemented in Indiana in 1892 and by 1918 it had become the norm for automatic exchanges in the United Kingdom.[84] The Bell system was much slower to adopt automated switching,[85] but by the 1920's it had substantially re-

---

[82] SMITH, supra note Error! Bookmark not defined., at 155; see also John Bray, THE COMMUNICATIONS MIRACLE: THE TELECOMMUNICATION PIONEERS FROM MORSE TO THE INFORMATION SUPERHIGHWAY 56 (1995):

> The problem of connecting a calling to a called customer was at first solved by manually operated telephone exchanges in which an operator simply plugged in a cord between the corresponding incoming and outgoing telephone line terminals on a switchboard. This system had the advantage that it provided, from the customer viewpoint, good service since the operator could, in systems with small numbers of lines, readily find the called customer by name, and answer queries made by the caller. But it became cumbersome when large numbers of lines were involved, a difficulty only partially solved by the use of `multiple' switchboards with groups of operators. And there was the inherent problem of `overhearing' the customers' telephone conversations by the operators and the consequent lack of privacy.

Id.

[83] BRAY, supra note Error! Bookmark not defined., at 57. "Strowger found that he was losing money in his undertaking business because one of the switchboard operators at the Kansas City telephone exchange was married to a rival undertaker and she would connect Strowger's callers wishing to make funeral arrangements to her husband." Id.

[84] Id. at 59.

[85] Id. One reason was a concern that automated switching could not efficiently handle the volume of phone traffic in large cities. See, e.g., Joan Nix & David Gabel, The Introduction of Automatic Switching into the Bell System: Market versus Institutional Influences, 30 J. OF ECON. ISSUES 737, 744 (1996).

Another belief that shaped AT&T's behavior toward automatic switching is

placed the operator-assisted system, at least in urban areas.[86]

Once automated switching was introduced, "Americans became comfortable using the telephone for personal and sensitive matters"[87] because they assumed their telephone conversations were confidential or "private." This was, however, an unresolved issue because the introduction of automated switching eliminated operator involvement and essentially resolved the "insider" problem, i.e., the concern that telephone employees would listen in on conversations[88] but it left the "outsider" problem. The outsider problem was the possibility that persons not associated with the telephone company would listen in on what the parties believed to be "private" telephone conversations.

This possibility was not unique to telephonic communication. Technology that could be used to tap telegraphic communications emerged soon after the invention of the telegraph.[89] During the Civil War, the Union and Confederate armies tapped each other's telegraphic communications to obtain infor-

---

> related to the perception of the proper role of customers in placing a call. Despite an abundance of information that customers preferred to dial on their own, a consensus was reached that in selecting technology, equipment should be selected that did not require customers `to do part of the service.' . . . . AT&T's management believed that keeping customer involvement to a minimum would enhance the popularity of telephony. . . . [T]he management of AT&T held on to the ideological presupposition that customers possessed limited capabilities for comprehending the steps involved in dialing a phone.

Id. (footnotes omitted).

[86] Id.; see also Richard R. John, The Politics of Innovation, 127.4 DAEDALUS 187, 206 (1998) ("Not until the 1920s, with the widespread introduction of the dial telephone, would Bell democratize telephony by permitting subscribers to hold a telephone conversation without having to rely on . . . operators to make the connection.").

[87] SMITH, supra note Error! Bookmark not defined., at 156.

[88] Id. That, of course, was not possible with telegraphy.

[89] Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 GEO. WASH. L. REV. 1264, 1270 (2004).

mation about battle plans and troop movements and after the war rival newspapers tapped each other's wire communications in an effort to be the first to report major stories.[90] Some states had enacted laws making it a crime to intercept telegraphic communications,[91] but there was no federa legislation on point.[92] It is possible that because law enforcement did not ap-

[90] Id. (quoting PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995)). "Interception of telegrams [during the Civil war] was such a threat that the Union army began using cipher codes to encrypt messages; only generals and the War Department possessed the codes." Thomas F. O'Neill III, Kevin P. Gallagher & Jonathon L. Nevett, Detours On The Information Superhighway: The Erosion Of Evidentiary Privileges In Cyberspace And Beyond, 1997 STAN. TECH. L. REV. 3, 4 (1997).

[91] See SMITH, supra note Error! Bookmark not defined., at 157. See, e.g., 1862 CAL. STAT. 288 (cited in Andrew Ayers, Note, The Police Can Do What? Making Local Governmental Entities Pay For Unauthorized Wiretapping, 19 N.Y.L. SCH. J. HUM. RTS. 651, 657 n.63 (2003)).

[92] See SMITH, supra note Error! Bookmark not defined., at 157. See, e.g., Ex parte Brown, 1880 WL 4234 at *5 ("Telegraphic messages are not privileged communications. . . . No statute of this State, or of the United States, has made them so."). There seems to have been little effort to apply Jackson's Fourth Amendment standard to telegrams. In Brown, the petitioner apparently did argue for this, contending that "the letter and telegram, so far as the incidents of transmission are concerned, should stand upon the same basis. . . . That the government sends the letter, and a private corporation the telegram, does not affect the principle." Brown, 1880 WL at *4. The court disagreed:

> That mode of communication is of recent origin, and, therefore, the common law furnishes nothing but analogies for our guide. Telegraphic lines are not operated by the government . . . . On the other hand postal facilities were established by Congress; the mails are carried by the government through its own agents, and penal statutes protect communications sent through the mail. The entire postal system is under the control and management of the government. . . . There is no such analogy between the transmission of communications by mail, and their tranmission by telegraph, as would justify the application to the latter of the principles which obtain with respect to the former.

Id. at *5; see also Martin v. Sheriff, 1894 WL 1440 (Ohio Prob. 1894) ("It is not a crime, under the laws of Ohio, to tap a telegraph wire."). There were, however, occasional references to the use of warrants to obtain telegraphic messages.

pear to have used wiretaps when investigating crimes,[93] this was not a topic of hot dispute for the public as of yet.

For whatever reason, law enforcement approached the telephone differently: Police had begun to tap telephone conversations at least by the 1890's.[94] The practice, which was not encompassed by state laws outlawing the interception of telegraphic communications, continued for years, becoming the focus of a controversy in 1916. The New York City Police were found to have intercepted telephone conversations with the assistance of the telephone company.[95] The police contended there was no impropriety given the realities of the then-prevalent operator-assisted telephone system: "Telephone conversations . . . cannot be private in the way that letters can be, since the employees of the telephone company cannot help hearing parts of conversations and may, if they are inclined, easily hear all."[96] During this era, there was no telephonic analogue of the sealed envelope.[97]

In the 1920's, the implementation of automated switching gave rise to the perception that telephone conversations were private, just as sealed mail was private.[98] This led to greater

---

[93] This may have been due to the fact that "original drafts of telegrams filed with clerks for dispatch, as well as the telegraph company's copies of the received messages, had to be produced for court trials and legislative investigations." John D. Woodward, Biometric Scanning, Law & Policy: Identifying The Concerns-Drafting The Biometric Blueprint, 59 U. PITT. L. REV. 97, 119 n.177 (1997) (citing ALAN F. WESTIN, PRIVACY AND FREEDOM 337 (1st ed. 1967)).

[94] See, e.g., Ayers, The Police Can Do What?, supra note 91, at 658 (in the early 1890's, New York police were the first to tap telephones) (citing WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 155 (1998)). Telephone tapping apparently began much earlier: "In 1881, only five years after the invention of the telephone, a patent was issued for a scrambler that thwarted telephone tappers." Id. at 657.

[95] Id. (citing SAMUEL DASH ET AL., THE EAVESDROPPERS 25 (1959)).

[96] Police Espionage in a Democracy, OUTLOOK 235 (May 31, 1916) (quoted in SMITH, supra note Error! Bookmark not defined., at 157).

[97] See supra note 55 and accompanying text.

[98] See supra note 86 and accompanying text.

use of telephones by the public, and by those engaged in unlawful activities; this, in turn, resulted in the Supreme Court's considering whether the Fourth Amendment constrained police wiretapping.[99] The issue in *Olmstead v. United States* was "whether the use of evidence of private telephone conversa-

[99] Prior to Olmstead, only a few reported decisions addressed wiretapping, mostly in the context of prosecutions under statutes that made it a crime to intercept telegraph or telephone messages. See, e.g., State v. Behringer, 172 P. 660, 619 (Ariz. 1918) (holding it was not a violation of Arizona Penal Code section 692—which made it unlawful "by means of any machine, instrument or contrivance" to read or attempt to read "any message, or to learn the contents thereof, whilst the same is being sent over any telegraph or telephone line"—to place a dictograph over the transom of a room and thereby hear what was said over a telephone); see also Olmstead, 277 U.S. at 479 n.13 (Brandeis, J., dissenting) (listing statutes that made it a crime to intercept telephone or telegraph messages).

Police wiretapping seems to have been idiosyncratic. See Orin S. Kerr, The Fourth Amendment And New Technologies: Constitutional Myths And The Case For Caution, 102 MICH. L. REV. 801, 841 n.229 (2004) ("[I]t appears that some state police agencies wiretapped defendants, but others did not."). See, e.g., People v. Hebberd, 96 Misc. 617, 162 N.Y.S. 80 (N.Y. Sup. Ct. 1916). In State v. Nordskog, 136 P. 694 (Wash. 1913), the Washington Supreme Court reversed the conviction of a former detective and "professional wire tapper" for "damaging" a telephone line. The court based the conviction solely on his having tapped the line to intercept a message. See id. at 694-95. It found that the mere act of tapping the line inflicted no damage, but it also noted the need for legislation to prevent further such acts:

> [T]here has been altogether too much of this form of pilfering going on in this state, and the omission of the law now disclosed calls aloud for legislative action . . . . [T]he law should be so framed that the privacy of all citizens . . . may be protected, and that any tampering or interference, however slight, that is not done under the rules of the company and by its agents, or under some regulation of the public service commission, may be prohibited.

Id. at 695; see also Robilio v. United States, 291 F. 975, 982-83 (6th Cir. 1923) (upholding the admissibility of evidence obtained by wiretapping the home of the defendant against evidentiary challenges as to its authenticity; no challenge was based on the act of wiretapping itself); People v. McDonald, 165 N.Y.S. 41, 44-45 (N.Y. App. Div. 1917) (refusing to suppress evidence obtained

by tapping the home of the defendant on the grounds that under New York law it was immaterial how the state obtained the evidence and that the Fourth Amendment did not apply to the states, only to the federal government).

tions . . . intercepted by means of wire tapping, amounted to a violation of the Fourth and Fifth Amendments."[100] Prohibition officers had installed wiretaps on telephone lines leading from the residences of suspected bootlegger Roy Olmstead and three of his associates.[101] The government used the information obtained by the wiretaps to prosecute Olmstead and the others for violating prohibition laws.[102] Since the taps were connected to the telephone lines as they ran toward the residences, there was no physical intrusion into the homes.[103]

---

[100] 277 U.S. 455 (1928).

[101] Olmstead, a former Seattle police lieutenant, had become the biggest bootlegger in western Washington. See W. MURPHY, WIRETAPPING ON TRIAL: A CASE STUDY IN THE JUDICIAL PROCESS 16 (1965); 277 U.S. at 455-56:

> The evidence . . . discloses a conspiracy of amazing magnitude to import, possess, and sell liquor unlawfully. It involved . . . not less than 50 person s, . . . two seagoing vessels for the transportation of liquor . . ., the maintenance of a central office manned with operators, and the employment of executives, salesmen, 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 two millions of dollars.

Id. Olmstead was the "leading conspirator and the general manager of the business" which utilized telephones in its operations:

> Of the several offices in Seattle, the chief one was in a large office building. In this there were three telephones on three different lines. There were telephones in an office of the manager in his own home, at the homes of his associates, and at other places in the city. Communication was had frequently with Vancouver, British Columbia. Times were fixed for the deliveries of the "stuff" to places along Puget Sound near Seattle . . . . One of the chief men was always on duty at the main office to receive orders by the telephones and to direct their filling by a corps of men stationed in another room . . . . The call numbers of the telephones were given to those known to be likely customers.

Id. at 456.

[102] See id. at 455 ("The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act . . . by unlawfully possessing, transporting and importing intoxicating liquors and . . . by selling intoxicating liquors").

[103] See id. at 456-57:

In an opinion by Chief Justice Taft, a majority of the Court held that the Fourth Amendment[104] did not apply because there was no trespass:[105] "The language of the amendment cannot be . . . 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."[106] Justice Taft was careful to distinguish telephone conversations from

> [I]nformation . . . was . . . obtained by intercepting messages on the telephones of the conspirators . . . . Small wires were inserted along the . . . telephone wires from the residences of . . . the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.

[104] The Court found there was no basis for applying the Fifth Amendment because there was "no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the Fourth Amendment." Id. at 462.

[105] See id. at 466:

> The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them are not within the protection of the Fourth Amendment. . . .
>
> We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

See id. at 457 (The taps were installed "without trespass upon any property of the defendants."); see also id. at 465 ("`The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted.'") (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

In affirming Olmstead's conviction, the Ninth Circuit explicitly noted the need for a physical trespass: "[The amendment] has never been extended to the exclusion of evidence obtained by listening to the conversation of persons . . . . The purpose . . . is to prevent the invasion of homes and offices and the seizure of incriminating evidence found therein." 19 F.2d 842, 847 (9th Cir. 1927).

[106] Id. at 465.

letters:

> It is urged that the language of Mr. Justice Field in Ex parte Jackson . . . offers an analogy to the interpretation of the Fourth Amendment in respect of wire tapping. But the analogy fails. . . . It is plainly within the words of the amendment to say that the unlawful rifling by a government agent of a sealed letter is a search . . . of the sender's papers of effects. The letter is a paper, an effect. . . .[107]

Justice Brandeis famously dissented, arguing that the "Fourth Amendment must adapt to a changing world."[108] He pointed out that when the amendment was adopted, force was

> the only means known to man by which a government could directly effect self-incrimination. . . . It could secure . . . papers and other articles . . . by breaking and entry. . . . But `time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government . . . .The progress of science . . . is not likely to stop with wire tapping. Ways may . . . be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and . . . expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[109]

After *Olmstead*, wiretapping might violate state law, but it was constitutionally permissible; Congress considered banning it, but ultimately did nothing.[110] In 1935, Congress adopted the

---

[107] Id. at 464. Justice Taft also held that there was no seizure because the evidence "was secured by the use of the sense of hearing and that only." Id.

[108] Id. at 474.

[109] Id. at 473-74.

[110] See Nardone v. United States, 302 U.S. 379, 382 (1937) ("Congressional committees investigated the wire-tapping activities of federal agents. . . . [B]ills were introduced to prohibit the practice, all of which failed to

Federal Communications Act for reasons having nothing to do with *Olmstead*;[111] section 605 of the Act prohibited intercepting a communication without the permission of the sender and divulging or publishing the contents.[112] In 1937, the Supreme Court held that § 605 applied to federal officers, and that evidence obtained in violation of the statute was inadmissible in federal prosecutions.[113] Two years later, it expanded its holding to encompass evidence derived from the use of wiretaps.[114] The Department of Justice took the position that § 605 did not prohibit wiretapping for "purely investigative purposes", and therefore continued to conduct electronic surveillance over the next three decades.[115] During this era, the Supreme Court occasionally heard cases involving the use of wiretaps or other types of surveillance, and always held that, absent a physical trespass, such activity was outside the Fourth Amendment.[116]

In 1967, the Supreme Court reversed *Olmstead* and held that FBI agents violated the Fourth Amendment by installing an "electronic listening and recording device" on the *outside* of a

pass.").

