3-1-1994

A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures

Sherry F. Colb
Cornell Law School, sfc44@cornell.edu

A WORLD WITHOUT PRIVACY: WHY PROPERTY DOES NOT DEFINE THE LIMITS OF THE RIGHT AGAINST UNREASONABLE SEARCHES AND SEIZURES

*Sherry F. Colb**

Imagine for a moment that it is the year 2020. An American company has developed a mind-reading device, called the "brain wave recorder" ("BWR"). The BWR is a highly sensitive instrument that detects electrical impulses from any brain within ten feet of the machine. Though previously thought impossible, the BWR can discern the following information about the target individual: (1) whether he or she is happy, sad, anxious, depressed, or irritable; (2) whether he or she is even slightly sexually aroused; (3) whether he or she is taking any medication (and if so, what the medication is); (4) if a female subject, whether she is pregnant; (5) whether he or she is experiencing a feeling of guilt or remorse; and (6) whether he or she is having aggressive impulses toward another person or persons. At this stage in its development, we do not know whether or not the BWR will advance beyond detection of this information and whether or not it will become generally available to the public. It is currently a technology that belongs exclusively to the government and to extremely wealthy private collectors.

Under Professor Orin Kerr's provocative and interesting thesis,[1] federal or state police could use the BWR on innocent people without implicating their Fourth Amendment rights against unreasonable

* Professor of Law and Judge Frederick B. Lacey Scholar at Rutgers Law School-Newark. A.B. 1988, Columbia (Valedictorian); J.D. 1991, Harvard (magna cum laude). —Ed. The author gratefully acknowledges Michael C. Dorf, for his extremely helpful comments, suggestions, and feedback, and William O'Sullivan, for his expert research assistance. Thanks are also due to the editors of the *Michigan Law Review* for their excellent work. This project was funded in part by the Dean's Summer Research Fund of Rutgers Law School-Newark. Finally, the author thanks Orin S. Kerr, for his eloquent and thought-provoking article. In this response, Professor Colb has taken the opportunity to articulate some of her own views on the subject at issue. As a result, some of her arguments do not directly contradict Professor Kerr's positions (at least not those expressed in the published version of his article). Also, in the interest of giving Professor Kerr the last word, Professor Colb has not advanced a rebuttal of his reply. She hopes and believes that her response piece stands on its own.

1. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 799, 855-86 (2004).

searches and seizures.[2] To be more concrete, if, for example, the police were to utilize the BWR to determine whether John Doe — a man who neighbors say seems "strange" and doesn't "fit in" — feels sexually aroused when he is in the presence of women, the man could not complain of an invasion of any Fourth Amendment reasonable expectation of privacy.

On Kerr's analysis, while existing Fourth Amendment doctrine nominally protects normatively and empirically reasonable expectations of privacy, in practice, in almost all cases, the doctrine protects only property (in a broad and flexible sense, so that it includes rented spaces, for example) but not privacy. Because the BWR reads Doe's internal state without physically trespassing on his property, the regulation of its use — as a matter of most of the case law — should be left to Congress. As a normative matter, Kerr proposes that the Supreme Court defer to Congress in the area of handling the privacy implications of evolving technologies.

The Supreme Court and other judicial bodies, according to Kerr, would have a difficult time understanding the mechanics of how the BWR works or the context in which it might be used, whether by private people or by law enforcement.[3] Moreover, the courts would be unlikely even to reach the issue of how the Fourth Amendment

---

2. Though Kerr acknowledges that cases such as *United States v. Karo*, 468 U.S. 705 (1984), *United States v. Knotts*, 400 U.S. 276 (1983), and *Kyllo v. United States*, 533 U.S. 27 (2001), might limit the use of such technologies, Kerr, *supra* note 1, at 830, he deems them departures from the Court's usual approach and explains them as linked to property rights with which the information disclosed was ordinarily associated, though not to any extant property right with which the technology interferes. This characterization, however, has no explanatory power, because any time one invades privacy without actually interfering with property rights, it is possible to characterize the invasion of privacy at a level of generality that associates it with some traditional property right. For example, the BWR device could be described as an attack on property rights by noting that it exposes information that traditionally could be obtained only by seizing a person's journals. Kerr's phrase "property, broadly construed" thus gives us no information, except post hoc, about whether the Court might see fit to extend Fourth Amendment protection to it.

3. *See* Kerr, *supra* note 1, at 871-83. Kerr describes several examples of courts struggling to understand new technologies. *Id.* at 876. For example, in *United States v. Bach*, 2001 WL 1690055 (D. Minn. Dec 14, 2001), *rev'd* 310 F.3d 1063 (8th Cir. 2002), the U.S. Court of Appeals for the Eighth Circuit reversed a district court's finding that the Fourth Amendment required law enforcement presence at an Internet Service Provider's facility during a search for information on the ISP's servers. Kerr, *supra* note 1, at 876-77. Kerr asserts that "[t]he district court judge apparently assumed that the skills required to search a computer server are similar to the skills required to search physical property." *Id.* at 877.

