Winter 1-1-2015

Two More Ways Not to Think about Privacy and the Fourth Amendment

David Alan Sklansky
Berkeley Law

Two More Ways Not to Think about Privacy and the Fourth Amendment

David Alan Sklansky†

This Essay challenges two increasingly common ideas about privacy and the Fourth Amendment. The first is that any protections needed against government infringements on privacy in the information age are best developed outside the courts and outside constitutional law. The second is that the various puzzles encountered when thinking about privacy and the Fourth Amendment can be solved or circumvented through some kind of invocation of the past: a focus on the text of the Fourth Amendment; the study of its history; or an effort to preserve the amount of privacy that used to exist, either when the Fourth Amendment was adopted or at some later point.

Fourth Amendment law is famously controversial, but for much of the past half century there was rough consensus about three things: first, the constitutional ban on "unreasonable searches and seizures" is aimed chiefly at protecting privacy; second, courts should take the lead in protecting privacy against new methods of surveillance; and third, the kind of privacy the Fourth Amendment should defend is the kind of privacy needed to keep a modern society free and democratic. That consensus has unraveled, for reasons I explore in a separate article.[1] That article takes issue with two increasingly common ideas about the Fourth Amendment and privacy: that the Fourth Amendment actually should be anchored in concerns other than privacy; and that, to the extent search-and-seizure law remains focused on privacy, privacy should be understood to consist of the ability to control the dissemination and use of information.[2]

Here, I want to challenge two other increasingly common ideas about privacy and the Fourth Amendment. The first is that any protections needed against government infringements

† Professor, Stanford Law School. I thank Orin Kerr, Erin Murphy, and participants at the 2014 University of Chicago Law Review symposium for comments and criticism, as well as Hamilton Jordan Jr and Masao MacMaster for research assistance.

1 David Alan Sklansky, *Too Much Information: How Not to Think about Privacy and the Fourth Amendment*, 102 Cal L Rev 1069 (2014).

2 See id at 1073–74.

on privacy in the information age are best developed outside the courts and outside constitutional law. The second is that the various puzzles encountered when thinking about privacy and the Fourth Amendment can be solved or circumvented through some kind of invocation of the past: a focus on the text of the Fourth Amendment; the study of its history; or an effort to preserve the "degree of privacy against government" that used to exist, either "when the Fourth Amendment was adopted" or at some later point.[3]

Variants of both these ideas have been advanced with particular clarity and influence by Professor Orin Kerr, a scholar I greatly admire. As I will disagree with Kerr frequently in this Essay, I want to make explicit at the outset what should be obvious: I will be singling out Kerr's arguments for criticism not because I think they are especially feeble but, on the contrary, because they constitute unusually thoughtful and fair-minded versions of the positions I want to contest.

I. PRIVACY AND INSTITUTIONAL COMPETENCE

The first idea I want to challenge here—that privacy protections are best developed by the political branches, without reliance on constitutional law—is a reaction against what has often been a myopic focus on constitutional adjudication as the beginning and end of criminal procedure. That tendency was especially strong during the Warren Court era and its aftermath, but it can still be seen today in a good deal of legal scholarship. So it is a healthy correction to draw attention to the ways that legislatures and regulatory agencies guard against invasions of privacy. But the correction can go too far.

In 1995, the Fourth Circuit had to decide whether the Fourth Amendment protected against the interception of radio signals sent out by the handset of a cordless telephone.[4] Using a radio receiver to eavesdrop on a cordless-telephone conversation requires a warrant under the federal wiretapping statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[5] but that requirement was not imposed until 1994.[6] The Fourth Circuit case involved warrantless surveillance carried out before

---

3 *United States v Jones*, 132 S Ct 945, 950 (2012), quoting *Kyllo v United States*, 533 US 27, 34 (2001).