111 See id.

112 See Ch. 652, Title VI, § 605, 48 Stat. 1103 (1934), as amended, 47 U.S.C. § 605.

113 See Nardone, 302 U.S. at 383-84.

114 See Nardone v. United States, 308 U.S. 338, 341-42 (1939).

115 See David S. Eggert, Note, Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches, 1983 DUKE L.J. 611, 621-22; see also Ken Gormley, One Hundred Years of Privacy, 1992 WIS. L. REV. 1335, 1362-66.

116 See, e.g., Goldman v. Unites States, 316 U.S. 129, 135-36 (1942) (declining to overrule Olmstead); Goldstein v. United States, 316 U.S. 114, 121-22 (1942) (Fourth Amendment did not apply to wiretapping but evidence obtained in violation of § 605 was inadmissible); see also Silverman v. United States, 365 U.S. 505 (1961) (use of spike mike which penetrated party wall and turned heating system serving petitioners' premises into a "conductor of sound" was a trespass and therefore a search under the Fourth Amendment); Irvine v. California, 347 U.S. 128, 131-32 (1954) (police entries into home to install microphone in closet and in a hall was a violation of the Fourth Amendment).

telephone booth to record calls being made by Charles Katz.[117] Katz was convicted of violating section 1084 of the United States Code, which makes it a crime to use facilities of interstate commerce to transmit wagering information.[118]

> The conviction was based on six tape recordings, averaging three minutes each, of his end of telephone conversations placed from three public phone booths. The recordings were obtained . . . by means of an electronic listening device attached to the outside of the booths; there was no physical penetration of the . . . booth . . . . . The eavesdropping was conducted only after an investigation indicated that Katz regularly used these phones to call a known gambler. No effort was made, however, to obtain judicial authorization for the eavesdropping.[119]

Katz raised two issues in his appeal, both of which involved the relationship between the Fourth Amendment and a "constitutionally protected area."[120] The Court declined to accept his formulation, explaining that the resolution of "Fourth Amendment problems is not . . . promoted by incantation of the phrase `constitutionally protected area.'"[121] The majority went on to announce a new Fourth Amendment standard:

> [T]he parties have attached great significance to the . . . telephone booth from which the petitioner placed his calls. The petitioner has . . . argued that the booth was a `constitutionally protected area.' The Government has maintained . . . that it was not. But this effort . . . deflects attention from the problem presented by this case. For the

---

117 Katz v. United States, 389 U.S. 347, 348 (1967).

118 See id. at 348-49.

119 Electronic Surveillance, 82 HARV. L. REV. 187, 187 (1968)

120 See 389 U.S. at 350-51. To this point in history, Fourth Amendment violations occurred only when there was a physical trespass onto a "constitutionally protected area." See, e.g., Erik G. Luna, Sovereignty and Suspicion, 48 DUKE L.J. 787, 793 n.20 (1999).

121 389 U.S. at 350.

> Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[122]

The majority then overruled *Olmstead,* explaining that "once it is recognized that the Fourth Amendment protects people—and not simply `areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[123]

In a concurrence, Justice Harlan articulated the standard that has been used to implement the *Katz* holding:[124]

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question . . . is what protection it affords to those people. . . . My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy . . . . On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[125]

It is important to note that Justice Harlan interpreted the

---

122 Id. at 351 (citations omitted).

123 Id. at 353.

124 The Court adopted his "reasonable expectation of privacy" standard in Terry v. Ohio, 392 U.S. 1, 9 (1968), and has applied it ever since. See infra Section I.A.4.

125 Id. at 361 (Harlan, J., concurring).

majority's opinion as holding "only" (i) that a telephone booth is an area in which one "has a constitutionally protected reasonable expectation of privacy"; (ii) that electronic invasions, as well as physical invasions, of such an area can violate the Fourth Amendment; and (iii) that the invasion of a "constitutionally protected area" without a warrant is presumptively unreasonable.[126] His standard therefore implicitly incorporates the spatially-based conception of privacy that had prevailed since *Olmstead*.[127]

[126] Id. at 360-61.

[127] See supra note Error! Bookmark not defined.. This is evident in his comment that the rule he cites "emerged from prior decisions'"; supra note 120 and accompanying text. Those decisions were, by necessity, based on Olmstead's trespass doctrine.

4. Other technology[128]

In *United States v. Knotts*,[129] the Supreme Court applied *Katz* to hold that "the warrantless monitoring of an electronic tracking device ("beeper") inside a container of chemicals did not violate the Fourth Amendment when it revealed no information that could not have been obtained through visual surveillance."[130] The Court found that the information provided by the beeper was nothing more than what the officers could have learned by following the vehicle carrying the container as it traveled to a private cabin:[131]

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements . . . . When Petschen travelled . . . 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

---

[128] The discussion of Supreme Court cases in this section is selective: It is limited to cases that have dealt with the use of new communicative technologies, as defined in supra note Error! Bookmark not defined.. The Court has used the Katz standard to decide whether a wide variety of police conduct constitutes a "search" under the Fourth Amendment. See, e.g., Florida v. Riley, 488 U.S. 445, 450-51 (1989) (not a search fly over greenhouse in a helicopter and observe marijuana plants through gaps in its roof); California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (not a search for police to fly over backyard in commercial airspace and view marijuana being grown there); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (not a search to fly over chemical plant and photograph premises). The "technologies" at issue in these cases were simply tools police used to gain a favorable physical vantage point from which to make observations with the unaided, or aided, naked eye; these cases did not involve the type of pervasive, autonomous technologies analyzed in this article. See infra Section II.

[129] 460 U.S. 276 (1983).

[130] United States v. Karo, 468 U.S. 705, 707 (1984).

[131] Officers suspected Knotts and others of buying chemicals and using them to manufacture "illicit drugs." See Knotts, 460 U.S. at 277-78. They therefore installed the beeper in a can of chemicals and used it to monitor Darryl Petschen as he drove the can to a cabin owned by Knotts. See id. at 278-79.

> destination when he exited from public roads onto private property.
>
> . . . Knotts, as the owner of the cabin . . . to which Petschen drove, undoubtedly had the traditional expectation of privacy . . . insofar as the cabin was concerned . . . . But no such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway.[132]

The Court reached the opposite conclusion in *United States v. Karo*.[133] When DEA agents learned that James Karo and his associates had ordered fifty gallons of ether, the agents concluded that the chemical would be used to manufacture drugs.[134] They arranged to have a beeper installed in one of the cans of ether and used it to track Karo as he drove the cans to his house.[135] On two occasions, they used the signal from the beeper to determine that (i) it was still in Karo's house and (ii) it had been moved to the home of one of his associates.[136] The Supreme Court applied *Katz* to hold that these latter uses violated the Fourth Amendment:

> [P]rivate residences are places in which the individual . . . expects privacy . . . and that expectation is plainly one that society is prepared to recognize as justifiable . . . . In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation

---

132 Id. at 281-82 (citations omitted).

133 468 U.S. 705, (1984).

134 See id. at 708-09.

135 See id.

136 See id.

> from outside the curtilage of the house.[137]

The Court reached a similar conclusion in *Kyllo v. United States*,[138] its most recent parsing of the *Katz* standard. The issue in *Kyllo* was whether "the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a `search' within the meaning of the Fourth Amendment."[139] Federal agents who suspected Danny Kyllo was growing marijuana in his home used a thermal imager to detect heat signatures in his home and garage:

> The scan . . . took only a few minutes and was performed from . . . Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was.[140]

Indicted for manufacturing marijuana, Kyllo moved to suppress the results of the thermal imaging on the grounds that the scan was a warrantless search conducted in violation of the Fourth Amendment.[141] He eventually pled guilty while reserving the right to pursue this issue on appeal.[142] The Ninth Circuit ultimately rejected Kyllo's argument, holding that he had "shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home"

---

137 Id. at 714-15 (citations omitted).

138 533 U.S. 27 (2001).

139 Kyllo, 533 U.S. at 29.

140 Id. at 30.

141 See id. at 30.

142 See id.

and that "there was no objectively reasonable expectation of privacy because the imager `did not expose any intimate details of Kyllo's life,' only `amorphous "hot spots" on the roof and exterior wall.'"[143]

The Supreme Court reversed:[144]

> [T]he Fourth Amendment draws "a firm line at the entrance to the house." That line . . . must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.
>
> "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens."
>
> 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" and is presumptively unreasonable without a warrant.[145]

---

143 Id. at 31.

144 See id. at 41.

145 Id. at 40 (citations omitted) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

Like Justice Taft, this post-Olmstead Court quotes Carroll v. United States, 267 U.S. 132, 149 (1925), for the proposition that Fourth Amendment construction is embedded in time, i.e., is based on what was deemed unreasonable when it was adopted. See supra note Error! Bookmark not defined.. Justice Taft used the quoted passage to buttress his conclusion that wiretapping unaccompanied by physical intrusion into the home was not a violation of the Fourth Amendment. See supra note 105. In Kyllo, Justice Scalia used it to support his conclusion that technology cannot be utilized as a substitute for physical intrusion. See Kyllo, 533 U.S. at 40.

As these cases demonstrate, despite its disavowal of a spatial conception of privacy in *Katz*, the Supreme Court continues to predicate Fourth Amendment privacy upon spatial constraints, that is, upon the occurrence of some type of "intrusion" into a private "place." In *Kyllo* and *Karo*, the "intrusion" is not a physical trespass; it results from the use of technology to extract information that would otherwise be unavailable from a private space. We return to this issue in Section I.C.

B. Third-party records

> *Recent inventions and business methods call attention to the next step which must be taken . . . for securing to the individual what Judge Cooley calls the right "to be let alone."*[146]

In 1890 Samuel Warren and Louis Brandeis published their famous article, *The Right to Privacy*.[147] Unlike the Fourth Amendment right discussed above,[148] the Warren-Brandeis right (i) was directed at private parties and (ii) did not involve a zero-sum approach to privacy.[149]

Warren and Brandeis were reacting to changes in society and in technology.[150] America was increasingly industrial and urbanized.[151] The urban population provided a market for the new "yellow journalism;" newspapers shifted from political coverage

---

146 Samuel Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890) (quoting THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888)), available at http://www.louisville.edu/library/law/brandeis/privacy.html (last visited Aug. 15, 2005).

147 See id.

148 See supra Section I.A.

149 See Warren & Brandeis, supra note Error! Bookmark not defined..

150 See Gormley, supra note Error! Bookmark not defined., at 1350.

151 See id.

to emphasizing "`sin, sex and violence.'"[152] Advances in photography, such as Eastman's hand-held camera, let amateurs to take "candid" photographs, often clandestinely.[153] These and other forces combined to create a culture in which journalists spied on the socially-prominent,[154] in which individuals had no recourse if their likeness was used for commercial purposes without their knowledge or permission,[155] and in which the use of eavesdropping devices threatened "to make good the prediction that `what is whispered in the closet shall be proclaimed from the house-tops.'"[156]

The Fourth Amendment offered no protection from these activities because it only applies to state action.[157] The "evils" Warren and Brandeis were addressing resulted from the efforts of private citizens, which is why they ultimately cast their right to privacy as a tort: Those whose privacy was violated could bring an "action of tort for damages in all cases" and could seek an injunction "a very limited class of cases."[158] This aspect of

---

[152] Id. at 1351 (quoting EDWIN EMERY & MICHAEL C. EMERY, THE PRESS AND AMERICA: AN INTERPRETATIVE HISTORY OF THE MASS MEDIA 349-50 (3d ed. 1972)).

[153] See SMITH, supra note Error! Bookmark not defined., at 124. Until 1884, when Eastman invented his hand-held camera, photography "was so cumbersome and the sittings so prolonged that . . . no one's image was captured without their fully knowing it." Id. Eastman's invention made it possible, for the first time, for a stranger to photograph someone without their knowledge or permission. See id. While we are accustomed to this, very few people in the years leading up to Eastman's invention would ever have seen an image of themselves: Mirrors were not common in American households, and only the rich could afford to have portraits painted. See id.

[154] See Warren & Brandeis, supra note Error! Bookmark not defined. ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life.").

[155] See SMITH, supra note Error! Bookmark not defined., at 138.

[156] See Warren & Brandeis, supra note Error! Bookmark not defined.. The concern here is with "private" eavesdropping, rather than with the official activity at issue in Olmstead.

[157] See, e.g., Poe v. Ullman, 367 U.S. 497, 549 (1961).

[158] Warren & Brandeis, supra note Error! Bookmark not defined.

the Warren-Brandeis right is relevant to the present discussion because it represents an early attempt to deal with the impact technology has upon "informational privacy," i.e., with an individual's ability to exercise some control over how the private sector gathers, disseminates and uses personal information.[159]

Warren and Brandeis were reacting, as noted earlier, to late nineteenth-century technology: improved printing and photograph reproduction; hand-held cameras; bugs and other eavesdropping devices. These and other technologies transformed personal information into a commodity; the press in prior eras had published information about "notables," but they were usually able to control the information that went to the press.[160] The proliferation of informational technologies and attendant demand for information that arose at the end of the nineteenth century changed all this; the socially- and politically-prominent were obvious targets,[161] but anyone could find that their control over their image or their personal information had been compromised.[162]

(notes omitted).

[159] See, e.g., Niall Waters, Personal Privacy and Popular Ubiquitous Technology, UbiConf 2004 (London), http://www.uclic.ucl.ac.uk/projects/ubiconf/materials/Papers/Niall%20Winters.pdf (last visited Aug. 15, 2005) (informational privacy is the ability of "`individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others'") (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967)); see also Alan F. Westin, Social and Political Dimensions of Privacy, 59 J. OF SOCIAL ISSUES 431, 431 (2003) (privacy as "as the claim of an individual to determine what information about himself or herself should be known to others . . . . This, also, involves . . . what uses will be made of it by others"). See generally Gormley, supra note Error! Bookmark not defined., at 1350.

[160] See, e.g., MICHAEL SCHUDSON, DISCOVERING THE NEWS: A SOCIAL HISTORY OF AMERICAN NEWSPAPERS 12-57 (1978). See generally FREDERICK HUDSON, JOURNALISM IN THE UNITED STATES FROM 1690-1872 (1873).

[161] See, e.g., id. at 1352 n.84 (press hounded President Grover Cleveland on his honeymoon).

[162] See SMITH, supra note Error! Bookmark not defined., at 125, 138-

Warren and Brandeis faced difficult conceptual difficulties in articulating their new right to informational privacy. One goes to the essence of the principle. The Fourth Amendment assumes a zero-sum conception of privacy in which only two states exist: private or not-private. When Crown officers burst into Entick's home and rummaged through his rooms and boxes, they annihilated the privacy of those spaces; what had been private was now not-private. The conduct with which Warren and Brandeis was concerned was very different; it typically involved capturing and exploiting information that was in the public domain, i.e., photographs and descriptions of the activities of the socially- or politically elite.[163] Since those activities occurred in public—either in public spaces or in homes to which members of the public had been invited—there was no compromise of information that was secluded, spatially or otherwise from observation. As Warren and Brandeis recognized, what they were concerned about was much more analogous to a property right than to a privacy right; the goal, after all, was to control the collection, dissemination and use of information about an individual.[164]

For various reasons, Warren and Brandeis ultimately chose to style the right for which they argued as a right to privacy, not a property right.[165] As we shall see in Section III, the same issues arise, albeit in different guises, from our experience with late twentieth-century and early twenty-first century technology.

---

39. Warren and Brandeis have been accused of being elitist, and they were primarily concerned about intrusions into the privacy of the "upper-crust," both because they belong to that society and because members of that society were primary targets for yellow journalists. See id. at 135-36.

[163] See id. at 121-22.

[164] See id. at 126; see also Warren & Brandeis, supra note Error! Bookmark not defined. ("[T]he legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.").

[165] See id. at 126; see also Warren & Brandeis, supra note Error! Bookmark not defined..

Section II reviews some pertinent technologies, and in Section III we consider whether this concern with controlling personal information that has been released into the public domain can be reconciled with Fourth Amendment principles. But first we need to review another strand of Supreme Court doctrine: decisions dealing with the Fourth Amendment's applicability to third-party records.