Similarly, in *Trulock v. Freeh*, the U.S. Court of Appeals for the Fourth Circuit held that a girlfriend's consent to the search of a computer that she shared with her boyfriend did not allow law enforcement officials to search the boyfriend's password-protected files stored on that computer. *See* Kerr, *supra* note 1, at 879 (citing 275 F. 3d 391, 403 (4th Cir. 2001)). Kerr criticizes the court's decision because it failed to discuss the technical details about password-protection necessary to articulate exactly what the court found to be improper. Kerr, *supra* note 1, at 878-80. Kerr suggests "that the judges . . . simply didn't understand enough about the technology of password-protection to know that their opinion left the rule unclear." *Id.* at 880.

applies to the BWR for many years after its appearance on the technological scene.[4] Congress would therefore represent (and has historically represented) a better source of protection for our privacy from hi-tech government intrusion than the judiciary.

In one sense, the source of our privacy does not seem to matter very much. Most people would presumably want to be protected from the use of the BWR, particularly when the government lacks probable cause or some other articulable basis for suspecting the individual targeted. But if we were effectively protected from such intrusion, then the fact that it was Congress doing the protecting rather than the courts would probably not make much of a difference in people's lives. Indeed, most Americans probably do not even know — when they think about particular privacy rights — whether those rights exist as a matter of statutory or constitutional law.

The question for courts, however, and for those like Professor Kerr and myself who study the constitutional law of criminal procedure, is not whether robust privacy protection from Congress is somehow better or worse than what courts can provide. The appropriate question is whether courts have (and whether they ought to have) an obligation to apply the Fourth Amendment to new technologies[5] that could invade privacy without physically trespassing on anyone's private property. Kerr answers this question no, and I answer it yes.

Because I like to draw links between substantive and procedural privacy,[6] I cannot resist drawing a comparison between Kerr's proposal regarding technology and the Fourth Amendment, on the one hand, and arguments about abortion and substantive due process, on the other. If the Supreme Court had decided *Roe v. Wade*[7]

---

4. *See id.* at 866-69. Kerr describes several examples of considerable time elapsing between the emergence of a new technology and the court's consideration of any resulting Fourth Amendment implications. For example, Kerr observes, "[t]he Supreme Court first considered the Fourth Amendment implications of wiretaps almost six decades after the invention of the telephone. Pen registers were in widespread use by the 1960s, but the Supreme Court did not pass on whether their use violated the Fourth Amendment until 1979." *Id.* at 867 (citations omitted). Kerr further notes:

> Even today, no Article III court at any level has decided whether an Internet user has a reasonable expectation of privacy in their e-mails stored with an Internet service provider; whether encryption creates a reasonable expectation of privacy; or what the Fourth Amendment implications of the 'Carnivore' Internet surveillance tool might be.

Id. at 867-68 (citations omitted).

5. Kerr limits his proposal to new and rapidly changing technologies. *See id. passim.* Given short product cycles for nearly everything, new technologies will almost invariably undergo rapid change. Accordingly, I refer here simply to new technologies.

6. *See* Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1644 (1998) (urging "a vision of the Fourth Amendment reasonableness requirement that contains both substantive and procedural safeguards").

7. 410 U.S. 113 (1973).

differently, some argue, state and/or federal law might well have protected the right to abortion.[8] Such protection would have been more legitimate than what the Supreme Court offered, critics suggest, because it would have emerged from a fact-sensitive body more able to give a nuanced consideration to all of the medical and technological dimensions of the problem.[9]

In a dissenting opinion in *City of Akron v. Akron Center for Reproductive Health, Inc.*,[10] for example, Justice O'Connor suggested that, with advances in technology that push fetal viability earlier into pregnancy, the trimester framework established by *Roe* was "clearly on a collision course with itself."[11] She thereby implied that the Court — by protecting the right to abortion — had ventured into territory where it lacked competence and in which it would continually have to revise its judgments.[12] The argument is similar to Kerr's regarding technological invasions of privacy. Justice O'Connor, moreover, also thought that legislative judgment would generally be more appropriate than judicial decisionmaking. Crucially, however, she was not willing (as Kerr is) to defer to state legislatures or Congress in the area of rapidly changing technologies.[13]

I. DOCTRINE

In evaluating Kerr's thesis, let us first consider the doctrinal claim. Kerr says that notions of property rather than privacy have driven the post-*Katz* decisions of the United States Supreme Court.[14] He supports

---

8. *See* MARY ANN GLENDON, ABORTION AND DIVORCE IN WESTERN LAW 42-43 (1987); ELIZABETH MENSCH & ALAN FREEMAN, THE POLITICS OF VIRTUE: IS ABORTION DEBATABLE? 126-27 (1993)Ruth Bader Ginsburg, *Speaking in a Judicial Voice*, 67 N.Y.U. L. REV. 1185, 1208 (1992).