4 See *In re Askin*, 47 F3d 100, 101–02 (4th Cir 1995).

5 Pub L No 90-351, 82 Stat 197, 211–25, codified at 18 USC §§ 2510–20.

6 *Askin*, 47 F3d at 102–03.

then, when Title III expressly did *not* apply to the interception of radio signals transmitted by a cordless telephone.[7] So the case squarely presented the question whether the surveillance counted as a search under the Fourth Amendment and therefore presumptively required a warrant.[8]

There was a decent argument that the Fourth Amendment did not apply. First-generation cordless phones used radio frequencies that could be picked up by an ordinary AM/FM receiver, so perhaps anyone using such a phone lacked a "reasonable expectation of privacy"—the sine qua non for a search under *Katz v United States*.[9] Other courts had deemed cordless-telephone conversations constitutionally unprotected for precisely this reason,[10] and the ease of interception was also why Congress initially directed that eavesdropping on a cordless telephone did not require a Title III warrant.[11] (Congress reversed course in 1994 in part, apparently, because cordless telephones had become harder to intercept, but mainly because the devices had become much more common.)[12] The Fourth Circuit, too, noted how easily calls on early cordless telephones could be monitored, but it did not rely on this consideration alone in denying Fourth Amendment protection to the captured conversations.[13]

Writing for the court, Judge J. Harvie Wilkinson III reasoned that judges should defer heavily to legislators in crafting privacy protections for new communication technologies.[14] Drawing lines in this "fast-developing area," he explained, "requires precisely the type of expertise that courts are institutionally ill-equipped to acquire and to apply."[15] Accordingly, "[a]s new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain

---

7 Id at 103.

8 See id at 105–06.

9 389 US 347, 360 (1967) (Harlan concurring).

10 See, for example, *State v Delaurier*, 488 A2d 688, 694 (RI 1985); *State v Howard*, 679 P2d 197, 198–99, 206 (Kan 1984).

11 See, for example, *Electronic Communications Privacy Act*, S Rep No 99-541, 99th Cong, 2d Sess 12 (1986). See also Adam P. Mastroleo, Note, *Does the Fourth Amendment Protect Cordless Telephone Communications, and If So, When?*, 56 Syracuse L Rev 459, 465 (2006).

12 See Mastroleo, Note, 56 Syracuse L Rev at 466 (cited in note 11).

13 See *Askin*, 47 F3d at 105–06.

14 See id.

15 Id.

with . . . the legislature,"[16] and "courts should be cautious not to wield the amorphous 'reasonable expectation of privacy' standard . . . in a manner that nullifies the balance between privacy rights and law enforcement needs struck by Congress."[17]

A decade later, Professor Kerr picked up and elaborated Judge Wilkinson's argument. For two different reasons, Kerr suggested, legislatures are much better than courts at devising rules for new technologies.[18] First, legislatures have good ways to inform themselves about new technologies; courts do not.[19] Second, statutes can be amended to adapt to new realities or to test alternative regulatory strategies; judicially created rules lack this kind of flexibility.[20] As a consequence, "legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies," and "courts should proceed cautiously and with humility" in this area[21]—just as Wilkinson suggested.

The idea that new technological threats to privacy are best addressed by legislatures rather than by courts recently picked up four new endorsements, from Justices Samuel Alito, Stephen Breyer, Ruth Bader Ginsburg, and Elena Kagan. Concurring separately in *United States v Jones*,[22] the GPS-monitoring case, Alito agreed with Kerr that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative," because "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[23] Alito also endorsed Kerr's suggestion that the history of protections against wiretapping demonstrates the superiority of legislatures in crafting privacy protections for new technologies.[24] And two years later, when the Court ruled in *Riley v California*[25] that the police generally need a warrant to search an arrestee's

---

16 Id at 106.

17 *Askin*, 47 F 3d at 105–06.

18 See Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich L Rev 801, 858–59 (2004).

19 See id at 875–76, 881–82.

20 See id at 871.

21 Id at 859.

22 132 S Ct 945 (2012).