In the decade after *Katz,* the Supreme Court twice considered whether the Fourth Amendment applies to the government's accessing records generated by, and held by, a third-party, i.e., by someone whom the records concern but who had no role in their creation. In *United States v. Miller,*[166] Miller, who had been indicted on tax charges, moved to suppress records concerning his bank account; federal agents had obtained the records by using a grand jury subpoena, not a warrant.[167] Miller invoked *Boyd*,[168] claiming that the agents had "improperly circumvented" his Fourth Amendment rights.[169] The district court denied the motion; the Fifth Circuit reversed because it found that the government had violated *Boyd*.[170] The Supreme Court disagreed: "We find that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress."[171] This post-*Katz* Court cited a pre-*Katz* opinion for the proposition that

> "no interest legitimately protected by the Fourth

---

166 425 U.S. 435 (1976).

167 Miller, 425 U.S. at 437-39.

168 See supra notes 38-39 and accompanying text.

169 Id. at 438-39.

170 See United States v. Miller, 500 F.2d 751, 757 (5th Cir. 1974), reversed 425 U.S. 435 (1976) ("The venerable Boyd doctrine still retains its vitality; the government may not cavalierly circumvent Boyd's precious protection by first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies.").

171 Miller, 425 U.S. at 440.

> Amendment" is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into "the security a man relies upon when he places himself or his property within a constitutionally protected area."[172]

The *Miller* Court also noted that "the documents subpoenaed here are not respondent's `private papers.' Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks."[173]

Three years later, the Court decided *Smith v. Maryland*.[174] *Smith* was the "other half" of *Katz*—the issue was "whether the installation and use of a pen register," which captures the numbers dialed on a telephone, "constitutes a `search' within the meaning of the Fourth Amendment.[175] After she was robbed, Patricia McDonough began receiving "threatening and obscene phone calls from a man identifying himself as the robber."[176] Police suspicion focused on Michael Lee Smith as the robber, and the

> telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at [his] home. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from [his] home to McDonough's phone. On the basis of this and other evidence, the police obtained a warrant to search [Smith's] residence. The search revealed that a page in [his] phone book was turned down to the name and number of Patricia McDonough; the phone book was seized.[177]

---

172 Id. (quoting Hoffa v. United States, 385 U.S. 293, 301-02 (1966)).

173 Id.; see supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text.

174 442 U.S. 735 (1979).

175 Smith, 442 U.S. at 736.

176 Id. at 737.

177 Id. (citations omitted).

Arrested and indicted, Smith moved to suppress "`all fruits derived from the pen register'" on the grounds that its installation and use was a warrantless search in violation of the Fourth Amendment.[178] The trial court denied the motion and a divided Maryland Court of Appeals affirmed.[179]

The *Smith* Court began its opinion by reviewing *Katz* and noting that the standard used to implement *Katz* is the two-pronged test Justice Harlan enunciated in his concurring opinion: (i) whether the individual has exhibited a subjective expectation of privacy in the thing, place or endeavor; and (ii) whether society is prepared to regard the individual's subjective expectation of privacy, if any, as reasonable.[180] The Court found that Smith met neither criterion:

> Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner . . . cannot claim that his `property' was invaded or that police intruded into a `constitutionally protected area.' Petitioner's claim . . . is that, notwithstanding the absence of a trespass, the State . . . infringed a `legitimate expectation of privacy' . . . . [A] pen register differs . . . from the listening device employed in Katz, for pen registers do not acquire the contents of communications. . . .
>
> [P]etitioner's argument that its installation and use constituted a `search' necessarily rests upon a claim that he had a "`legitimate expectation of privacy' regarding the numbers he dialed on his phone.
>
> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must `convey' phone numbers to the telephone company, since it is through telephone company

178 Id.

179 Id.

180 Id. at 740; see supra Section I.A.3.

> switching equipment that their calls are completed. All subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[181]

The Court also (i) rejected Smith's claim that he demonstrated a subjective expectation of privacy by making the calls from his home,[182] and (ii) held that even if he could show such a subjective expectation, it is not one society would regard as reasonable: "[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not `one that society is prepared to recognize as "reasonable."' This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[183] The Court cited *Miller*

---

[181] Id. at 741-42 (citations omitted).

[182] See id. at 743:

> [T]he site of the call is immaterial . . . . Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company . . . if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Id.

[183] Id. at 743-44 (quoting Katz v. United States, 389 U.S. 347, 361

for the last statement.[184]

The Supreme Court has applied the *Miller-Smith* principle in a variety of cases.[185] It summarized the rationale for the principle in *United States v. Jacobsen*:

> [W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . .The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.[186]

This brings us back to the Warren-Brandeis issue: If, as the Supreme Court indicates, the Fourth Amendment conception of privacy is zero-sum (i.e., private or not-private), how can individuals have any control over the information they (knowingly, unknowingly, willingly, unwillingly) provide to others?

The assumption of risk principle articulated above assumes one has a choice: reveal information and lose privacy or do not reveal information and retain privacy. The Warren-Brandeis article was concerned with disclosures made that were made to other people by chance, i.e., by being in a particular place at a particular time. One could argue that the element of choice is missing, but there is another difficulty with assuming privacy in this context: The complained-of information (photography, description of what someone did) was gathered in an ostentatiously public place—a street, a restaurant, a hotel, etc. It is, after all, inevitable that certain of our actions will occur in

(1967) and citing Miller v. Unites States, 425 U.S. 435, 442-44 (1976)).

184 See id.

185 See, e.g., California v. Greenwood, 486 U.S. 35, 41 (1988); S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 735-36 (1984).

186 466 U.S. 109, 117 (1984).

public spaces; we cannot insist that our every action is private and must be ignored.

The early third-party records cases—*Smith* and *Miller*—go to a different issue. They both concern the privacy of information that was disclosed to a specific party for a specific purpose; the party making the disclosure chooses to reveal the information, but intends that it be a "controlled disclosure." This issue, which was of relatively minor import in the 1970's when *Smith* and *Miller* were decided, becomes extremely important in a world of ubiquitous technology for, as Section II explains, in such a world we interact, necessarily and almost continuously, with systems that gather information, utilize it and share it with other systems. The effect, as Section II explains, is essentially to eliminate private places; Section III considers how this could, and should, impact on the Fourth Amendment principles discussed above.

C. Evolution

Privacy is a distinctly modern product . . . .[187]

When we discuss Fourth Amendment privacy, we need to realize first, that it is so far a relatively narrow concept[188] and, second, that the conception of privacy itself is a very recent development.

> In earlier times, individuals were not seen as separate from their families, small communities, or society as a whole. Rather, they were a part of their tribe or social group, and they lived in an environment where people spent much of

[187] E.L. Godkin, The Rights of the Citizen IV—To His Own Reputation, 8 SCRIBNER'S MAG., July, 1890, at 58 available at http://cdl.library.cornell.edu/cgibin/moa/pageviewer?frames=1&cite=http%3A%2F%2Fcdl.library.cornell.edu%2Fcgi bin%2Fmoa%2Fmoa-cgi%3Fnotisid%3DAFR7379-0008-7&coll=moa&view=50&root=%2Fmoa%2Fscri%2Fscri0008%2F&tif=00072.TIF&pagenum=65.

[188] See supra §§ I(A)-(B).

> their time living closely together or under the watchful eye of others in their family or community. Also, they spent little time alone or thinking private thoughts that might question the communal practices and pressure for conformity in the community.[189]

New England colonies had laws prohibiting people from living alone and "forbade construction of homes beyond half a mile from the meeting house, the center of town. This was . . . the layout of the villages in England that the settlers had left."[190] People, even travelers, shared beds and many colonial homes had "no ceilings, so sounds could easily be heard from room to room and anybody willing to climb to the roof beams could peer into another room."[191] "[I]in the early 1800s as the population expanded and city life increasingly closed in on the rural and small village communities, there were increased glimmerings of dissatisfaction" and desires for more privacy.[192] These desires prompted the nineteenth-century Supreme Court decisions discussed in Section I.A. and the Warren-Brandeis effort to establish a "civil" right to privacy.[193] Our interest in, and desire for, privacy increased in the twentieth century, for a variety of reasons.[194] That interest seems to have reached new levels in

---

189 GINI GRAHAM SCOTT, MIND YOUR OWN BUSINESS: THE BATTLE FOR PERSONAL PRIVACY 24 (1995).

190 SMITH, supra note Error! Bookmark not defined., at 10, 17.

191 Id. at 19-20.

192 SCOTT, supra note 189, at 34.

193 See supra Section I.B.

194 See SCOTT, supra note 189, at 50:

> [F]rom the 1850s through the 1950s, a new concern with the right to privacy emerged, because in an increasingly complex, urbanized, multicultural society, there were more and more ways in which one's privacy might be invaded by others—from the government to the press and advertisers to other citizens. At the same time, there were fewer informal community ways to deal with these problems. . . .

Id. The expansion of surveillance technology during and after World War II created increased concerns about a loss of privacy.

the early years of the twenty-first century, given our need to accommodate privacy with the realities of the technology discussed in the next section.

The Twentieth-century world is vastly different from the Eighteenth-century realities that produced the Fourth Amendment. If we are to preserve its spirit—the desire to maintain an equitable balance between the personal lives of individuals and the needs of law enforcement—we cannot rely on the letter of the law as it existed when the Fourth Amendment was adopted. We must be flexible and forward-looking. We cannot rely solely on what has been, because what will be, has never been.

> By the 1950s, the technology that enabled government surveillance had grown by exponential leaps. Parabolic microphones, transmitters the size of cigarette packs, induction-coil devices and miniature television transmitters made it possible for government agents, police, private investigators and average citizen snoopers to watch, listen and record virtually any sound or movement. Accompanying this perfection in technology came the growing use of private detectives as surreptitious information-gatherers in business and family disputes . . . . Attempts by the states to . . . prohibit wiretapping were . . . ineffective. The state statutes tended to create broad exceptions for police conducting eavesdropping . . . . [T]he language of the statutes was rarely drafted to keep up with the swiftly-changing technology, rendering them quickly obsolete. By the time the United States entered the 1960s, most of the attempts to protect individual privacy by curbing electronic surveillance at the state level had failed.
>
> The 1960s soon witnessed a national uproar over the unchecked ability of government and private investigators to eavesdrop . . . . Influential scholars . . . produced volumes of literature detailing the threat of surveillance technology to individual privacy. Newspapers and periodicals . . . featured articles . . . decrying the runaway use of electronic surveillance . . . .

Gormley, supra note Error! Bookmark not defined., at 1363-64 (citations omitted). And in his State of the Union address in 1967, President Johnson declared, "We should protect what Justice Brandeis called the `right most valued by civilized men'—the right to privacy." Id. at 1364 (quoting Text of Message by President Johnson to Congress on State of the Union, N.Y. TIMES, Jan. 11, 1967, at A16).

II. TECHNOLOGY

"*Ubiquitous technology/computing will permeate all aspects of our physical world . . . .*"[195]

Olmstead and *Katz* were products of the same nineteenth-century technology: the telephone.[196] The Warren-Brandeis right to privacy was the product of other nineteenth-century technologies: improved printing, mobile photography and private surveillance techniques.[197] At the beginning of the twenty-first century, we occupy an environment that has been changed dramatically by twentieth century technologies; telephone booths like the one Charles Katz used are an endangered species,[198] as is the one-to-one mode of communication he utilized. Our communications are multi-modal; we communicate synchronously or asynchronously by voice, text or data, and combine modes.[199] As everything about our lives becomes more portable, more exposed to scrutiny, we will have to decide how to reconcile the inherent tension between privacy and the need for effective law enforcement.

---

[195] UbiCorp: A Vision of the Ubiquitous Corporation, Accenture, at http://www.accenture.com/xd/xd.asp?it=enweb&xd=services%5Ctechnology%5Ctech_ubicorp.xml (last visited Aug. 15, 2005).

[196] See supra Section I.A.3.

[197] See supra Section I.B.

[198] See, e.g., Archive of Addresses by Andy Rooney, Andy Rooney's Phone Dilemma (Jan. 9, 2005), http://www.cbsnews.com/stories/2005/01/07/60minutes/rooney/main665523.shtml ("The public telephone booths that used to be on every big city street corner are rapidly disappearing."). See also Oliver Lucazeau, Last Call for Britain's Little Red Telephone Booths, THE GLOBE & MAIL (Toronto) June 21, 2004, at A11 (explaining the gradual disappearance of red telephone booths in Britain).

[199] See, e.g., Highlight of the Month: The Ultimate VAS Environment, COMVERSE ANALYST NEWSLETTER (Comverse, New York, N.Y.), December 2002, http://www.comverse.com/news/newssub/NEWSLETTER7.htm#What's%20New:

> "Total communication" creates a borderless environment where people are

A relatively recent Ninth Circuit case illustrates how far we have come from *Katz*; *In re the Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications*[200] arose from the Federal Bureau of Investigation's (FBI) efforts to wiretap a vehicle. More precisely, it resulted from the FBI's efforts to use technology already integrated into a private vehicle to intercept conversations taking place within it.[201] As the Ninth Circuit explained, some vehicles are equipped with "telecommunication devices" that assist with navigation or with "emergencies or obtaining road-side assistance. Such systems operate via a combination of GPS . . . and cellular technology."[202] The appellant in the case (the Company) operated one such service (the System).[203] One feature of the System [let] the Company open a cellular connection to a vehicle and listen to [conversations in] the car."[204] The purpose was to help recover stolen vehicles, but it could also be used to eavesdrop on legitimate conversations carried on in a vehicle

> free to communicate in the way that is most appropriate . . . for them. It encompasses the full range of real-time and non-real-time multimedia communications and messaging services. As a result, talking, voice messaging, emailing, text messaging, chatting and conferencing become equally accessible options.

Id.; see also Posting of Angus Davis to Om Malik's Blog-About the Next Generation Internet, http://gigaom.com/2004/11/29/building-the-phone-platform/ (Nov. 29, 2004) ("IP-powered telecommunications will . . . chang[e] the way people . . . use the telephone. . . .[T]he two-party voice calling will shift towards multimodal and multi-party communication[s]. . . .").

200 349 F.3d 1132 (9th Cir. 2003).

201 Id. at 1134. Law enforcement installation of listening devices in vehicles is far from novel. See, e.g., Massiah v. United States, 377 U.S. 201, 202-03 (1964) (in 1959, federal agents "install[ed] a Schmidt radio transmitter under the front seat of [a car]" and used it to listen in on conversations held by the occupants of the vehicle).

202 In re The Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d at 1133.

203 Id.

204 Id.

equipped with the System.[205]

Realizing this, the FBI obtained "orders requiring the Company to assist in intercepting conversations taking place in a car equipped with the System."[206] The Company complied with the first order but challenged the next, claiming that the district court did not have authority to order the use of its "equipment, facilities, system, and employees."[207] The district court rejected the challenge and the Company appealed.[208]

The orders were issued under the federal wiretap statutes: Title III.[209] Congress responded to the *Katz* decision by adopting Title III of the Omnibus Crime Control and Safe Streets Act of 1968;[210] Title III was intended "to implement a uniform procedure for conducting constitutionally acceptable electronic surveillance."[211] Since it is founded upon the Fourth Amendment, Title III makes it illegal to intercept communications except pursuant to a court order.[212] In issuing a Title III order, a court can require "a provider . . . of wire or electronic communication service, landlord, custodian or other person" to provide "technical assistance necessary to accomplish the interception . . . with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person

---

205 Id. at 1133-34.

206 Id. at 1134.

207 Id. at 1134-35.

208 Id. at 1135.

209 Id. at 1136-38.

210 See Title III, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (1998); see also supra Section I.A.3. Congress was specifically responding to Berger v. New York, 388 U.S. 41 (1967). In Berger, a companion to Katz, the Court held that because of the potential for intrusiveness, wiretapping authorizations must be carefully crafted to satisfy the probable cause and particularity requirements of the Fourth Amendment. Id. at 55-64.