9. *See, e.g.*, GLENDON, *supra* note 8, at 47-50.

10. 462 U.S. 416 (1983).

11. *Id.* at 458 (O'Connor, J., dissenting).

12. But cf. Justice O'Connor's opinion for the Court in *Grutter v. Bollinger*, 539 U.S. 306, 343 (2003), forecasting a twenty-five-year limit to the need for (and therefore, potentially, the constitutional validity of) affirmative action in public higher education.

13. *See Akron*, 462 U.S. at 465. O'Connor stated that:

> [I]n determining whether the State imposes an "undue burden," we must keep in mind that when we are concerned with extremely sensitive issues . . . "the appropriate forum for their resolution in a democracy is the legislature." . . . This does not mean that . . . we defer to the judgments made by state legislatures. . . . Rather, that when we face a complex problem with many hard questions and few easy answers we do well to pay careful attention to how the other branches of Government have addressed the same problem.

Id. (citations omitted).

14. *See* Kerr, *supra* note 1, at 828-30. Kerr asserts that after *Katz v. United States*, 389 U.S. 347 (1967),

this claim by attempting to demonstrate that a large number of the cases supposedly decided under the "reasonable expectation of privacy" framework are in truth more faithful to property law, broadly construed, than they are to privacy. There are a few reasons to question this claim, however, one of which is ultimately a matter of interpreting precedents.

First, in explaining its decisions, the Court refers repeatedly to "reasonable expectations of privacy" rather than to property, in the cases following *Katz*. These references may indeed reflect only some misguided need to profess fidelity to the *Katz* decision (or at least to Justice Harlan's concurring opinion in that case), while in fact pursuing the property-based reasoning that animated the law prior to *Katz*. Certainly, this explanation could provide an account of the failure of the Court's precedents to live up to the promise of *Katz*, a failure that is acknowledged by both supporters of and detractors from the privacy approach.[15]

On the other hand, it seems peculiar that the Court would pursue a property-based approach to the Fourth Amendment, one that it had previously embraced, and simultaneously pay lip service to a privacy-based approach that may — as Kerr suggests[16] — not even be necessary to the *Katz* decision itself. If the Court were truly interested in applying the Fourth Amendment only to property it could easily have said so and thereby pursued its agenda openly.

As Kerr acknowledges, the Court does sometimes decide cases in a manner that seems to reflect its consideration of privacy rather than

---

> These cases suggest that courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies. For better or for worse, courts have tended to apply the same property-based principles to such cases that they have applied elsewhere.

Id. at 829.

15. Both supporters of and detractors from *Katz* have argued that the cases supposedly following *Katz* did not carry out the expected privacy revolution. *See, e.g.*, Kerr, *supra* note 1, at 818 n.99 (citing James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L. J. 645, 647 (1985); Jonathan Todd Laba, Comment, *If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imaging, Emerging Technologies, and the Fourth Amendment*, 84 CAL. L. REV. 1437, 1454 (1996); and Richard S. Julie, Note, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 131 (2000)).

16. *See* Kerr, *supra* note 1, at 819-24. Kerr states that "for my purpose here, the trick is to note that *Katz* is correctly decided from the standpoint of [a] loose property-based approach." *Id.* at 820. Additionally, Kerr argues that attaching things to a person's property (here, the phone booth would be Katz's property for the duration of his telephone call, supported by his payment of the toll) is an invasion of property rights under *Loretto v. Teleprompter Manhattan CATV*, 458 U.S. 419 (1982), which said it was a taking to attach a cable box to a person's roof.

property concerns.[17] As Kerr notes, though, some of the cases protecting (or finding *no* reasonable expectation of) privacy are also equally defensible on property grounds[18] — but this should come as no surprise. There has long been significant overlap between property rights and reasonable expectations of privacy. Privacy is one of the things that people value about private property. We cherish the right to exclude others not only from *using* our privately owned (or rented) spaces, but also from occupying and observing us within our private spaces. For instance, to avoid being observed while engaged in private activities (or to be free of observation even when they have no particular private activity to pursue), people can enter their homes and shut the door. People can hide personal items in their houses or cars or hotel rooms and thereby prevent others from knowing of those items. Protecting property, in other words, has in the past largely encompassed protecting privacy as well, and it is thus misleading to characterize the Fourth Amendment, textually or historically, as relevant to property but not to privacy.