23 Id at 964 (Alito concurring), citing Kerr, 102 Mich L Rev at 805–06 (cited in note 18).

24 See *Jones*, 132 S Ct at 964 (Alito concurring).

25 134 S Ct 2473 (2014).

cell phone,[26] Alito again concurred separately (this time by himself) and suggested that cell phone searches, too, are an issue that legislatures are better suited to address.[27] Wilkinson's suggestion has become a full-fledged meme, and it may be approaching the status of conventional wisdom.

It is far from clear, though, that legislatures really are better than courts at fashioning privacy rules for new technologies—or even that this is a sensible comparison to draw. Legislatures have advantages over courts, but it works the other way too. True, legislative hearings take a broader, more systemic view than hearings in a court case.[28] Judicial hearings are by their nature adversarial, though, which assures at least some representation for both sides, whereas legislative hearings on privacy issues in criminal investigations can easily be dominated by law enforcement interests. And while statutes theoretically can be revised at any time, without waiting for the proper case to arise and without regard for precedent, in practice Congress is often notoriously sluggish. The case-by-case method of decisionmaking can prompt reconsideration of rules that legislatures would never get around to amending.[29] Surveying the regulation of law enforcement practices by federal statutes, Professor Erin Murphy finds: (1) "Congress does less leading and much more following when it comes to regulating privacy";[30] (2) "law enforcement . . . plays a critical role in shaping" statutory protections of privacy through its "clear and constant voice in the political process";[31] and (3) while privacy statutes are sometimes amended, Congress often has proven unwilling or unable

---

26 Id at 2493.

27 See id at 2497–98 (Alito concurring).

28 See Kerr, 102 Mich L Rev at 875 (cited in note 11).

29 See Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* 165–67 (Yale 2011). Professor Daniel Solove concludes that, "[i]f anything, the historical record suggests that Congress is actually far worse than the courts in reacting to new technologies." Id at 167. He explains:

> Federal legislation is not easy to pass, and it usually takes a dramatic event to spark interest in creating or updating a law. In contrast, courts must get involved every time an issue arises in a case. As a result, issues are likely to be addressed with more frequency in the courts than in Congress.

Id.

30 Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich L Rev 485, 498 (2013).

31 Id at 503, 535.

to correct "obviously flawed and outdated provisions."[32] In fact, Murphy concludes, many of the most successful privacy statutes have stayed current "largely because of vague terms that can be adapted by judicial officials to apply to changed circumstances."[33]

Generalizing from this last observation, Murphy suggests that neither Congress nor the courts should "assume sole or even primary responsibility for regulating privacy."[34] Instead, she suggests that sensible protections for privacy are most likely to emerge from a collaborative process of "interbranch dialogue."[35] As Murphy points out, the rules regulating wiretapping emerged from precisely that kind of process.[36] In the 1920s, wiretapping was statutorily prohibited in many states and banned as a matter of policy by federal investigative agencies, but after the Supreme Court concluded that the Constitution permitted the use of wiretap evidence in criminal prosecutions,[37] the Prohibition Bureau openly embraced the practice.[38] The Court slowly backtracked, first by creatively reading a ban on wiretap evidence into a federal statute that in fact said nothing about the admissibility of intercepted conversations,[39] and then—when Congress did not cry foul—by narrowing the scope of the earlier constitutional holding.[40] Eventually, the Court struck a compromise: electronic eavesdropping was constitutionally permissible, but only with a warrant based on a showing of probable cause.[41] That compromise followed the pattern set by many state statutes,[42] and it triggered, in turn, federal legislation along the same lines.[43] Congress later extended the scope of

---

32 Id at 533.

33 Id at 533–34. See also id at 536.

34 Murphy, 111 Mich L Rev at 537 (cited in note 30).

35 Id at 538.

36 See id at 493–94, 538. See also David Alan Sklansky, *Killer Seatbelts and Criminal Procedure*, 119 Harv L Rev F 56, 59–60 (2006).

37 See *Olmstead v United States*, 277 US 438, 465–67, 469 (1928).

38 See Walter F. Murphy, *Wiretapping on Trial: A Case Study in the Judicial Process* 13, 125–29 (Random House 1965).

39 See *Nardone v United States*, 302 US 379, 381–83 (1937). See also *Nardone v United States*, 308 US 338, 339 (1939).

40 See *Silverman v United States*, 365 US 505, 507–09 (1961).

41 *Katz*, 389 US at 358–59.