211 Jie Xiu, Note, The Roles Of The Judiciary In Examining And Supervising The Changing Laws Of Electronic Surveillance, 28 SETON HALL LEGIS. J. 229, 233 (2003).

212 Id.

whose communications are to be intercepted."[213]

The Company claimed it was not a "provider of communication service" under Title III.[214] The Ninth Circuit found it was subject to Title III either as a provider of communications services or as an "other person" who could be required to assist law enforcement in intercepting communications.[215] The Ninth Circuit reversed the district court, however, because it concluded that the surveillance could not be carried out "with a minimum of interference with the services" the Company provided the owner of the vehicle.[216] The court found that "eavesdropping is not performed with `a minimum of interference' if a service is *completely* shut down as a result of the surveillance."[217] Since officers using the System to eavesdrop shut down its emergency and other functions, the Ninth Circuit held that the district court erred in ordering the Company to cooperate with the FBI.[218]

---

213 18 U.S.C. § 2518(4) (2000).

214 In re The Application of the U.S., 349 F.3d at 1139.

215 Id.

216 Id. at 1144-46; see also 18 U.S.C. § 2518(4).

217 Id. at 1145 (quoting 18 U.S.C. § 2518(4)).

218 Id. at 1146. A California legislator responded to this decision by introducing Senate Bill 1330, which would prohibit "eavesdropping involving an embedded automotive telematic device." See Committee Report for 2003 California Senate Bill No. 1330, 2003-04 Regular Session (July 12, 2004) [hereinafter Committee Report]; see also California Senate Bill 1330, as amended June 30, 2004. After the Department of Justice expressed concern that the original bill would preclude "law enforcement agencies from applying for an order authorizing interception of electronic cellular telephone communications that occurred by means of a technology such as" the System, the bill was revised so it does not "reduce the ability of law enforcement agencies to apply for a wiretap order." Committee Report, supra ("[B]y enacting a series of prohibitions in the invasion of privacy laws . . . without concurrently creating some explicit, though limited, authority in the wiretapping provisions, this bill reduced the scope of the existing wiretap authority."). According to a committee report, it reaffirms

> California's wiretapping law—bugging by law enforcement is prohibited . . . . [R]ecognizing that emerging forms of technology may combine electronic

This case highlights issues we will face as technology becomes an increasingly pervasive feature of our lives.[219] We have for many decades assumed that a vehicle is a "private" place; fictional characters often take advantage of the privacy a vehicle offers to discuss sensitive matters.[220] The privacy of vehicles has, of course, been compromised on occasion;[221] but while we might be aware, at some level, that cars *could* be "bugged," we could not imagine that our vehicles would themselves *become* instruments of surveillance.

If cars can become instruments of surveillance, what about our homes? The case discussed above illustrates a trend—the perva-

> communications capabilities, this bill provides that a cellular telephone, or a similar device, may not be used to overhear confidential communications between persons who are not using some form of communication technology.

Id. On July 2, 2004, S.B. 1330 was withdrawn from the Assembly Committee on Appropriations and set for a second reading. On August 9, 2004, it was amended in Assembly. See S.B. 1330, http://info.sen.ca.gov/pub/bill/sen/sb_1301-1350/sb_1330_bill_20040809_amended_asm.html. On August 17, a first hearing was set for the bill, but it was canceled at the request of the bill's author. See California State Senate, Complete Bill History: S.B. 1330, http://info.sen.ca.gov/pub/bill/sen/sb_1301-1350/sb_1330_bill_20040817_history.html. If it passes, the bill would prohibit intercepting conversations between the occupants of a vehicle. See Committee Report for 2003 California Senate Bill No. 1330, supra: "California law authorizes the interception of wire, electronic pager, or electronic cellular telephone communications. Unlike federal law, the statutory scheme set forth in Penal Code Section 629.50 et seq. does not authorize intercepting oral communications, commonly referred to as `bugging.'"

[219] See generally, Centre for Pervasive Computing, http://www.pervasive.dk/ (last visited Aug. 16, 2005).

[220] The Ninth Circuit case discussed above focused exclusively on the specific statutory structure Title III created for the authorization and implementation of wiretaps, so the question of whether the interior of the vehicle was a "private" place was not raised, though it was presumably assumed. See generally, In re The Application of the U.S., 349 F.3d 1132 (9th Cir. 2003) (showing how the court focused on the statutory structure of Title III).

[221] See supra note Error! Bookmark not defined. and accompanying text.

siveness of technology[222]—that will find its way into our homes. As computer technology becomes an embedded feature of every aspect of our lives, our homes, too, will come equipped with technology that can be used to eavesdrop on our conversations and track our activities.[223] Like the System, this technology will

[222] See, e.g., SeachNetworking.Com Definitions, http://searchnetworking. techtarget.com/sDefinition/0,,sid7_gci759337,00.html (last visited Aug. 16, 2005):

> Pervasive computing is the trend towards increasingly ubiquitous . . . connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic-and particularly, wireless-technologies and the Internet. Pervasive computing devices are not personal computers as we tend to think of them, but very tiny-even invisible-devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods-all communicating through increasingly interconnected networks. According to Dan Russell, director of the User Sciences and Experience Group at IBM's Almaden Research Center, by 2010 computing will have become so naturalized within the environment that people will not even realize that they are using computers. Russell and other researchers expect that in the future smart devices all around us will maintain current information about their locations, the contexts in which they are being used, and relevant data about the users.

Id.

[223] See supra note Error! Bookmark not defined.; see also Marc Langheinrich, et al., Living in a Smart Environment: Implications for the Coming Ubiquitous Information Society, 15 TELECOMM. REV. 1 (2005), at http://www.vs.inf.ethz.ch/publ/papers/ sktelecom2005.pdf (last visited Aug. 16, 2005):

> By virtue of its very definitions, the vision of ubiquitous computing has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life: "The old sayings that `the walls have ear' and if these walls could talk' have become the disturbing reality. The world is filled with all-knowing, all-reporting things' . . . . Today's economic reality—shopping without participating in comprehensive profiling . . . might become an expensive luxury for well-off citizens . . . .

Id. (quoting R. Lucky, Everything Will Be Connected To Everything Else, Connections, IEEE SPECTRUM (March 1999), at http://www.argreenhouse.com/papers/rlucky/ spectrum/connect.shtml (last visited Aug. 16, 2005)).

be included because it has other uses.[224] Efforts are underway to develop "aware homes" that incorporate intelligent, embedded systems which interact with the occupants and with outside systems.[225] An "aware home" will "be able to recognize

[224] See, e.g., Mahesh S. Raisinghani, et al., Ambient Intelligence: Changing Forms of Human-Computer Interaction and their Social Implications, 5 J. DIGITAL INFO., Issue 4, Art. 271 (Aug. 24, 2004), available at http://jodi.ecs.soton.ac.uk/ Articles/v05/i04/Raisinghani/ (last visited Aug. 16, 2005):

> A young mother is on her way home, driving . . . with her 8-month old daughter who is sleeping in her child seat on the passenger side of the car. The infant is protected by an intelligent system called SBE 2 against airbag deployment, which could be fatal in the case of an accident. SBE 2 detects when there is a child seat on the passenger seat instead of a person and automatically disables the airbag . . . . Arriving home, a surveillance camera recognizes the young mother, automatically disables the alarm, unlocks the front door as she approaches it and turns on the lights to a level of brightness that the home control system has learned she likes. After dropping off her daughter, the young mother gets ready for grocery shopping. The intelligent refrigerator has studied the family's food consumption over time and knows their preferences as well as what has been consumed since the last time she went shopping. This information has been recorded by an internal tracking system and wireless communication with the intelligent kitchen cabinets. Based on this information, the refrigerator automatically composes a shopping list, retrieves quotations for the items on the list from five different supermarkets in the neighborhood through an Internet link, sends an order to the one with the lowest offer and directs the young mother there. When arriving at the supermarket, the shopping cart has already been filled with the items on her shopping list. Spontaneously, she decides to add three more items to her cart and walks to the check-out. Instead of putting the goods on a belt, the entire cart gets checked out simply by running it past an RFID transponder that detects all items in the cart at once and sends that information to the cash register for processing.

Id.

[225] See, e.g., Georgia Institute of Technology, The Aware Home, at http://www.cc.gatech.edu/fce/ahri/ (last visited Aug. 24, 2005); Philips Research, Ambient Intelligence: A New User Experience, at http://www.research.philips.com/ technologies/syst_softw/ami/vision.html; see also Mark Ward, Smart Homes Offer A Helping Hand, BBC NEWS, May 19, 2004, at

the people that live in it, adapt . . . to them [and] learn from their behavior".[226] Similar systems will become features of offices, hotel rooms and other environments.[227]

Pervasive technology raises difficult issues about privacy.[228]

---

http://news.bbc.co.uk/2/hi/technology/ 3715927.stm (last visited Aug. 16, 2005).

[226] Philips Research, supra note 225; see also supra note Error! Bookmark not defined..

[227] See, e.g., European Commission, ISTAG: Scenarios for Ambient Intelligence in 2010, 4-7, 2001, at http://www.research.philips.com/technologies/misc/homelab/downloads/evr.19763en.pdf.

[228] See, e.g., Marc Langheinrich, Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems, Proceedings of UbiComp 2001 273 (2001), http://www.vs.inf. ethz.ch/publ/papers/privacy-principles.pdf (last visited Aug. 24, 2005):

> What is it that makes ubiquitous computing any different from other computer science domains with respect to privacy? . . . Four properties come to mind:
>
> • UBIQUITY: Ubiquitous computing is everywhere—this is its essence, its explicit goal. Consequently, decisions made in ubiquitous system and artifact design will affect large, if not every part of our lives, from crossing a street to sitting in the living room to entering an office building.
>
> • INVISIBILITY: Not only should computers be everywhere, we want them to actually disappear from our views. With the ever shrinking form factor of computing and communication devices, this goal seems far from being science fiction. Naturally, we will going to have a hard time in the future deciding at what times we are interacting with (or are under surveillance by) a computing or communication device.
>
> • SENSING: As computing technology shrinks and processing power increases, so does the abilities of sensors to accurately perceive certain aspects of the environment. Simple temperature, light, or noise sensors have been around for quite some time, but next generation sensors will allow high quality audio and video feeds from cameras and microphones smaller than buttons. Even emotional aspects of our lives, such as stress, fear, or excitement, could then be sensed with high accuracy by sensors embedded in our clothings [sic] or in our environment.
>
> • MEMORY AMPLIFICATION: Advancements in speech and video processing, combined with the enhanced sensory equipment available soon, make it

Our Fourth Amendment conception of privacy is spatially-driven in the sense that it equates privacy with exclusion.[229] The Supreme Court held that Charles Katz had a Fourth Amendment expectation of privacy in his calls because by retreating to a telephone booth, he sought to prevent others from hearing what he said.[230] *Katz* has created an "assumption of risk" standard:[231] My communications and activities are private only insofar as I shield them from observation by others. We consequently tend to associate "privacy" with enclaves such as our homes, our cars, our offices.[232]

The pervasiveness of technology erodes those enclaves. Cell phones have basically eliminated phone booths; vehicles are equipped with surveillance technology; and with wireless networks and cellular communications, much of what goes on in our homes leaks into the public domain. Offices may be somewhat more secure, but much of our work takes place outside our offices. "Road warriors" equipped with the latest in wireless communication conduct business from—and on their way to and from—other offices, other places. The notion of private enclaves

---

> actually feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and movement of ourselves and our surroundings, feeding them into a sophisticated back-end system that uses video and speech processing to allow us browsing and searching through our past.

Id.

229 See supra Section I.A.3.

230 See supra Section I.A.3.

231 See, e.g., Gavin Skok, Establishing a Legitimate Expectation of Privacy in Clickstream Data, 6 MICH. TELECOMM. & TECH. L. REV. 61, 71-73 (2000).

232 In the Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications case, the FBI proceeded under Title III. Since Title III applies only when one has a reasonable expectation of privacy in the communications at issue, the FBI either (i) operated on the assumption that the interior of the vehicle was a "private" enclave requiring a warrant to access or (iii) proceeded under Title III because the agents needed the cooperation of the Company to exploit the System for eavesdropping purposes. See supra notes 200-18 and accompanying text.

as places separate and apart from the world, areas in which our activities and communications are not subject to observation, is disappearing.

III. TWENTY-FIRST CENTURY PRIVACY?

"*You have no privacy. Get over it.*"[233]

In effect, we must decide if the Katz Court meant what it said when it held that the Fourth Amendment "protects people, not places."[234] Notwithstanding that holding, the Court has continued to approach Fourth Amendment privacy as if it is nothing more than a spatial concept; what I seclude from others is private, what I fail to shield is not.[235] The question is whether this is inevitable: Can we construe Fourth Amendment privacy in a fashion that is expansive enough to encompass life in a society where physical barriers have little, if any, meaning?[236] If we cannot, we will have little, if any, privacy.

---

[233] On the Record: Scott McNealy, SAN FRANCISCO CHRONICLE, Sept. 14, 2003, at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/09/14/BU141353.DTL&type=business (last visited Aug. 18, 2005) (comment from Chairman, President and CEO of Sun Microsystems, Inc.: "The point I was making was someone already has your medical records. Someone has my dental records. Someone has my financial records. Someone knows just about everything about me.").

[234] See Katz, supra note 124 and accompanying text.

[235] Historically, the only way to shield my activities and personal information from prying eyes was to physically seclude it from observation, e.g., in locked rooms, sealed chests, etc. See supra note Error! Bookmark not defined. and accompanying text. This is apparent in Katz; the Supreme Court found that Charles Katz had a reasonable expectation of privacy in his phone calls because he secreted himself in a sealed telephone booth, thereby preventing the unaided ear from hearing what was said. See supra Section I.A.3. The physical seclusion of communicated information was also the basis for the Court's decision in Jackson; the Supreme Court found a Fourth Amendment expectation of privacy in letters that had been sealed to frustrate casual access to their contents. See supra Section I.A.1. As we move into a digital world, we necessarily develop different ways to frus-

A. Dynamics

"*. . . replacing . . . Big Brother . . . with a lot of Little Brothers.*"[237]

To understand why that is true, we must consider how ubiquitous technology will alter the basic law enforcement dynamic. Jackson, Boyd, Olmstead, Katz and most of the Supreme Court's other Fourth Amendment decisions involved law enforcement's locating the presumptive situs of physical evidence[238] and then taking affirmative steps to find and seize that evidence, a scenario older than general warrants.[239] The scenario has two notable characteristics. First, officers seek evidence of a specific crime which they believe was committed by a specific person; this focus circumscribes the scope of their efforts.[240] Second, officers seek out and collect this evidence from places associated with the suspect.[241] Fourth Amendment analysis has consequently focused on the interaction between the officers and the suspect; the concern has been with controlling the process by which officers intrude into that person's "private" spaces.[242] The procedures we have devised to prevent "unwarranted" intrusions into personal, private spaces—a search warrant supported by probable cause or an exception—all reflect this.[243] Evidence-gathering that does not intrude into such space is outside the Fourth Amendment, at least as far as the object of the search is concerned.[244]

---

trate access to data; encryption is an obvious example. Encryption frustrates access by "obscuring information to make it unreadable without special knowledge." Encryption, Wikipedia, http:// en.wikipedia.org/wiki/Encryption. It is not a physical barrier but it has the same effect, and the same logic: to block undesired access.

[236] See supra Section II.