As Kerr shows, however, new technology unmoors privacy from property. Now threats to privacy can arise without in any way implicating rights to private property. Intercepting email communications, utilizing thermal detection devices, and applying my

---

17. *E.g.*, Kyllo v. United States, 533 U.S. 27, 38-40 (2001) (finding that police use of an infrared thermal imager to identify hot spots on the outside surface of a suspect's home was a search for Fourth Amendment purposes, and concluding that "[w]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") United States v. Karo, 468 U.S. 705, 707-17 (1984) (finding a Fourth Amendment violation where police used an electronic tracking device to track a suspected drug conspirator's movement into several private homes, because use of the tracking device gave police access to information that would ordinarily have been concealed inside the privacy of people's homes)United States v. Knotts, 460 U.S. 276, 279-85 (1983) (finding no Fourth Amendment violation where police used an electronic device to track the location of a car owned by a suspected member of a drug conspiracy, because the information exposed was merely the car's location, which could have been obtained entirely through publicly available information, by following the car at a distance). The differing outcomes in *Knotts*, *Karo*, and *Kyllo*, respectively, seem to turn not on any link to physical invasions of property (which both *Knotts* and *Karo* contain and which *Kyllo* does not) but on the extent to which previously hidden and private matters are newly exposed through the use of the particular technology in question.

18. *See* Kerr, *supra* note 1, at 819-24. Kerr argues:

> *Katz* is correctly decided from the standpoint of [a] loose property-based approach . . . . Charles Katz became entitled to Fourth Amendment protection in the public phone booth when he 'pa[id] the toll that permit[ted] him to place a call,' because at that point he became a legitimate user of the phone booth. In effect, Katz rented out the booth for the 'momentary' period of his call much like a hotel guest rents out a hotel room for the night. Like the hotel guest gaining Fourth Amendment rights in the hotel room during his stay, Katz acquired the owner's privacy rights in the phone booth during the period of his phone call.

Id at 820-21. (citations omitted).

hypothetical brain-reader device all share in common the attribute of leaving traditional property rights untouched. No physical trespass need occur. But does that mean that the Fourth Amendment — drafted and ratified in a simpler time, when the overlap between invasions of property and invasions of privacy was more complete — has no bearing on these activities? To the extent that original understanding bears on constitutional law, it is sensible to attribute a concern about privacy to the founding generation and to the text of the Fourth Amendment itself.

In the late eighteenth century, someone who cared deeply about privacy could secure its effective protection by writing an amendment that guaranteed the people a robust right of security in their houses, papers, and effects. Such an amendment would automatically cover privacy interests as well. In a world where privacy and property were so intimately linked, it would have seemed unnecessary to craft a separate protection for privacy per se, particularly when the Fourth Amendment includes a right of security in one's "person" — an extension beyond contemporary notions of property that might have seemed adequate to cover any unusual invasions of privacy that failed to trespass upon real property or personal effects. The right to be secure against unreasonable searches and seizures, in historical context, thus necessarily encompassed privacy.

As the world changed, however, and invasions of privacy without invasions of property became possible and increasingly likely, Fourth Amendment doctrine had to adapt. As no less an originalist than Judge Bork argued in the First Amendment context, "it is the task of the judge in this generation to discern how the framers' values, defined in the context of the world they knew, apply to the world we know."[19]

Accordingly, even on jurisprudentially conservative premises, one can legitimately interpret the Fourth Amendment as protecting privacy independent of property. Though privacy historically received protection primarily through the exercise of property rights, it is inappropriate to assume that only the property rights survive within the Fourth Amendment domain when property and privacy become disconnected from each other — as in the case of technologies that permit invasive long-distance surveillance without physical trespass. Far more plausible is the claim that because property and privacy were (as Kerr implicitly observes) historically tied so closely to one another, it would not have seemed necessary to the framers and ratifiers of the Fourth Amendment to craft a separate amendment to protect the privacy that did not arise from a property right. Instead, the Fourth Amendment, by going to the trouble of explicitly guarding security in

19. Ollman v. Evans, 750 F.2d 970, 995 (D.C. Cir. 1984) (en banc) (Bork, J., concurring).

houses, persons, papers, and effects, would naturally be understood to recognize the value of privacy in all of its incarnations.

Of course, outside of new technologies, it remains the case that one can expect the greatest ability to enjoy privacy and exclude unwanted others in locations that one owns or rents. To the extent that a person does not own or exercise dominion over a place, enjoyment of privacy rights develops by custom and understanding (and law) rather than by a clearly designated and historically entrenched bundle of rights.