42 See Kerr, 102 Mich L Rev at 846 (cited in note 18) (indicating that, by 1967, "[t]hirty-six states had banned wiretapping" and "twenty-seven [states] allowed some type of 'authorized'" wiretapping).

43 See Omnibus Crime Control and Safe Streets Act, 82 Stat at 211–25, codified at 18 USC §§ 2510–20.

the Court's compromise, requiring warrants for foreign-intelligence wiretaps of US citizens[44] and, eventually, for interception of calls made on cordless telephones.[45] This history does not demonstrate, as Alito has claimed, that "the regulation of wiretapping was a matter better left for Congress."[46] Instead, it suggests that legal restrictions on wiretapping benefited from the participation of both courts and legislatures.[47]

It is therefore to Alito's credit that he has recognized, ultimately, that courts do have a role to play in regulating privacy threats from new technologies, at least when legislatures fail to act. In *Jones*, for example, Alito concluded that, since "Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes," the Court had little choice but "to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[48] In *Riley*, Alito suggested he would defer to a "reasonable" legislative balancing of law enforcement interests and the privacy interests of cell phone owners, but since legislators had not acted, he joined the Court in requiring a warrant before a cell phone was searched incident to an arrest.[49]

Kerr takes a harder line. He argues that courts should not just defer to legislative determinations about the best way to protect privacy from new technologies; even when legislatures have *not* acted, Kerr suggests that courts should hesitate to step in for fear of taking the wind out of the legislature's sails. "The absence of judicial regulation invites legislative action," he explains.[50] Conversely, judicial efforts to protect privacy can

---

44 See Foreign Intelligence Surveillance Act of 1978 (FISA), Pub L No 95-511, 92 Stat 1783, 1787, codified at 50 USC § 1802(b).

45 See Communications Assistance for Law Enforcement Act (CALEA) § 202, Pub L No 103-414, 108 Stat 4279, 4290–91 (1994), codified at 18 USC §§ 2510–11.

46 *Jones*, 132 S Ct at 963 (Alito concurring). See also *Riley*, 134 S Ct at 2497 (Alito concurring) (suggesting that "electronic surveillance has been governed primarily" by federal legislation rather than by the Supreme Court).

47 Much of this paragraph is adapted from Sklansky, 119 Harv L Rev F at 60 (cited in note 36).

48 *Jones*, 132 S Ct at 964 (Alito concurring).

49 *Riley*, 134 S Ct at 2497 (Alito concurring).

50 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich L Rev 311, 350 (2012).

"discourage legislative action by fostering a sense that the courts have occupied the field."[51]

Is judicial restraint the best way to encourage legislative action to protect privacy? It's a plausible claim,[52] but the evidence is thin. We lack good examples of Congress stepping in to regulate a technological threat to privacy that the Court has left entirely unaddressed.[53] Wiretapping is not an example of that, as Murphy explains.[54] Searching for another example, Kerr and others have pointed at times to the statutory regulation of pen registers.[55] But the pen register statute turns out to be a case study in the *hazards* of leaving privacy protection to Congress.

A pen register records the numbers called from a particular telephone line. It is the opposite of a "trap-and-trace device," which records the numbers associated with incoming calls. Federal law prohibits installing or using a pen register or trap-and-trace device without a court order.[56] As Kerr points out, this

---

51 Id.

52 See David A. Sklansky, *Proposition 187 and the Ghost of James Bradley Thayer*, 17 Chicano-Latino L Rev 24, 31–32 (1995).

53 Nor, for that matter, are there good examples of legislatures stepping in to regulate *non*technological threats to privacy about which constitutional law is largely silent—the use of confidential informants, for example.