[237] What Is the Matrix? ACLU Seeks Answers on New State-Run Surveillance Program, American Civil Liberties Union, October 30, 2003, at http://www.aclu.org/ Privacy/Privacy.cfm?ID=14257&c=130 (quoting Barry Steinhardt) (last visited Aug. 18, 2005).

[238] The evidence consists of items of tangible or intangible personal

property. See supra Section II.A. This includes bodily substances. See, e.g., Schmerber v. California, 384 U.S. 757 (1966).

239 See supra notes 20-21 and accompanying text.

240 See, e.g., WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT Vol. 1, § 1.1(a) (4th ed. 2005).

241 See supra Section I.A. Law enforcement may also seek evidence from those associated with suspects, as well as from suspects; indeed, officers may seek evidence from "civilians," i.e., those who have no involvement in the suspected criminal activity. That does not alter the structure of the dynamic outlined above. In all of these scenarios—law enforcement searches the suspect's premises, the premises belonging to suspect's associate and the "civilian" premises—the inquiry is whether law enforcement violated the privacy of the person or persons whose premises were the object of a search. The focus is on law enforcement officers' actively targeting someone's premises (Boyd) or activity (Katz) for scrutiny. See supra Section II.A. If the officers violate someone's privacy, they can move to suppress the evidence, if any, resulting from the violation or bring a civil rights suit seeking damages for the violation. See, e.g., FED. R. CRIM. P. 41(h); Groh v. Ramirez, 540 U.S. 551, 554-56 (2004).

242 See supra Section I.A.

243 See, e.g., FED. R. CRIM. P. 41(c)-(e); LAFAVE, supra note 240, § 2.2(a). This assumption is also embedded in Title III, the legislative product of Katz. See supra notes 209-12 and accompanying text. Title III's wiretap provisions specify that the transmission of the contents of communications is not to be interrupted by "interception;" this is simply an application of the Jackson principle. See 18 U.S.C. §§ 2510-22; see also supra Section I.A. Instead of using an adhesive envelope, one relies upon communication systems that, it has heretofore been reasonable to assume, are "closed" to the general public. See, e.g., COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § IV(A) (2002), at http://www.cybercrime.gov/s&smanual2002.htm#_IVA_ (last visited Aug. 19, 2005):

> Since its enactment in 1968 . . . Title III has provided the statutory framework that governs real-time electronic surveillance of the contents of communications. When agents want to wiretap a suspect's phone, "keystroke" a hacker breaking into a computer system, or accept the fruits of wiretapping by a private citizen who has discovered evidence of a crime, the agents first must consider the implications of Title III.
>
> The structure of Title III is surprisingly simple. The statute's drafters assumed that every private communication could be modeled as a two-way

Now, consider how this dynamic changes in a world of ubiquitous technology. Ambient technology creates an "invisible and comprehensive surveillance network," the constituent parts of which are operated by private entities. As Section II explained, this network effectively eradicates the distinction between "public" and "private" spaces.[245] Information that has historically been secluded behind physical barriers leaks out into the public domain.[246] The data gathered by such a network, along with the data I generate through my online activities, provides a tremendous opportunity for law enforcement.[247] In-

> connection between two participating parties, such as a telephone call between A and B. At a fundamental level, the statute prohibits a third party (such as the government) who is not a participating party to the communication from intercepting private communications between the parties using an "electronic, mechanical, or other device," unless one of several statutory exceptions applies.

Id.; see 18 U.S.C. § 2511(34)(b). See, e.g., Telephone tapping, Wikipedia, http://en.wikipedia.org/wiki/Wiretap (last visited Aug. 19, 2005).

[244] See supra Section II.

[245] See supra note Error! Bookmark not defined.; see also ROBERT D. O'HARROW, JR., NO PLACE TO HIDE 291 (2005):

> Before long, our phones, laptop computers, PalmPilots, watches pagers, and much more will play parts in the most efficient surveillance network ever made. Forget dropping a coin into a parking meter or using a pay phone discreetly on the street. Those days are slipping by. The most simple, anonymous transactions are now becoming datapoints on the vast and growing matrix of each of our lives.

Id.

[246] See supra Section II.

[247] The data gathered by these sources can be divided into three broad categories:

(i) Tool Data

Tool data encompasses personal information that is valued not for its content but for its utility. It includes Social Security numbers, dates of birth, driver's license numbers and other data; it will no doubt come to include biometric identifiers such as DNA. Tool data is a given; it is not the product of my will or effort but is assigned, more or less arbitrarily, to me. Tool data has "value" because it is an implement that can be used for good or evil. My Social Security number, for example, is a tool I can

use to identify myself for various benign purposes (positive value) and one a criminal can use to steal my identity (negative value). See, e.g., Bowen v. Roy, 476 U.S. 693, 710-11 (1986).

Though tool data is something I "receive," it is not inherently "public." My Social Security number and date of birth may be "public," in that I have shared them with others, but that is not inevitable, like the other types of tool data in current circulation, they are "public" because we have not conceptualized tool data as a commodity that has "value" and must therefore be protected. The need for, and use of, tool data is a historical accident, an ad hoc solution to the complexity of modern society; we use tool data to identify ("I am Susan Brenner") and authenticate ("Here is proof I am Susan Brenner"). See, e.g., BRUCE SCHNEIER, BEYOND FEAR 182-95 (2003). For most of human history, these functions were relational; people were born, raised and lived their lives in the same community, where everyone knew and recognized them. SCHNEIER, at 184. As populations became increasingly mobile and urbanized, relational identification and authentication no longer sufficed; it became necessary to find some surrogate, and that is what Social Security numbers, driver's licenses and other personal data became. See, e.g., Matt Sundeen, License to Drive = Proof of Identity, STATE LEGISLATURES, April, 2003.

(ii) Biographical Data

Biographical data derives from my activities in real- and cyber-space; it includes where I live and where I have lived, where I work and where I have worked, the car I drive, the routines I follow and the places and people I visit. Biographical data is considered "public" because it is the product of my behavior in public places, where what I do can be observed by anyone who shares that space with me. See Remsburg v. Docusearch, Inc. 816 A.2d 1001 (N.H. 2003). Consequently, biographical data, defined as information which was or could have been obtained by observing activity in a "public" place, is not private under Katz or under cognate tests used to implement civil privacy protections. See United States v. Knotts, 460 U.S. 276, 282-85 (1983); Remsburg, 816 A.2d at 1009. As Section II explained, the implementation of ubiquitous technology makes the assumptions underlying this category increasingly problematic because it is based on a purely spatial bifurcation of "public" and "private."

(iii) Transactional Data

Transactional data is generated by our interactions with others. In analyzing the privacy of transactional data, it is useful to divide it into two types: (a) professional transactional data, which results from interactions with attorneys, physicians, religious advisors, psychiatrists, accountants and other professionals; and (b) commercial transactional data, which results from interactions with those who provide commercial goods or services offline or online. There are certain constants across

these categories: Each generates data which establishes (i) that I interacted with a particular professional or commercial resource on one or more occasions, (ii) the nature of that interaction (seeking legal advice, making a purchase) and (iii) the details of that interaction (seeking legal advice about an estate; purchasing vitamins, electronics or clothing). None of this data is private under the Katz test or cognate civil standards because by interacting with external entities (human or automated) I have knowingly exposed (i)-(iii) to public view; I assumed the risk that those with whom I interact will reveal the details of that interaction to others.

There can be some overlap between transactional data and biographical data. To understand why, it is useful to consider two real world transactions. In the first, I consult with an attorney whose office is in my neighborhood; in the second, I purchase a prescription from a pharmacist at my local drug store. My traveling to the law office and to the drug store takes place in public, and so can be considered biographical data. It is also transactional data insofar as it shows that I interacted with the lawyer and with the pharmacist. These respective encounters differ somewhat in the extent to which the nature and details of the interactions are biographical. My purchasing a prescription from the pharmacist takes place in "public," and so the nature of the transaction tends toward the biographical; but the details of the purchase will remain confidential unless I choose to share them or unless the pharmacist is indiscreet enough to announce the nature and uses of the medication I buy. Since it is reasonable to infer that I went to a law office to obtain legal advice, the nature of that transaction also tends towards the biographical; but since the transaction itself does not take place in public, the details do not constitute biographical data.

The law has treated the categories differently: Professional interactions are usually encompassed by privileges that bar the professional from revealing details of the interaction without the client's permission; the purpose is to provide confidentiality when it is "essential to the full and satisfactory maintenance of the relationship between the parties." PAUL F. ROTHSTEIN & SUSAN W. CRUMP, FEDERAL TESTIMONIAL PRIVILEGES § 1.1 (2004). For commercial interactions, the general rule is that "the facts of a transaction belong jointly and severally to the participants. If Alice buys a chattel from Bob, ordinarily both Alice and Bob are free to disclose this fact." A. Michael Froomkin, The Death of Privacy?, 52 STAN. L. REV. 1461, 1521-22 (2000) (noting that a "very small number of statutes impose limits upon the sharing of private transactional data collected by persons not classed as professionals"). Neither type of transactional data is private in the constitutional-common law sense, but the evidentiary and other constraints American law places on the dissemination of data resulting from professional interactions limit its circulation to those involved in the professional consultation; therefore, while professional transactional data is not

stead of having to search variously for discrete bits of information from a disjointed array of physical sources, officers can harvest information that is held by these private entities.[248]

private, it is secured.

[248] See, e.g., Michael D. Birnhack & Niva Elkin-Koren, The Invisible Handshake: The Reemergence of the State in the Digital Environment, 8 VA. J.L. & TECH. *2-3 (2003) (LEXIS):

> The Internet was initiated by the State, and soon after was privatized . . . . Market powers . . . facilitated the rise of new players . . . who gained power and control in the information environment . . . . A convergence of interests seems to be developing among players such as copyright owners and service providers on the one hand, and the State's growing interest in the digital environment, on the other hand. Law enforcement agencies seek to enhance their monitoring capacity and online businesses seek to prevent fraud and combat piracy while strengthening their ties with authorities. This convergence might lead to an unholy alliance with potentially troublesome results . . . .
>
> The most explicit example . . . is reflected in a presentation by Joseph E. Sullivan, director of compliance and law enforcement relations at eBay. Addressing law enforcement agents at a conference on cybercrime, Sullivan offered to hand over information, when requested . . . . eBay is one of the largest online e-commerce businesses, and the owner of PayPal, which provides clearing services for online financial transactions. eBay controls access to a colossal amount of information, including financial records, names, user IDs and passwords, affiliations, e-mail addresses, physical addresses, shipping information, contact information, and transaction information (i.e., bidding history, prices paid, feedback rating). But eBay is not alone in implementing law enforcement-friendly policy. The emerging regime of recent years facilitates cooperation between the State and the private sector in law enforcement efforts, beyond the reach of judicial review.

Id. (note omitted); see also O'HARROW, supra note 245, at 300:

> Law enforcement and intelligence services don't need to design their own surveillance systems . . . . They only have to reach out to the companies that already track us so well while promising better service, security, efficiency, and, perhaps most of all, convenience. It takes less and less effort each year to know what each of us is about. When we were at the coffee shop and where we went in our cars. What we wrote online, who we spoke to on the phone, the names of our friends and their friends and all the people they know. When we road the subway, the candidates we supported, the books

Under current Fourth Amendment principles, I have no expectation of privacy in information I have shared with these entities or information they have gathered about me.[249] The essential dynamic is missing. The officers are not directing their efforts *at* me and my private spaces; they instead direct their efforts at others in order to obtain information *about* me. The focus shifts from official intrusions into spaces under my temporary or permanent control to the acquisition of evidence from sources over which I exercise no control. I become irrelevant except as the object of the data acquisition.

The harvesting scenario will not supplant the traditional dynamic. We are physical beings and, as such, will continue to act, and to generate physical evidence, in the real world. The primary locus of evidence for traditional crimes such as rape, murder and drug trafficking will no doubt remain in the real world.[250] The "harvesting" scenario instead represents a new,

> we read, the drugs we took, what we had for dinner, how we like our sex. More than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe . . . .

Id.

[249] See supra Section I.B.; see also supra note Error! Bookmark not defined.. There are a number of federal statutes—such as the Health Insurance Portability and Accountability Act (HIPAA), the Right to Financial Privacy Act, the Gramm-Leech-Bliley Act and the Electronic Communications Privacy Act (ECPA)—which impose restrictions on the dissemination of various types of personal data. See, e.g., 45 C.F.R. § 164.512(e) (HIPAA); 12 U.S.C. § 3405) (Right to Financial Privacy Act); 15 U.S.C. § 6802(e)(8) (Gramm-Leech-Bliley); 18 U.S. Code § 2703 (ECPA). These and similar statutory provisions are not relevant to this discussion (a) because the restrictions they impose are usually less than those required by the Fourth Amendment and (b) they are far more fragile than the Fourth Amendment. See, e.g., Peter P. Swire, Katz Is Dead, Long Live Katz, 102 MICH. L. REV. 904, 916 (2004). What Congress gives, Congress can take away. Public awareness is another issue: The average American is unlikely to be aware of the provisions of these statutes (except, perhaps, to the extent that some require one to fill out paperwork), but does have at least a pragmatic grasp of Fourth Amendment guarantees.

[250] Even crimes such as this generate evidentiary data. See, e.g., Eric

added dynamic, a twenty-first century variation of the "assault on the castle" that ultimately resulted in the adoption of the Fourth Amendment.[251] There are commonalities between the two. A concern for the sanctity of personal information runs from *Entick* through *Jackson* and *Boyd,* and is implicit in *Katz* and *Berger*.[252] These cases, however, all involved the traditional Fourth Amendment dynamic: a direct assault upon personal information in the hands of the person to whom it pertains. The issue we must resolve is whether the Fourth Amendment can, and should, be construed as encompassing indirect assaults as well.

We begin with whether it *should* be construed in this fashion.[253] The impetus, if any, for such a construction must lie in

---

Weslander, Web Evidence Used in Murder Hearing, Lawrence (Kansas) Journal-World, December 10, 2004, at http://www.ljworld.com/section/crime_fire/story/ 189998:

> The case of a Kansas State University professor charged with murdering his ex-wife headed into uncharted legal territory Thursday as prosecutors presented evidence of an Internet search history from the suspect's computers.
>
> . . . .
>
> A Lawrence Police detective who examined computers seized from Thomas E. Murray testified that in the month before Carmin D. Ross' killing, Murray's computers had been used to search the Internet for phrases that included `how to hire an assassin,' `how to kill someone quickly and quietly' and `how to murder someone and not get caught.'
>
> . . . . [The detective] testified that even though Murray appeared to use his computer regularly on Thursday mornings, there was virtually no file activity on Murray's computers the morning of Nov. 13, 2003, the day prosecutors allege he drove to Lawrence and stabbed and beat Ross to death.

Id.

[251] Wilson v. Layne, 526 U.S. 603, 609-10 (1999); see supra Section I.A.

[252] See supra note Error! Bookmark not defined.; Section I.A. See, e.g., Berger v. New York, 388 U.S. 41, 49 (1967) (citing Entick and noting that the "law, though jealous of individual privacy, has not kept pace with . . . advances in scientific knowledge" such as wiretapping).

[253] The issue as to whether we can construe the Fourth Amendment in

the current interpretation's inability to protect us from new and "unwarranted" governmental intrusions. And that brings us back to the new dynamic. The "harvesting" dynamic has troubling implications for our ability to balance the often-conflicting demands of privacy and of effective law enforcement. This is because it supports two types of law enforcement evidence-gathering, both of which are outside the strictures of the Fourth Amendment.[254] The first scenario is the one discussed above, in which officers collect information about me, specifically, from private entities.[255] While it is outside the Fourth Amendment, this scenario is conceptually more analogous to the traditional Fourth Amendment dynamic in that its focus is narrower; the concern is with gathering evidence about a specific person who is suspected of specific criminal activity.[256] The second scenario is based on the same principle as the first, but is broader in scope. Since none of us have a Fourth Amendment expectation of privacy in data held by private entities,[257] it follows that law enforcement should be able to utilize the resources of these entities to harvest information generally, for strategic, as well as investigative, purposes.[258]

---

this fashion is examined in Section III.B., infra.