Nonetheless, privacy is important and valued, whether within or outside of the property context. That may indeed be what motivated the Supreme Court to hold in *Kyllo*[20] that the use of a thermal detection device to investigate the contents of an individual's home implicates the Fourth Amendment in (more or less) the same way as physically entering the home and looking at its contents would.[21] Rather than demonstrating a misunderstanding of physics, as Kerr suggests,[22] the decision in *Kyllo* instead demonstrates a sophisticated appreciation of how privacy independently contributes to the security of one's house. Through that appreciation, the Court finds that unwanted exposure is as inimical to security when it occurs through thermal detection as it is when police enter one's home to observe what happens inside. Properly understood, *Kyllo* is therefore not an anomaly in its fidelity to privacy nor is it a property decision; rather, *Kyllo* stands out precisely because property and privacy are separated in the case of the technology at issue, and privacy still survives.

Even before the advent of the newest computer technologies, of course, courts on occasion protected privacy in cases where property played little or no role. Examples include the content of telephone conversations in public booths[23] (though Kerr correctly notes the

---

20. *Kyllo*, 533 U.S. at 40.

21. *Id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search — at least where (as here) the technology in question is not in general public use."(internal citations omitted)).

22. *See* Kerr, *supra* note 1, at 833 n.200.

> The difficulty is that under *Kyllo* the frequency of light determines whether it receives Fourth Amendment protection. Light in the visible spectrum does not receive Fourth Amendment protection: looking at an object using human eyes is not search. However, light in the infrared spectrum is protected by the Fourth Amendment, at least when the object emitting the infrared light is a home. From the standpoint of physics, this is something like saying that the government needs a search warrant to look at blue objects but not red objects.

Id.

Rather than show fidelity to traditional property rights, however, as Kerr claims, the *Kyllo* decision represents a refusal to ignore the privacy that once received automatic protection from existing property law but now (due to technological innovation) may be violated without touching existing property entitlements.

23. *See Katz*, 389 U.S. at 351-54.

decline of such spaces with the rise of mobile phones); and the chemical composition of one's urine.[24]

In the past, because privacy tended to correspond most closely with the ability to exclude others physically, it followed that privacy rights would closely track (although not mirror entirely) property rights. Kerr makes an important contribution in showing that interests in privacy and physical rights in property become less tied to each other with the advent of new technologies such as thermal detection devices and the Internet. Two questions arise out of this development, both of which Kerr answers in the negative. First, has the Court's doctrine up until this point indicated that privacy — apart from its incidental connection to property rights — will receive protection under the Fourth Amendment? And second, is it normatively appropriate for the Court to apply Fourth Amendment doctrines to new, developing technologies? Insofar as the first question calls for a descriptive account of the post-*Katz* cases, I respectfully disagree with Kerr's characterization.

Kerr notes that many of the cases following *Katz* reached the same results as those decided prior to *Katz* and that, further, many refer explicitly to such things as the lack of physical trespass or disruption of property to rule out a putative reasonable expectation of privacy.[25] Examples include what I have termed the "pretend friend" line of cases, which permit the government to freely utilize informants

---

24. See Sherry F. Colb, What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 STAN. L. REV. 119, 170 (2002). In that article, I discussed several cases in which the Court considered the Fourth Amendment implications of testing the chemical composition of one's urine. E.g., Ferguson v. City of Charleston, 532 U.S. 67 (2001) (finding that, absent consent, a hospital had violated the Fourth Amendment rights of several of its female patients who had sought obstetrical care, by performing drug tests on those patients in a manner aimed at providing evidence to the police; the Court held that such drug testing constituted a search triggering the application of Fourth Amendment safeguards). But see Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding a public school program that subjected student athletes to random drug tests, where the test results would be maintained confidentially, separate from the student's other records, and released only to school personnel on a "need to know" basis). *See also* Colb, supra note 6, at 1709 (criticizing as counterintuitive the holding and reasoning in Smayda v. United States 352 F.2d 251 (9th Cir. 1965). Colb observes:

> In *Smayda*, the petitioners were convicted of engaging in oral copulation with each other through a hole carved between two stalls within a restroom in Yosemite National Park, in violation of California law. Police [had] . . . arranged for a hole to be cut in the ceiling over each stall, "for purposes of observation." [Many were observed using the restroom stall for various purposes even though [t]he police . . . lacked individualized suspicion prior to any individual bathroom viewing. The Court of Appeals held that there was still no Fourth Amendment violation, reasoning that "when people resort to such a public toilet for criminal purposes, they deliberately take the chance that they may be observed by police officers, and that they are not protected from such observation" — a waiver argument. The court added that, alternatively, no search had occurred, because "these stalls were, in essence, a public place." (citations omitted).

Id.

25. Kerr, *supra* note 1, at 815-25.

wearing wires and recording devices to form relationships with private people, without probable cause, a warrant, or any level of suspicion.[26] Because such practices obviously invade privacy, Kerr argues, it follows that the Court has not truly been interested in protecting privacy that does not happen to intersect with property rights.