54 See Murphy, 111 Mich L Rev at 538–39 (cited in note 30).

55 See, for example, Kerr, 102 Mich L Rev at 855 & 886 n 509 (cited in note 18); Kerr, 111 Mich L Rev at 350–51 (cited in note 50); Jen Manso, *Cell-Site Location Data and the Right to Privacy*, 27 Syracuse J Sci & Tech L 1, 21 n 102 (2012); Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 Touro L Rev 93, 133 (2007). Kerr also cites federal statutes protecting, for example, the privacy of bank records and journalists' records. See Kerr, 111 Mich L Rev at 350 (cited in note 50); Kerr, 102 Mich L Rev at 856 (cited in note 18). But these are not examples of Congress regulating new technological threats left unaddressed by the courts. They are better described as gap-filling measures that provide heightened protection for particular categories of information. The protections provided to e-mail and other stored electronic communications may be better examples of Congress acting without judicial prodding to protect against new technological threats to privacy. See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208, 1209–18 (2004). But those protections were enacted against the backdrop of *Katz*'s broad principle that the Fourth Amendment protects "reasonable expectations of privacy" in telecommunications, and even then they likely would not have been adopted without industry pressure. See *Electronic Communications Privacy Act, Hearings on HR 3378 before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary*, 99th Cong, 1st Sess 2 (1985) (statement of Representative Robert Kastenmeier). Moreover, as Kerr points out, although the statutory protections for stored electronic communications are now "widely perceived as outdated," the revisions that Congress has so far considered "mostly nibble at the edges." Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U Pa L Rev 373, 375 (2014). See also id at 386 ("[I]t has become commonplace to recognize that ECPA is outdated.").

56 18 USC § 3121(a).

prohibition is entirely statutory, and it was enacted after the Supreme Court held that pen registers and trap-and-trace devices are unregulated by the Fourth Amendment.[57]

The pen register statute is also notoriously undemanding. All that a prosecutor needs to do to secure judicial authorization for a pen register or trap-and-trace device is to certify "that the information likely to be obtained is relevant to an ongoing criminal investigation."[58] No proof or explanation is needed, just the government's say-so. And once the certification is made, issuance of the order is automatic; the court has no discretion to deny the application.[59] This doesn't sound like a regime aimed at protecting privacy. It sounds like a regime designed to get the government the information it wants while giving legal cover to telecommunication companies.

And, in fact, the legislative history of the pen register statute makes clear that it had precisely this purpose. The Supreme Court's pen register case, *Smith v Maryland*,[60] was decided in 1979. Later the same year, at least two bills were introduced to bring pen registers within the ambit of Title III—that is, to require the same kind of warrants for pen registers that were needed for wiretaps.[61] Neither bill went anywhere. Early the next year, legislation was introduced to condition the use of pen registers and trap-and-trace devices on a judicial finding of "reasonable cause" that the proposed surveillance would uncover evidence of criminal activity.[62] This bill, too, went nowhere. Other bills were introduced over the following years to regulate pen registers and trap-and-trace devices.[63] All foundered.

---

57 See *Smith v Maryland*, 442 US 735, 742, 746 (1979).

58 18 USC § 3122(b)(2). The certification can also come from a state law-enforcement officer. 18 USC § 3122(a)(2).

59 18 USC § 3123(a)(1)–(2).

60 442 US 735 (1979).

61 See S 1207, 96th Cong, 1st Sess, in 125 Cong Rec 22668 (Aug 3, 1979) (statement of Senator Carl Levin); HR 5285, 96th Cong, 1st Sess, in 125 Cong Rec 25955 (Sept 24, 1979) (statement of Representative Robert Drinan).

62 See HR 933, 97th Cong, 1st Sess, in 127 Cong Rec 514, 518 (Jan 19, 1981) (statement of Representative Ted Weiss). Alternatively, the bill provided that telephone-toll records could be accessed by subpoena, but if they were then the telephone customer would need to be notified and given an opportunity to challenge the request in court. See id.