[254] There are, as noted earlier, statutory restrictions on certain types of information-gathering. See supra note 249 and accompanying text.

[255] See supra note 248-49 and accompanying text.

[256] See id.

[257] See supra Section I.B. Again, there are statutory restrictions on certain types of information-gathering. See supra note 249 and accompanying text.

[258] See Creating a Trusted Information Network for Homeland Security 31, Second Report of the Markle Foundation Task Force, December, 2003, at http://www. markletaskforce.org/reports/TFNS_Report2_Master.pdf:

> Government agencies have always had access to certain kinds of privately held information. But historically, information requests to commercial organizations were made on a case-by-case basis . . . .
>
> With the advent of data-mining and . . . the increasing computational power of computers . . . agencies at all levels of government are now interested in collecting large amounts of data from commercial sources. Such data might be used not only for investigations of specific people . . . but also to perform

These scenarios are troubling because they allow law enforcement officers to accomplish indirectly what they may not be able to accomplish directly. Assume, for example, that officers are investigating illegal activity and suspect I am involved in this activity. Historically, the only ways for them to pursue that suspicion were (i) to question my associates (which does not implicate my privacy);[259] (ii) to question me (which raises

large-scale data analysis and pattern discovery . . . .

Id. See, e.g., William J. Krouse, The Multi-State Anti-terrorism Information Exchange (MATRIX) Pilot Project 1, Congressional Research Service (2004), http://www.matrix-at.org/CRS_MATRIX_Report.pdf (last visited Aug. 19, 2005) (project intended to let investigators "share and analyze information that is already available to law enforcement from open public and state-owned data, without a subpoena or court order"); see also id. at 8:

> [I]n the past decade, the quantity of personal data held by the private sector has exploded, as computing and storage capabilities have rapidly advanced, and associated costs have correspondingly diminished. The same could be said of public data held by federal, state, and local governments.
>
> Much public and private sector data have been aggregated into "data marts." This information is often available commercially for sale from companies specializing in data aggregation, like ChoicePoint, Equifax, Experian, Qsent, LexisNexis, and Westlaw. With advanced computing technologies tera- and petabytes of data can be manipulated, and multiple data marts can be merged or crossreferenced. Moreover, computer applications are available to `mine' these data for the purposes of profiling, pattern analysis, link analysis, transactional footprinting, and identity verification.

Id. (notes omitted). "Link analysis" is "uncovering relationships that may be indicative of suspicious patterns, groups, or connections." Id. at n.42. "Transactional footprinting" involves identifying "the data trails of suspicious activities by individuals and groups" from the records of their online activity. Id. at n.43. For the evolution of the Matrix Project, see, e.g., ROBERT D. O'HARROW, JR., NO PLACE TO HIDE 98-124 (2005). For another perspective, see, e.g., Creating a Trusted Information Network for Homeland Security 30, Second Report of the Markle Foundation Task Force, December, 2003, at http://www.markletaskforce.org/reports/TFNS_ Report2_Master.pdf (last visited Aug. 19, 2005).

[259] See, e.g., Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the

Fifth Amendment issues);[260] and (iii) to search for physical evidence that was likely to be in my possession and consequently likely to be in "private" areas under my control. The officers cannot pursue option (iii) unless and until they develop probable cause, obtain a search warrant and execute the warrant with the precision it requires.[261]

But option (iii) is compelling only insofar as the information the officers need to confirm my involvement in criminal activity is physical evidence located in "private," physical spaces. Assume that the physical evidence (if any) is not the only means of accomplishing this; assume that I exist in a world where the pervasiveness of technology surpasses its current levels. I may live and work in circumscribed physical spaces, but those spaces, as well as my modes of transportation and the implements I use to conduct my routine activities, are all "live," i.e., they all track my activities.[262] It is almost certain that, in such an environment, the officers could find the confirmatory evidence[263] they need indirectly, by consulting the private enti-

---

Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); see also infra Section III.B.2.

[260] See, e.g., United States v. Mandujano, 425 U.S. 564, 572-73 (1976) (grand jury testimony); Miranda v. Arizona, 384 U.S. 436, 444 (1966) (custodial interrogation).

[261] See supra Section I.A. This is true regardless of whether the officers seek evidence in "private" spaces belonging to me, the suspect, or to others who may or may not have been involved in my criminal activity. See supra note Error! Bookmark not defined. and accompanying text.

[262] See supra Section II.

[263] They can do this in either of two ways: First, in an era of cyberlife and cybercrime, digital evidence may be all they need. If that is true, they should be able to obtain what they need from the various service providers, in the form of transactional data and biographical data (records of my comings and goings, etc.). See supra note Error! Bookmark not defined. and accompanying text. Second, if the criminal activity necessarily involves physical evidence (drugs, murder, theft of tangible property), the information they obtain from these third-parties should be sufficient, directly or inferentially, to provide the probable cause they need to enter my premises to search for and seize the physical evidence.

ties which provide these technologies and, in so doing, incidentally compile information about me.[264] Since I have no Fourth Amendment expectation of privacy in this information, the officers can obtain it without a warrant[265] based on suspicion or simple curiosity. That possibility creates the specter of a twenty-first century analogue of the general warrant,[266] an *ad hoc*

[264] See supra Section II. There are two ways the officers can gain access to this information: The private entities can provide it voluntarily or, if they decline to do so, officers can obtain process not requiring probable cause (court order, subpoena) to compel the entities to cooperate. See supra note 247 and accompanying text.

[265] See supra Section I.B.; see also California Bankers Ass'n v. Shultz, 416 U.S. 21, 94-95 (1974) (Marshall, J., dissenting):

> By compelling an otherwise unwilling bank to photocopy the checks of its customers, the Government has as much of a hand in seizing those checks as if it had forced a private person to break into the customer's home or office and photocopy the checks there . . . . Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that through microfilming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force characteristic of the general warrants which raised the ire of the Founding Fathers . . . . As we emphasized in Katz v. United States, 389 U.S. 347 (1967), the absence of any physical seizure of tangible property does not foreclose Fourth Amendment inquiry . . . . By the same logic, the Fourth Amendment should apply to the recording of checks . . . . And such a massive and indiscriminate search and seizure, not only without a warrant but also without probable cause to believe that any evidence to be obtained is relevant to any investigation, is plainly inconsistent with the principles behind the Amendment . . .

Id. (internal citations omitted). Again, there are statutory restrictions on certain types of information-gathering. See supra note 247 and accompanying text.

[266] See supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text; see also supra note Error! Bookmark not defined. and accompanying text. The dangers of this practice were pointed out almost three decades ago. See Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, Chapter 9, 1977, at http://aspe.hhs.gov/ datacncl/1977privacy/c9.htm (last visited Aug. 19, 2005):

> Traditionally, the records an individual might keep on his daily activities, financial transactions, or net worth were beyond government reach unless the government could establish probable cause to believe a crime had been

procedure that would let officers "investigate merely on suspicion that the law is being violated, or . . . because [they want] assurance that it is not."[267]

Now consider a variation of this hypothetical: Officers are curious about specific illegal activity, either because they have reason to believe it is occurring or because they want assurance that it is not. Since their belief (if any) is not based on articulable facts indicating that the activity is attributable to particular individuals, they cannot utilize the traditional Fourth Amendment dynamic (option (iii)).[268] Instead, they decide to rely on the second scenario available under the new

committed. If government were merely suspicious and wanted to investigate, such records were unavailable. The legal standards that protected them evolved in a world where such records were almost universally in the actual possession of the individual. Reflecting that reality, the law only barred government from seizing records in the possession of the individual . . . . [T]hat world no longer exists. Third parties . . . now keep a great many records documenting various activities of a particular individual. Indeed, these third parties keep records about the individual he would not ordinarily have kept in the past. Records for life and health insurance, for example, are repositories of highly intimate personal data . . . which were virtually unknown until recent decades . . . .

. . . .

The existence of records about an individual that are not in his possession poses serious privacy protection problems . . . . Record keepers can [and] often do, . . . disclose records . . . to government without seeking the individual's approval . . . . A government request made informally through a personal visit to the record keeper or by a telephone call . . . may leave no trace . . . . Even if the individual is given notice and documentation of the disclosure, he has no legal right to challenge the propriety of government access to his records, despite the possibility that the government agent might have been on a "fishing expedition."

Id. (notes omitted).

[267] United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950) (referring to grand jury).

[268] See supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text.

"harvesting" dynamic.[269] They therefore analyze data "harvested" from private entities[270] in an effort to identify transactional or other patterns which inferentially support the conclusion that particular individuals may be engaging in the suspected illegal activity.[271] Some of the data they analyze may pertain to me, but as I have no Fourth Amendment expectation of privacy in that data, I cannot challenge its use.[272] The procedure in this hypothetical is even more analogous to the general warrants the Fourth Amendment was intended to eliminate.[273]

But while the procedures in both hypotheticals—each a variant of the "harvesting" dynamic—are functionally analogous to general warrants, one element is lacking: a violation of privacy. Unless we conclude that the data at issue in scenarios such as these is "private," what is hypothesized here can become reality.

---

[269] See supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text.

[270] They can do this in any of several ways: (i) ask the relevant private entities to provide them with data sets encompassing the individuals and parameters they wish to explore so they can perform the analysis; (ii) ask the relevant private entities to use their data to perform the analysis; or (iii) use data sets they have already acquired from private entities to perform the analysis. See supra note Error! Bookmark not defined.. As noted earlier, the officers can obtain the data voluntarily or through the use of non-Fourth Amendment process. See supra note Error! Bookmark not defined..

[271] See supra note Error! Bookmark not defined..

[272] See supra Section I.B. Again, there are statutory restrictions on certain types of information-gathering. See supra note Error! Bookmark not defined..

[273] See supra note Error! Bookmark not defined. and accompanying text. The purely indiscriminate nature of this procedure makes it more precisely analogous to the writs of assistance which the colonist deeply resented. See, e.g., LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION, supra note Error! Bookmark not defined., at 54 (writ of assistance "was good as a continuous license and authority during the whole lifetime of the reigning sovereign" so the "discretion delegated to the official was therefore practically absolute and unlimited").

B. Options

What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. . . .[274]

If we decide we should address the "harvesting" dynamic by adopting a more expansive interpretation of the Fourth Amendment,[275] we have to deal with the second issue: How *can* we possibly find that information I have shared with others is private? The notion seems hopelessly contradictory: I tender information to others, thereby surrendering control over it and assuming the risk that the recipients will disseminate it, but insist that it somehow remains "private."[276]

To resolve this issue, we must parse the apparent contradiction. It derives from the "assumption or risk" principle articulated in *Katz*:[277] Something is "private" only as long as I shield it from "public" view.[278] Privacy is therefore an oppositional concept; I must take steps to secure my spaces, my activities, and my communications if I am to claim they are "private."[279] But is it also a zero-sum concept? That is, can I share my spaces, my activities and my communications with (some) others and still legitimately claim they are "private?" Does the Fourth Amendment encompass a concept of "shared privacy"? Or is there no middle ground between "private" and "public?"

We actually have very little guidance on this issue. The *Katz*

---

274 Katz v. United States, 389 U.S. 347, 351 (1967).

275 See supra Section III.A.

276 See supra Section I.B.

277 See supra note Error! Bookmark not defined. and accompanying text; see also Section II, supra.

278 See id.

279 See, e.g., Susan W. Brenner, The Privacy Privilege: Law Enforcement, Technology and the Constitution, 7 U. FLA. J. TECH. L. & POL'Y 124, 168-82 (2002), http://grove.ufl.edu/~techlaw/vol7/issue2/brenner.pdf.

Court talked about "public" view, but did not define "public."[280] Inferentially, however, it is clear that I do not forfeit my Fourth Amendment expectation of privacy if I expose my spaces, my activities and my communications to "some" others; the critical distinction seems to be between controlled exposure to those with whom I have a relationship and promiscuous exposure to a generalized public.[281] This distinction is implicit in decisions that have recognized a reasonable expectation of privacy in premises shared by those who have some type of relationship (family, houseguests, roommates).[282] It is clear that I do not surrender my Fourth Amendment expectation of privacy by

---

[280] See supra Section I.A.

[281] See, e.g., Mary I. Coombs, Shared Privacy and the Fourth Amendment, Or the Rights of Relationships, 75 CAL. L. REV. 1593, 1618 (1987):

> The exact contours of . . . shared privacies remain to be explored. Clearly, however, where the claimant is part of a sufficiently small and intimate group that shares a place, she has an expectation of privacy there that should be recognized. For example, assume that a husband has sole legal ownership of the family residence. Few would dispute that his wife, or adult child living at home, should be able to challenge a search of that home.

Id. (notes omitted).

[282] See, e.g., Minnesota v. Olson, 495 U.S. 91, 96-97 (1990); see also id. at 98-99:

> To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share. Staying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society. We stay in others' homes when we travel to a strange city for business or pleasure, when we visit our . . . relatives out of town, when we are in between jobs or homes, or when we house-sit for a friend. We will all be hosts and we will all be guests many times in our lives. From either perspective, we think that society recognizes that a houseguest has a legitimate expectation of privacy in his host's home.

Id. This notion of shared, relational privacy is also evident in Supreme Court decisions recognizing the privacy inherent in our "intimate associations with others." See, e.g., Kendall Thomas, Beyond the Privacy Principle, 92 COLUM. L. REV. 1431, 1445-46 (1992) (quoting Bowers v. Hardwick, 478 U.S. 186, 206 (1986) (Blackmun, J., dissenting)).

"knowingly expos[ing]"[283] my spaces, my activities and my communications to those with whom I share a home, for example.[284] As Justice Scalia said in *O'Connor v. Ortega*, "[i]t is privacy that is protected by the Fourth Amendment, not solitude. A man enjoys Fourth Amendment protection in his home . . . even though his wife and children have the run of the place . . . ."[285]

There *is*, therefore, a middle ground between "private" and "public"; I can claim Fourth Amendment privacy without having to exclude *everyone* from my spaces, my activities, and my communications.[286] But this notion of "shared privacy" seems to be limited; currently, the only relationship that clearly supports a non-zero-sum conception of privacy is the intimate relationship that exists between those who reside together.[287]

---

[283] See supra note Error! Bookmark not defined. and accompanying text.

[284] See supra notes Error! Bookmark not defined.-; see also Coombs, supra note Error! Bookmark not defined., at 1618 ("One reason we protect the legal right to exclude others is to empower the owner to choose to share his home or other property with his intimates"); James B. White, The Fourth Amendment as a Way of Talking About People: A Study of Robinson and Matlock, 1974 SUP. CT. REV. 165, 217 ("Part of the . . . personal privacy is . . . social or communal privacy, the interest people have in the security of their arrangements for sharing what they have with others.").

I do assume the risk of treachery on the part of those with whom I share my home. If, for example, my spouse decides to collect evidence of my criminal activity from our home and take it to the police, I cannot complain. My privacy may have been compromised, but not by state actors. See, e.g., Coolidge v. New Hampshire, 403 U.S. 443, 487-90 (1971).

[285] O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring).

[286] For more on this, see infra Section III.B.2.