I interpret these and other cases differently. First, the use of deception to enter a private home strikes me as directly implicating interests in property as well as privacy, because both are part and parcel of the right to exclude people from one's house. Using deception to do what would otherwise constitute trespass, then, is no more respectful of property rights than using deception to acquire visual and aural access to private areas and conversations is respectful of privacy rights. With respect to both property and privacy, the Court demonstrates an assumption of risk approach — if you trust people, you do so at your own peril — that fails to keep faith with either a property or privacy conception of Fourth Amendment rights.

As I argued in a recent article,[27] this approach (of equating risk of exposure with actual exposure) is inappropriate, because the government has an obligation to act in a normatively appropriate way and thereby to expose people to no greater intrusion than would exist in the world of purely private interactions. In other words, rather than inadvertently but faithfully developing a property-based Fourth Amendment doctrine, the Court has erroneously embraced an improper "move" in sincerely attempting to apply the Fourth Amendment to protect reasonable expectations of privacy. I identify this move as the equation between taking a risk of exposure (however remote in the world of private actors), on the one hand, and acting in a manner that knowingly exposes one's private matters, on the other.[28]

Kerr acknowledges that in some of the case law, including *United States v. Knotts*,[29] *United States v. Karo*,[30] and *Kyllo v. United States*,[31] "the Court has deviated from a strict focus on how the technology works and instead created rules to preserve the degree of surveillance

---

26. *See* Colb, *supra* note 24, at 139-40 (characterizing "pretend friend" cases). Colb characterizes "pretend friend" cases as those in which the government:

> [B]ehaves like an intimate who betrays a friend's trust .... In reviewing challenges to various undercover operations, the Court has held that nothing in the Fourth Amendment prevents a government agent from feigning a relationship with a person and thereby insinuating himself into the person's confidence .... [T]he Court recognizes no reasonable expectation of privacy in one's friends." (citations omitted).

Id.

27. *See id.*

28. *See id.* at 126-27.

29. 460 U.S. 276 (1983).

30. 468 U.S. 705 (1984).

31. 533 U.S. 27 (2001).

authority in the home that property law principles have traditionally allowed."[32] He claims, however, that rather than suggesting a privacy-based Fourth Amendment, "a better reading is that these cases are essentially conservative, based on the primacy of property law to the Fourth Amendment."[33]

Kerr attempts to reconcile *Knotts*, *Karo*, and *Kyllo* with his property-based view of the Fourth Amendment precedents by saying that the Court simply shifts its focus from "*how* the information was obtained — the usual inquiry — [to] *what* information was obtained"[34] in order "to retain the very core of traditional Fourth Amendment protections: the protection of information about the home *traditionally enforced by property law.*"[35] But in observing the shift in focus, from how a surveillance method works to *what* the method exposes, Kerr implicitly acknowledges that the Court in these cases has decided to protect privacy (or, as in one of the cases, to reject a Fourth Amendment claim when privacy is not implicated) regardless of whether the surveillance method *in fact* makes it possible to invade privacy without transgressing any existing property rights. In other words, Kerr's attempt to reconcile these three cases with a view of property as primary fails precisely because privacy could previously have been characterized as only *incidentally* protected by property rights but can no longer be so characterized once it receives protection, even when there is no property trespass involved at all.

Though I take issue with the Court's notion that everyone can already follow a car's whereabouts in public (in the way that a tracking device permits),[36] it is clear that the Court's analysis, however flawed, rests on a conception of privacy from public observation that exists independently of property rights (one of which property rights, as Kerr notes,[37] ordinarily includes an interest in not having things affixed to

32. Kerr, *supra* note 1, at 830.

33. *Id.*

34. *Id.* at 831.

35. *Id.* at 833 (emphasis added).

36. *See* Colb, *supra* note 24, at 132-37. I criticized *Knotts* "because people do not expect to be followed when they move about in public areas," *see id.* at 134, and further faulted the *Knotts/Karo* distinction as failing to correspond to people's actual concerns about privacy from exposure. *Id* at 134-37.

37. *See* Kerr, *supra* note 1, at 821 (citing *Loretto v. Teleprompter Manhattan CATV* 458 U.S. 419, 435-38 (1982), in which the Court found an installation similar to the tape recorder involved in *Katz* to be a direct taking of property, which required just compensation to the owner. In *Loretto*, an apartment building owner protested the state-sanctioned installation on her building of cable television boxes and associated wires. The Court characterized the placement of the boxes as a "permanent physical occupation" of the owner's property. Kerr argues that the same logic applies to *Katz*. In particular, Kerr suggests that in *Katz*, the government installed the device on a property that Katz had rented (i.e., the phone booth), and used information obtained through that invasion of Katz's property to procure damaging evidence against him).

one's property, as the tracking device must be in both *Knotts*, where the Court did not find a violation, and *Karo*, where it did). *Kyllo* is yet another instance in which the usual freedom from public observation that one enjoys inside one's home generates a privacy-regarding ruling regulating the use of heat detection technology to discern goings-on within the house even absent an invasion of a property right. Though Kerr finds the analysis anomalous (mocking, for example, the distinction between visible and invisible light waves),[38] it is entirely in keeping with a Fourth Amendment approach that regards as sacred the individual's right to keep out public observation of her home, i.e., the "privacy" dimension of private property.