[287] See, e.g., Reardon v. Wroan, 811 F.2d 1025, 1027 n.2 (7th Cir. 1987) (holding that members of fraternity had a reasonable expectation of privacy in their fraternity house because a fraternity is an exclusive living arrangement with the goal of maximizing the privacy of its affairs). In O'Connor v. Ortega, a majority of the Supreme Court held that a physician had a reasonable expectation of privacy in his office, but only because he "did not share his desk or file cabinet with any other

That is no doubt because this principle is artefactual; the Fourth Amendment and its common law antecedents were, after all, primarily concerned with protecting the "castle," the home, from unauthorized government intrusions.[288]

How, you may ask, does this narrow non-zero sum conception of privacy pertain to our inquiry into whether we can adopt the more expansive interpretation of the Fourth Amendment that is needed to address the consequences of pervasive technology?[289] It gives us a second alternative, so that we have two conceivable ways of frustrating the "harvesting" scenario:[290] one is to continue to rely on the "assumption of risk" calculus and put the onus on individuals to prevent identifiable personal data from leaking into the "public" domain,[291] and the other is to expand the non-zero sum conception of privacy outlined above so it protects the sharing of personal information in relationships other than those based on common occupancy of a home. These alternatives are examined below.

---

employees." O`Connor, 480 U.S. at 718-19.

[288] See supra Section I.A. See, e.g., Oysted v. Shed, 13 Mass. 520, 522-23 (Mass. 1816):

> The authorities do not clearly show what persons are considered as belonging to the family of a householder, and so having a right to protection under his castle. The very learned judges, Foster, Hale, and Coke . . . say, that the outer doors or windows shall not be forced by an officer, in the execution of civil process against the occupier or any of his family, who have their domicil or ordinary residence there . . . . According to these principles, not only the children and the domestic servants of the occupier are . . . entitled to protection; but, also, permanent boarders, or those who have made the house their home, may properly be considered as a part of the family.

Id. at 522-23

[289] See supra note Error! Bookmark not defined. and accompanying text.

[290] See supra Section III.A.

[291] See supra note Error! Bookmark not defined. and accompanying text; see also Section II, supra.

1. Risk

If we apply the "assumption of risk" calculus,[292] the only way we, as individuals, can frustrate the "harvesting" dynamic is to ensure that our personal information does not fall into the hands of third-parties, e.g., service providers, online merchants, etc.[293] This approach in effect continues the spatial conception of privacy: If I use barriers and other devices to shield my information from others, it is private; if I do not employ such efforts, or if they are futile, I knowingly expose my information to "public" view and it loses any claim to Fourth Amendment protection.[294]

The problem with this approach is that the "assumption of risk" calculus is an unreasonable methodology for a non-spatial world. It assumes, as noted earlier, that I have a choice: to reveal information by leaving it unprotected or to shield it from "public" view.[295] In the real, physical world, these options make sense: I can shield my activities from public scrutiny by drawing the curtains in my living room, installing a fence around my backyard, putting lock on my doors, etc. Inherent in the "assumption of risk" calculus is the assumption that I am *able* to withdraw information about myself (my activities, my health, my preferences) from the public domain. This assumption will continue to retain its validity for the spatially-based activities of my life: I can frustrate my nosy neighbor's attempt to ascertain what I do in the evenings by closing the curtains and employing whatever other devices real-world technology gives me to exclude the physically prying eye. But how can I do this in a world of pervasive technology, a world in which I am necessarily surrounded by devices that collect data and share it

---

[292] See supra note Error! Bookmark not defined. and accompanying text; see also Section II, supra.

[293] See supra Section III.A.

[294] See supra note Error! Bookmark not defined. and accompanying text; see also Section II, supra.

[295] See supra Section II.B.

with external entities?

This is the *Smith-Miller* problem:[296] In *Smith v. Maryland,* the Supreme Court held that Smith had no "expectation of privacy" in the numbers he dialed from his home telephone.[297] The Court held that Smith "voluntarily conveyed numerical information to the telephone company and `exposed' that information . . . . In so doing," he "assumed the risk that the company would reveal to police the numbers he dialed."[298] The problem with this holding is that it erroneously assumes Smith had a choice. In fact, since had no way to shield the numbers he dialed from the telephone company, the only choice Smith had to minimize his risk of being observed was to leave home and use a pay phone.[299]

That may seem a trivial matter, but consider the implications this decision has for life in a world of more pervasive technology: I install an alarm system in my home; it lets the security company monitor my routines (when I retire and arm the system, when I rise and disarm it), my comings and goings (arming and disarming the system each time) and the extent to which I give others access to my home (canceling false alarms, adding new user codes, etc.). Under *Smith*, I have no reason-

---

296 See supra Section I.B.

297 See Smith v. Maryland, 442 U.S. 735, 744 (1979); see also supra Section I.B.

298 Smith, 442 U.S. at 744. See supra Section I.B.

299 See, e.g., Smith, 442 U.S. at 749-50 (Marshall, J., dissenting):

> Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of `assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.

Id. (citing Lopez v. United States, 373 U.S. 427 (1963); Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 475 (1971) (plurality opinion)).

able expectation of privacy in the data gathered by the security company because I voluntarily allowed the company to collect this information without encrypting or otherwise shielding it from their review; of course, if I did that (assuming I was able to do so), it would frustrate the purpose of the alarm system. My only choices under *Smith*, therefore, are to (i) trade security for privacy or (ii) trade privacy for security.[300]

The evolution and proliferation of more pervasive, more complex technologies will present us with other, equally-illogical choices. If I am elderly and choose to live in one of the "smart homes" currently being developed, have I surrendered all privacy? The home monitors my activities, my intake of food and medications, my temperature, my sleep and wake cycles, my interactions with vendors and with friends; its embedded systems interact with me and, in so doing, compile data continually.[301] The home uses this data to assess whether I need assistance, perhaps to order food and other necessities for me and to call for assistance if I seem ill or injured. In so doing, it shares data about me with its central control center and with a host of other entities. By choosing to live in such a home, again for the sake of security, have I surrendered all privacy in the data it compiles?[302]

This question arises for any technology that results in the collection of personal data.[303] Essentially, *Smith* presents us with a Hobson's choice:[304] Embrace technology and surrender

---

300 See supra note Error! Bookmark not defined..

301 See, e.g., Cory D. Kidd, et al., The Aware Home: A Living Laboratory for Ubiquitous Computing Research 7, GEORGIA INSTITUTE OF TECHNOLOGY—THE AWARE HOME RESEARCH INITIATIVE (1999), available at http://www.cc.gatech.edu/fce/ahri/publications/cobuild99_final.PDF ("An important issue that must be addressed . . . is . . . privacy. The home is constantly monitoring the occupants' whereabouts and activities, using audio and video observation methods, and even tracking its inhabitants' medical conditions").

302 The same question arises, of course, if I choose to live in such a home merely because of convenience.

303 See supra Section III.A.

304 A Hobson's choice is a choice with no real alternative. See Hobson's

privacy in the data it compiles and disseminates or reject technology and thereby prevent the exposure of one's personal data. The problem with this equation is that one must become a Luddite to frustrate the "harvesting" dynamic.[305] It ignores the fact that we are not living in the seventeenth century; we live in an environment in which technology is an increasingly essential, invisible component of our lives.[306] There is no twenty-first century analogue of the adhesive envelope.[307] I may be able to encrypt the contents of my communications,[308] but I cannot shield my online activity from my service provider, conceal the nature and extent of my online purchases, or mask information generated by systems in my home, my office, and my vehicle. There can, therefore, be no legitimate inference that in sharing that information with that narrow circle I am willing to share it with the entire world or with the government.

Smith is another *Olmstead*. When *Olmstead* was decided, the technology was in place but the implications were not clear; by the Supreme Court decided *Katz*, it had become clear what was at stake in wiretapping. When *Smith* was decided a quarter of a century ago, the Internet was in its infancy and personal computers had yet to appear; the technology was not yet in place, and so the implications were not clear.[309] We are now

choice, Dictionary.com, at http://dictionary.reference.com/search?r=10&q=Hobson's%20choice (last visited Aug. 16, 2005).

[305] See supra Section III.A.

[306] See supra Section II.

[307] See supra notes Error! Bookmark not defined.-Error! Bookmark not defined. and accompanying text.

[308] See, e.g., About Hushmail, Hushmail.com, at http://www.hushmail.com/about?PHPSESSID=994c85ba654ae97074f261d2dceb5190 (last visited Aug. 16, 2005).

[309] See, e.g., Barry M. Leiner, et al., A Brief History of the Internet, at http:// www.isoc.org/internet/history/brief.shtml#Initial_Concepts (last visited Aug. 16, 2005).

approaching a critical set of issues—the effects of technology of an unparalleled sophistication on our privacy. While the *Katz* "assumption of risk" calculus may still be valid for traditional activity in the real, physical world, it cannot be used to operationalize privacy in an era of pervasive technology.[310] The sophistication and functionality of these technologies means that the element of choice is lacking. Our only hope, therefore, for frustrating the "harvesting" scenario is to expand the non-zero-sum conception of privacy outlined above.[311]

2. Relationship

Smith is another *Olmstead* conceptually, as well as in the more pragmatic sense noted above.[312] The Supreme Court held that Roy Olmstead did not have a Fourth Amendment expectation of privacy in the content of his telephone communications because he used a "telephone instrument" with "connecting wires" to "project his voice to those quite outside" his home.[313] The *Olmstead* majority did not recognize that Olmstead was not broadcasting the content of his communications to the world at large; instead, he was making a controlled, focused disclosure of communicative content to an identified individual over a network inaccessible to one not equipped with specialized interception devices.[314]

The *Katz* Court understood this and therefore reversed *Olmstead*.[315] The *Smith* Court somehow failed to see the analogy between Katz conveying substantive data via the telephone

---

310 The Supreme Court recognized this, at least to some extent, when it held that using thermal imaging technology to detect information from inside a home is a search under the Fourth Amendment. See Kyllo v. United States, 533 U.S. 27, 34 (2001) (to hold otherwise would "be to permit police technology to erode the privacy guaranteed by the Fourth Amendment").

311 See supra Section III.B.

312 See supra Section III.B.1.

313 See supra note Error! Bookmark not defined..

314 See supra Section I.A.3.

315 See supra Section I.A.3.

company and Smith conveying switching information to the telephone company.[316] If we take the *Katz* Court at its word, and operate on the premise that the Fourth Amendment protects "people, not places,"[317] the result should be the same in both cases.[318] If substantive, consciously intelligible communication is protected (the conversation), nominally intelligible data should be protected as well.

To understand why that is so, we must consider the implications of the non-zero-sum conception of privacy outlined earlier.[319] That so far narrow conception of privacy recognizes a middle ground between "private as sequestered" and "public."[320] It derives from common law principles that anteceded the Fourth Amendment and were intended to secure citizens' right to enjoy the "intimate activities" of the home free from arbitrary intrusions by government authorities.[321] As noted earlier, these common law principles recognized a concept of "shared privacy" based upon certain relationships—e.g., family members,

---

316 See supra Section I.B.; see also Section I.A.3.

317 See supra note Error! Bookmark not defined. and accompanying text.

318 See, e.g., Smith, 442 U.S. at 752 (Marshall, J., dissenting):

> Just as one who enters a public telephone booth is `entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' . . . so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded . . . solely for the phone company's business purposes. Accordingly, I would require law enforcement officials to obtain a warrant before they enlist telephone companies to secure information otherwise beyond the government's reach.

Id. (quoting Katz, 389 U.S. at 352).

319 See supra Section III.B.

320 See supra Section III.B.

321 See supra Section I.A. See, e.g., United States v. Dunn, 480 U.S. 294, 301 n.4 (1987) (Fourth Amendment intended to protect the "intimate activities associated with domestic life and the privacies of the home"); Dow Chemical Co. v. United States, 476 U.S. 227, 236 (1986) (Fourth Amendment protects the "intimate activities associated with family privacy and the home"); see also supra Section III.B.

servants, guests—and this concept was implicitly incorporated into the Fourth Amendment.[322]

Building on *Ex parte Jackson*,[323] the *Katz* Court recognized that this shared privacy was portable, i.e., could survive transmission from one private enclave (home, office, telephone booth) to another.[324] Interestingly, neither of the communications at issue in these cases involved the "intimate activities" of the home, the original locus of shared privacy: Ireland Jackson mailed a lottery circular,[325] and Charles Katz was a bookie who called a gambler to place bets for his customers.[326] Both cases recognized a Fourth Amendment expectation of privacy in the content of secure communications—including "commercial" communications—that are in transit to another. The fact that the contents were to be revealed to another person was not fatal because the sender had taken steps to ensure that the information was only communicated to that person; both Jackson and Katz, in other words, were attempting to make a controlled disclosure of information to another person.

Now, one can argue that the result in these cases is irrelevant to the point under consideration here—the privacy of information conveyed to third parties—because both of these cases were concerned with "sealed" information that *had not yet been revealed to another*. Viewed in this light, these cases can be seen as involving nothing more than an application of the

---

322 See supra Section III.B.

323 See supra Section I.A.1.

324 See supra §§ I(A)(1) and I(A)(3); see also Katz, 389 U.S. at 352 (citing Jackson for the proposition that what one seeks to preserve as private, even in a "public" area, can be protected by the Fourth Amendment).

325 See supra Section I.A.1. Jackson was indicted for "unlawfully depositing . . . in the mail of the United States . . . a circular concerning a lottery . . . enclosed in an envelope addressed to one J. Ketcham, at Gloversville, New York." Ex parte Jackson, 96 U.S. 727, 727 (1877).

326 See, e.g., William W. Greenhalgh & Mark J. Yost, In Defense of the "Per Se" Rule: Justice Stewart's Struggle to Preserve the Fourth Amendment's Warrant Clause, 31 AM. CRIM. L. REV. 1013, 1068 (1994).

"assumption of risk" principle:[327] By employing measures to secure (adhesive envelope, phone booth)[328] the contents of their communications, Jackson and Katz had a Fourth Amendment expectation of privacy in their contents until they reached their respective destinations. In this view, the contents of Jackson's circular and of Katz's calls were private only while they were in transit; once they reached the recipients they were no longer private because they had been communicated to another person.

But why must it follow that a "private" communication inevitably ceases to be private once the information it contains has been received? This proposition apparently rests on the assumption that by revealing information to another I assume the risk she will prove unfaithful and reveal that information to the police. But we recognize a narrow concept of shared privacy which encompasses communications and activities we reveal to those with whom we share the "intimate activities" of the home, even though they, too, could prove unfaithful.

This concept of shared privacy is so embedded in our history and culture that the reasons for its existence are seldom articulated.[329] Clearly, though, it is based on two considerations: (1) It facilitates intimacy and security in our domestic lives, which would be poor and solitary[330] if we had to shield our every word and action from those with whom we live; and (2) it encompasses disclosures made to those with whom we share a relationship that makes it "reasonable" to assume they will respect the limited nature of these disclosures.[331] These consid-

---

[327] See supra note Error! Bookmark not defined. and accompanying text; see also Section II, supra.

[328] See supra §§ I(A)(1) and I(A)(3).

[329] See generally supra Section III.B.

[330] See supra note Error! Bookmark not defined. and accompanying text. In Leviathan, Thomas Hobbes described the life of man in a state of nature as "solitary, poor, nasty, brutish, and short." THOMAS HOBBES, LEVIATHAN, available at http://oregonstate. edu/instruct/phl302/texts/hobbes/leviathan-c.html#CHAPTERXIII (last visited Aug. 15, 2005).

[331] See generally supra Section III.B.

erations differentiate this shared domestic privacy from the line of cases in which the Supreme Court has held that wrongdoers assume the risk of the disclosures they make to our criminal associates.[332] Recognizing shared privacy among criminal confreres would serve no useful purpose and would run contrary to the pragmatic observation that there is no honor among thieves.