In yet another case that implicates privacy but not property, the Court decided implicitly in *Ferguson v. City of Charleston*[39] that informed consent was a necessary precondition, as a matter of Fourth Amendment law, to the legality of testing the chemical composition of a public hospital patient's urine (for cocaine, in this case). Though one does not own the urine that leaves one's body (particularly when one has voluntarily agreed to give doctors a sample), the Court indicated that the privacy of its contents (beyond the facts medically necessary for treating the patient's condition) retains Fourth Amendment protection.

II. NORMATIVE INQUIRY

Normatively, Kerr poses the critical Fourth Amendment question presented by new technologies as involving a choice between judicial protection of privacy and congressional (or state legislative) protection of privacy. Kerr argues that because Congress has so far done a good job of protecting privacy in the area of technology, and because the judiciary has tended to fall behind the curve in protecting privacy (for various institutional reasons), Congress is a sensible repository for our trust in securing privacy, while the judiciary is not.

Yet Kerr offers a false choice between courts and legislatures. Judicial protection of Fourth Amendment privacy from technological intrusion hardly bars similar or additional protection by Congress. In some instances in which the Supreme Court has decided not to protect privacy, Kerr notes that Congress has filled the gap.[40] For example, after the Court ruled that people have no reasonable expectation of

38. *See supra* note 22.

39. 532 U.S. 67 (2001).

40. *See* Kerr, *supra* note 1, at 837 (asserting that "[a]dditional privacy protections are needed to fill the gap between the protections that a reasonable person might want and what the Fourth Amendment actually provides" and that "those protections historically have come from Congress").

privacy in their bank records,[41] Congress enacted the Right to Financial Privacy Act, which imposes Fourth Amendment-like restrictions on government access to such records.[42] To the extent that the Supreme Court or other courts similarly failed to keep up with the times, there would be nothing to stop Congress from doing the same in the area of technology. Having two separate government bodies protecting privacy, moreover, does not create conflict, because the roles of the two branches are distinct from each other. It is the courts' job to interpret the Fourth Amendment right against unreasonable searches and seizures. By contrast, Congress may extend protection beyond that covered by the Constitution as a matter of majoritarian preferences.

To be sure, there would be the potential for conflict if the Court systematically overprotected privacy. In those circumstances, as a matter of constitutional law, Congress could not "correct" the Court's errors through ordinary legislation. Kerr's arguments, however, (which I find persuasive on this point) indicate that where the Court errs it will typically err in underprotecting privacy. In those circumstances, Congress can generally provide supplemental protection without any conflict.

Indeed, because the "reasonable expectation of privacy" test calls for an inquiry about how much privacy people would have in the absence of law enforcement surveillance, Congress can generate new and more protective norms about privacy simply by limiting the amount of exposure that individuals must suffer at the hands of other private parties who have access to technological tools of surveillance. The relationship between the two branches can therefore be complimentary rather than conflicting, and in any event, there is no principle that bars Congress from continuing to protect privacy in the beneficial ways that it has done in the past.

Furthermore, and perhaps more importantly, from a practical perspective, Congress does not (as the Court does under the Fourth and Fourteenth Amendments) have the authority to regulate the behavior of state governments without an affirmative grant of power. The Commerce Clause is one such affirmative grant, but not all state and local threats to privacy would trigger application of the Commerce Clause.[43] Thus the Fourth Amendment (as incorporated through the

41. *See* United States v. Miller, 425 U.S. 435, 440-45 (1976).

42. 12 U.S.C. §§ 3401-3422 (2000).

43. *See* United States v. Morrison, 529 U.S. 598, 619-27 (2000) (holding that neither the Commerce Clause nor the Enforcement Clause of the Fourteenth Amendment provided Congress with the authority to enact the Violence Against Women Act (VAWA)); *see also* United States v. Lopez, 514 U.S. 549, 567-68 (1995) (holding that Congress lacked authority under the Commerce Clause to enact the Gun-Free School Zones Act of 1990, which made the knowing possession of a firearm within a school zone a federal crime).

Fourteenth Amendment) could be a crucial source of authority for congressional privacy legislation.

If the Fourth Amendment in fact protects privacy, then Congress may pass legislation to effectuate that constitutional right under Section Five of the Fourteenth Amendment, even if the legislation goes substantially beyond what the Court says the Fourth Amendment itself requires. If, however, as Kerr claims, the Fourth Amendment does not protect privacy in the area of new technology, then congressional efforts to regulate state invasions of privacy would likely be deemed too distant from any constitutional interest recognized by the Court to count as valid action under the Section Five power.[44]

Kerr is correct to suggest that Congress can achieve a great deal by regulating private actors,[45] such as banks and internet service providers, because they are often the source for law enforcement's acquisition of technologically created private material. Congress can regulate *them* as actors in interstate commerce. But when state police themselves (or, as will increasingly become the case, technologically educated employees who work for the police) invade individuals' privacy in technologically advanced ways, Congress may not have the power to protect privacy from such invasions.

Perhaps most fundamentally, Kerr's argument that Congress alone should be entrusted with protecting privacy because it does a better job than the Court when new technologies are involved is a non sequitur. If in fact the Fourth Amendment provides a constitutional right to privacy, then the Court has an affirmative obligation to apply that right to new contexts, just as it has an obligation to protect the First Amendment or the Fifth Amendment when previously unimagined threats to the rights of free speech or freedom from compelled self-incrimination arise. The Supreme Court and lower federal courts, in other words, are charged with the responsibility of saying what the Constitution means and applying it to factual scenarios presented by litigants. If Congress does a smashing job of

---

44. As the Court's recent decision upholding the Family and Medical Leave Act's application to states demonstrates, there is a crucial doctrinal difference between a federal statute that extends further protection to an interest the Court's doctrine already recognizes as special (such as the interest in avoiding sex discrimination), and a federal statute that purports to "enforce" constitutional rights that the Court says don't exist in the first place. *See* Nevada Dep't of Human Res. v. Hibbs, 538 U.S. 721, 735-36 (2003) (distinguishing cases in which the Court forbade Congress's extension of constitutional protection against discrimination that, under the Court's precedents, would only trigger low-level scrutiny). In other words, Congress's power under the Fourteenth Amendment to "enforce" existing constitutional rights against the states is far broader than its power to protect rights that the Court has said are not found in the Constitution.

45. *See* Kerr, *supra* note 1, at 854-855 (stating, for example, that "Congress enacted the Right to Financial Privacy Act to protect the privacy of bank records" and that "Congress's handiwork in the field of Internet surveillance law offers a promising framework" (citations omitted)).

protecting privacy, then litigants will have recourse to legislative *and* constitutional arguments when they appear in court. But the availability of one kind of protection does not and should not preclude the availability of the other. To refuse to enter into the thicket of Fourth Amendment rights against new technologies, in other words, would be an abdication of the courts' responsibilities.

The real normative and empirical questions, then, are, respectively, whether the Fourth Amendment ought to be read, and whether it has been read, to protect privacy in addition to and independent of any link to property. Kerr answers the latter question in the negative: doctrinally, he argues, the post-*Katz* cases can best be explained as applications of a Fourth Amendment right of property, broadly construed. As I have already explained, this reading of the precedents is strained. The normative question, however, does not necessarily turn on this answer. If, in fact, it is a mistake to apply the Fourth Amendment to privacy, then any doctrinal suggestion to the contrary ought to be rejected for the future, and what better place to do it than a context in which property is no longer at issue?

So we face the normative question: Is it a mistake to protect privacy? Professor William Stuntz has put forward that suggestion.[46] If Stuntz is right that privacy is not valuable, then it makes perfect sense to reject the application of Fourth Amendment law to technology, where only privacy but not property is at issue. But I think Stuntz is wrong,[47] and perhaps more importantly for present purposes, so does Kerr. Kerr clearly does value privacy; he praises rather than laments congressional vigilance in stepping into the void to protect privacy from technological invasion. He apparently views privacy as an important value, but one located primarily outside of the Fourth Amendment.

As I have argued, Kerr's analysis does not support his conclusion. Fourth Amendment doctrine does not purport to protect privacy merely when it is tied to property, but actually, and appropriately (if imperfectly), protects privacy, even from governmental invasions accomplished through new technology when property rights are not directly implicated. Kerr may be correct that Congress is as good as or better than the courts at protecting privacy, but absent some reason to think that the courts will systematically overprotect privacy, the fact that we can generally rely upon the democratic process is no reason to forego the additional protection for individual rights that the judiciary affords for those occasions when majority rule threatens to become majority tyranny.

---

46. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1048 (1995) (arguing that "[i]f we could start over, perhaps privacy would not receive constitutional protection anywhere" (emphasis omitted)).

47. *See* Colb, *supra* note 6, *passim*.