We may want miscreants to betray each other, but that should not be true for other, legitimate relationships. Trust is a fundamental principle of democracy; we need to be able to trust those with whom we have certain relationships, and we need to be able to trust that law enforcement will respect those relationships.[333] Otherwise, we descend into a state of paranoia and keep each other at arm's length;[334] this is the basic flaw in the "assumption of risk" principle. In a world of evolving technology, it results in an "arm's race" in which I have a reasonable expectation of privacy only as long as and insofar as my technology successfully frustrates law enforcement efforts to subject my activities to scrutiny.[335] And there is nothing I can do to

---

[332] See, e.g., Hoffa v. United States, 385 U.S. 293, 302 (1966) (Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[333] See, e.g., Erik Luna, Transparent Policing, 85 IOWA L. REV. 1107, 1158-60 (2000):

> Trust is . . . a fundamental ingredient of modern liberal democracy, with social contract theorists maintaining that consent grounded in public trust provides the very basis for governmental authority . . . . Distrust leads to the self-interested atomization of the citizenry and a lack of cooperation within the community. Most importantly, popular mistrust of government undermines the perceived legitimacy of the law, which in turn reduces public compliance with legal commands.

Id. (notes omitted).

[334] See supra note 333.

[335] See supra Section III.B.1. See, e.g., Scott Granneman, Email Privacy Is Lost, SECURITY FOCUS (July 29, 2004), at http://www.securityfocus.com/columnists/258 ("This is an arms race. Every time the technology changes to enable further surveillance, something happens to render that surveillance inopera-

maintain informational privacy[336] as long as we insist that any disclosure of information not encompassed by the narrow conception of shared privacy outlined earlier automatically puts that information in the "public" domain.[337]

Can we alter the latter principle? Would it be "reasonable" to incorporate another, broader conception of shared privacy into the Fourth Amendment in order to protect the privacy of information I share with certain third parties? Would such a step be fundamentally inconsistent with the history and purposes of the Fourth Amendment?

We could extrapolate such a principle from the narrower conception of shared privacy that anteceded and was implicitly incorporated into the Fourth Amendment. The critical issue is deciding how far we want to go in protecting information held by various third parties.

Let us begin with the easiest case. The current conception of shared privacy evolved to protect the "intimate activities" of the home and, as such, encompassed those who were privy to such activities, e.g., family, houseguests, and servants.[338] We cannot "reasonably" construe third-party information holders as family members or houseguests because the familial and residential ties are lacking; even entities that provide alarm and other services and that will interact with systems in "smart homes" do so remotely, from some other physical location. But these entities are functionally analogous to "servants" who are also encompassed by this conception of shared privacy; unlike the servants of centuries ago, they do not reside in the home, but they provide services that promote and sustain activities within the home. And we maintain a relationship with them that is analogous to the relationship householders of the common law era maintained with their servants; the basis of this

ble . . . at least until the next technological change.").

[336] See supra note Error! Bookmark not defined. and accompanying text.

[337] See supra Section I.B.

[338] See supra Section III.B.

relationship is a pecuniary arrangement, but it also involves continuity and trust.

We rely on "servant" entities for support; we may sometimes switch between entities, but this is the exception; our preferred mode is one of stability in which we have established, ongoing relationships with entities that provide the various types of support we require. It is reasonable to anticipate that the continuity of these relationships will increase as we come to rely on increasingly complex, interdependent technologies; it is one thing to change our telephone company, quite another to modify a multi-functional network.[339] The other notable feature of these relationships is trust:[340] We give those with whom we have established such a relationship access to personal, "private" information so they can discharge the functions for which they are employed.[341] We do, as the *Smith* Court said, volun-

[339] See supra Section II.

[340] See, e.g., State v. Hunt, 91 N.J. 338, 346-47, 450 A.2d 952, 956 (1982):

> The telephone caller is . . . entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes. From the viewpoint of the customer, all the information which he furnishes with respect to a particular call is private. The numbers dialed are private. The call is made from a person's home or office, locations entitled to protection under . . . Article I, par. 7 of the New Jersey Constitution.

Id.

[341] See supra Section II.

Some states have recognized a reasonable expectation of privacy in third-party records under their own constitutions. See, e.g., State v. McAllister, 366 N.J. Super. 251, 264-65, 840 A.2d 967, 975-76 (2004):

> [W]e hold that there exists a reasonable expectation of privacy in a person's bank records. . . . We are in full accord with Justice Mosk's articulation of the pervasiveness of the need to make and maintain bank records as an incident of private, personal financial life and participation . . . in modern economic life. . . .
>
> The discomfort in finding a stranger poring over one's checkbook, deposit slips and cancelled checks is equal to seeing someone . . . reviewing a list of dialed telephone numbers called from home . . . . Banks, like telephones, are

> an extension of one's desk or home office. Indeed, as in the case of the telephone, technological advances in the form of personal computers with access to the internet and electronic banking services have made those services available to the homes of its depositors. Bank records kept at home could not be seized in the absence of a duly issued search warrant based upon probable cause and they should not be vulnerable to viewing, copying, seizure or retrieval simply because they are readily available at a bank.
>
> Finally, the fact that financial affairs are memorialized in written records of banks or maintained in their electronic data systems to which, as part of its legitimate business, a bank's employees have access, does not suggest that persons have any sense that their private and personal traits and affairs are less confidential when they deal with their bank than when they make telephone calls . . . . The repose of confidence in a bank goes beyond entrustment of money, but extends to the expectation that financial affairs are confidential except as may be reasonable and necessary to conduct customary bank business.

Id. (citing Burrows v. Superior Court, 13 Cal. 3d 238, 118 Cal. Rptr. 166, 172, 529 P.2d 590 (1974)). States have also rejected the logic of Smith. See, e.g., People v. Spoerleder, 666 P.2d 135, 141 (1983):

> A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society. When a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office . . . . The concomitant disclosure to the telephone company, for internal business purposes, of the numbers dialed by the telephone subscriber does not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government. . . .
>
> We view the disclosure to the telephone company of the number dialed as simply the unavoidable consequence of the subscriber's use of the telephone as a means of communication . . . . Any use the telephone company might make of such information for its own internal accounting purposes is far different from governmental evidence gathering. . . .
>
> . . . .
>
> One's disclosure of certain facts to the telephone company as a necessary concomitant for using an instrument of private communication hardly supports the assumption that the company will voluntarily convey that information to others. Telephone companies are in the business of providing telephone subscribers with the equipment necessary for electronic communication in today's world. . . . The expectation that information ac-

tarily convey information to these entities,[342] but we do not do so recklessly, or promiscuously; we convey information to our "servant" entities in a secure fashion intending that it be used only for the purpose of allowing the entity to perform the services for which we have contracted.[343]

We trust our "servant" entities not to reveal our personal information to tabloids, disgruntled relatives, and other "civilians," and they generally live up to our expectations. Why, then, is this relationship, and the information it generates, not within the Fourth Amendment?[344] The obvious response to this question is that bringing this relationship within the Fourth Amendment is unnecessary since these entities are not *obligated* to provide this information to law enforcement. This, however, ignores reality.[345] A private entity may find it unsettling to refuse to cooperate with law enforcement, or may not understand the consequences of doing so, in terms of larger-

> quired by the telephone company will not be transferred . . . to the government for use against the telephone subscriber appears to us to be an eminently reasonable one.

Id.; see also State v. Thompson, 114 Idaho 746, 750-51, 760 P.2d 1162, 1166-67 (1988) (use of a pen register is a search requiring a warrant under Idaho Constitution).

[342] See supra Section I.B.

[343] See Smith, 442 U.S. at 749 (Marshall, J., dissenting): "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." See, e.g., State v. Mollica, 114 N.J. 329, 344-45, 554 A.2d 1315, 1323 (1989) (police must obtain search warrant to secure telephone records); see also supra note Error! Bookmark not defined..

[344] One might argue that the information itself is not worthy of protection because while it is data that can give rise to inferences about activities taking place within the home, this information does not, in and of itself, describe such activities. The Supreme Court rejected a similar argument in Kyllo v. United States, 533 U.S. 27, 37 ("The Fourth Amendment's protection of the home has never been tied to . . . the quality . . . of information obtained"); see also supra Section I.A.4.

[345] See supra note Error! Bookmark not defined..

scale privacy issues.[346] And a subpoena can be used to compel a truly reluctant entity to provide this information without providing the protection accorded under a warrant.[347]

The critical question is who should bear the risk: the individual (who currently loses privacy by sharing information with external entities) or law enforcement (which will have to demonstrate individualized suspicion to obtain shared information if we define it as private).[348] If we bring this information within the Fourth Amendment by incorporating a shared privacy principle into our Fourth Amendment doctrine, we (1) enhance the security of the relationship between individuals and their "servant" entities, thereby enhancing privacy and trust; and (2) do not put this information totally outside the reach of law enforcement. Bringing this information within the Fourth Amendment simply means that to obtain information from "servant" entities, law enforcement officers have to obtain a warrant supported by probable cause.[349] That reduces the possibility that the officers will be able to bypass the protections of the Fourth Amendment by utilizing the "harvesting" scenarios outlined earlier[350] and ensures that we maintain the proper bal-

---

346 See supra note Error! Bookmark not defined..

347 See, e.g., United States v. Miller, 425 U.S. 435, 437 (1976).

348 See PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, CHAPTER 9 (1977), http://aspe.hhs.gov/datacncl/1977privacy/c9.htm:

> The balance to be struck is an old one; it reflects the tension between individual liberty and social order. The sovereign needs information to maintain order; the individual needs to be able to protect his independence and autonomy should the sovereign overreach. The peculiarly American notions of legally limited government and the protections in the Bill of Rights provide broad . . . standards for reaching a workable balance. But the world has a way of disrupting the particular balance struck in past generations; the theory may remain unaltered but circumstances change, requiring a reworking of the mechanisms which maintained the balance in the past.

Id.

349 See supra note Error! Bookmark not defined..

350 See supra Section III.A.

ance between privacy and law enforcement.[351] If we incorporate this conception of shared privacy into our Fourth Amendment doctrine, we will then have to address a secondary issue: Do we limit shared privacy to information generated by relationships directed at our homes, or do we expand it out to encompass any relationship with a "servant" entity? Do we, in other words, recognize shared privacy in the information individuals engaging in commercial, professional and service endeavors share with their "servant" entities, as well? If we do that do we also extend the concept to encompass the relationship commercial, educational and other entities share with their "servant" entities? Or do we limit shared privacy to information that can, in effect, be used to gain access to the activities within our homes?

Those are difficult questions, the resolution of which is quite beyond the scope of this essay. Essentially, they raise two dichotomies: individual and entity; home and not-home. Extending Fourth Amendment principles to encompass information an individual shares with a "servant" entity that provides support services for the individual's home is the easiest scenario because it is the closest to the spatially-based conception of privacy upon which the Fourth Amendment is predicated.[352] Extending Fourth Amendment shared privacy to encompass the information an individual shares with a "servant" entity that provides support services to the individual's place of business seems to be more of a stretch, simply because we think of places of business as inherently "public." But the Supreme Court has extended traditional Fourth Amendment spatial privacy to places of business;[353] officers therefore must get a search war-

---

[351] It has the added advantage of eliminating the current, increasingly unworkable, distinction between content information and "other" information. See, e.g., Susan Freiwald, Uncertain Privacy: Communication Attributes After The Digital Telephony Act, 69 S. CAL. L. REV. 949, 954-58 (1996).

[352] See supra Section I.A.

[353] See Marshall v. Barlow's, Inc., 436 U.S. 307, 311-12 (1978):

> The . . . Fourth Amendment protects commercial buildings as well as private

rant to seek evidence they believe is located in commercial or professional offices.[354] We could, therefore, "reasonably" extend shared privacy to individually-owned places of business; our primary concern, after all, is with protecting the privacy of individuals,[355] and information-sharing in this context involves a relationship initiated by an individual. Such an extension of shared privacy would also recognize the extent to which we conduct "personal" matters that were once limited to our homes, from our offices.[356]

The entity/not-home option is more problematic. The Supreme Court has held that "corporations can claim no equality with individuals in the enjoyment of a right to privacy."[357] Since privacy is a personal construct, it seems we cannot justify extending shared privacy to artificial entities, unless we were to decide such a step is necessary to protect the privacy of individuals associated with the artificial entity. Of course, if we felt that such a step was necessary, the more logical approach

> homes. To hold otherwise would belie the origin of that Amendment, and the American colonial experience. . . . The general warrant was a recurring point of contention in the Colonies immediately preceding the Revolution. The particular offensiveness it engendered was acutely felt by the merchants and businessmen whose premises and products were inspected for compliance with the several parliamentary revenue measures that most irritated the colonists. `[The] Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance . . . [that] granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods.' Against this background, it is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence.

Id. (citations omitted) (quoting United States v. Chadwick, 433 U.S. 1, 7-8 (1977)).

[354] See Camara v. Municipal Court, 387 U.S. 523, 528-529 (1967); See v. City of Seattle, 387 U.S. 541, 543 (1967).

[355] See supra note Error! Bookmark not defined. (privacy of "merchants and businessmen").

[356] It would also eliminate conceptual difficulties that would arise when someone's home and office were physically located on the same premises.

[357] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

would be to focus on the individuals, not the artificial entity; that is, we could decide to extend the concept of shared privacy to encompass an individual's relationship with an artificial entity that was not engaged in providing support services to the individual's home or office. This would protect the individual's information-sharing with the artificial entity without requiring us to extrapolate an individually-based notion of shared privacy (e.g., individual-individual and individual-"servant" entity) to a collective entity.

IV. CONCLUSION

Ubiquitous technology presents us with the challenge of deciding how we want to apply the Fourth Amendment in a world that is very different from the world from which it sprang.[358] Informational privacy[359] was almost nonexistent in the seventeenth and eighteenth centuries; in that world there were no computers, no copying machines, no credit card transactions, no telephones or other services provided by externalities, no insurance companies, no educational or employment records, none of the kinds of data we routinely generate in the course of our lives.

Citizens of that era engaged in transactions with vendors, but the transactions were in cash and generated few, if any, written records;[360] while a vendor may have recalled some details of my transactions, those details were not documented and preserved in some more or less permanent form. And whatever information resulted from these transactions was in limited form; I traveled to the vendors and dealt with them externally in a "public" place. They were not privy to the details of life in my home; those details were available only to the inti-

358 See supra Section I.A.

359 See supra note Error! Bookmark not defined. and accompanying text.

360 Credit existed in the seventeenth and eighteen centuries, but it was limited to the mercantile and privileged classes. See, e.g., MAUREEN WALLER, 1700: SCENES FROM LONDON LIFE 7, 204, 242 (2000).

mates—family, guests, servants—with whom I shared the physical privacy of my home. The only records that were likely to exist as to me and my activities were in my possession: "papers" I created myself and letters from others. Since copying machines, carbon paper and other implements of replication did not exist, a "paper" was usually an original,[361] which made it relatively easy to control access to the information it contained; it could be held by only one person at a time. I could therefore physically secure my "papers" inside my home, in a chest or a cabinet, or a desk; once the common law antecedents of the Fourth Amendment appeared, it was clear that law enforcement could not enter my home to violate my privacy and inspect my "papers" without securing a warrant.[362] This was sufficient to protect my spatial and informational privacy from arbitrary governmental action; aside from physical entry into my premises, there was no other way law enforcement could access my personal information (other than the generalized, reputational information I disseminated by acting in "public" places).

This approach is no longer sufficient. The physical and informational barriers we once used to differentiate between our "private" and "public" selves are being eroded by technology, and the erosion is accelerating. If we persist in utilizing a zero-sum, spatial conception of privacy to implement the Fourth Amendment, we will render it ineffective as a guarantor of privacy in the face of arbitrary government action.[363] If we continue along this path, the Fourth Amendment will become, in effect, an artifact—a device that protects against a limited class of real-world intrusions (which will become increasingly unnecessary given the other alternatives).[364]

---

361 See, e.g., WALTER M. BESANT, LONDON IN THE TIME OF THE STUARTS 53 (1903) (describing seizure of the "papers" of James Howell, who was a suspected spy).

362 See supra Section I.A.

363 See supra Section III.A.

364 See supra Section III.A.