63 See, for example, *Criminal Code Revision Act of 1981*, HR 1647, 97th Cong, 1st Sess 297–98 (Feb 4, 1981) (barring installation or use of a pen register without a judicial finding of "reason for the belief" that the information obtained would be "relevant to a legitimate criminal or civil investigation"); *Electronic Surveillance Act of 1984*, HR 6343, 98th Cong, 2d Sess 5–6 (Oct 1, 1984).

Nonetheless, federal prosecutors routinely obtained court orders when asking the telephone company (or, after 1982, any of the new telephone companies) to provide records of outgoing or incoming calls. The government followed this practice because telephone companies wanted the legal protection provided by a court order. As a telephone-company lawyer later recalled:

> After *Smith v. Maryland* was decided, the question was graciously raised by law enforcement, would we be interested in cooperating in Pen Register situations without a court order. And our answer was no. And we do request a court order for that, even though it may be legally permissible to voluntarily undertake rendering such assistance.[64]

A federal magistrate judge familiar with these orders explained in congressional testimony that they were "intended simply to protect the telephone company and to enable the Government authorities to obtain the assistance of the phone company."[65]

In 1985, when the Electronic Communications Privacy Act[66] (ECPA) was first introduced,[67] it conditioned the use of pen registers and trap-and-trace devices on judicial findings of "reasonable cause," the same standard that had been proposed unsuccessfully in 1979.[68] Federal prosecutors objected strongly to this proposal, arguing that it would "severely limit the effectiveness of pen registers" and "create serious problems for law enforcement."[69] All that should be required for a pen register, the DOJ explained, is a prosecutor's representation that the information

---

64 *Hearing on Privacy in Electronic Communications before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary*, 98th Cong, 2d Sess 12 (1984) ("1984 Privacy Hearings") (statement of H.W. William Caming, Senior Counsel, AT&T). The successor companies to AT&T apparently followed the same policy. See id.

65 *1984: Civil Liberties and the National Security State, Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary*, 98th Cong, 2d Sess 150 (1984) (testimony of US Magistrate Judge James Carr).

66 Electronic Communications Privacy Act of 1986, Pub L No 99-508, 100 Stat 1848, codified in various sections of Title 18.

67 *Electronic Communication Privacy, Hearing on S 1667 before the Subcommittee on Patents, Copyrights and Trademarks of the Committee on the Judiciary*, 99th Cong, 1st Sess 4–31 (Nov 13, 1985) ("ECP Hearing").

68 See text accompanying note 61.

69 ECP Hearing at 46–47 (statement of Deputy Assistant Attorney General James Knapp). See also, for example, Letter from Mary C. Lawton, Counsel for Intelligence Policy, US DOJ (May 20, 1985), in *Electronic Communications Privacy Act, Hearings on HR 3378 before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Judiciary Committee*, 99th Cong, 1st & 2d Sess 484, 494.

obtained would be relevant to a criminal investigation.[70] The bill was amended in accordance with the DOJ's wishes.[71] Enacted in 1986, ECPA simply codified the preexisting practices that federal prosecutors had worked out with the telecommunications industry. The statute authorized—and in fact required—the issuance of a pen register or trap-and-trace order based solely on a prosecutor's assertion that the requested surveillance would be "relevant to an ongoing criminal investigation"—the key statutory language that has persisted to this day.[72]

The result of leaving regulation of pen registers and trap-and-trace records to Congress has not been just that these tools have gone essentially unregulated. The statutory treatment of pen registers has served as a model for the statutory treatment of metadata surveillance—for example, the collection and monitoring of routing information in e-mails and text messages, and the wholesale archiving of the kind of telephone records that pen registers and trap-and-trace devices previously collected much more selectively. Metadata surveillance has expanded explosively over the past two decades, with only weak restrictions.[73] If *Smith* invited legislative action, it is not an invitation that generated a meaningful response.

II. PRIVACY AND THE PAST

The other idea I want to challenge here is that the privacy protected by the Fourth Amendment can best be gauged by an appeal to the past: to the language of the Amendment, to its history, or—a suggestion made with increasing frequency—to the amount of privacy people used to have. Each of these approaches promises to make search-and-seizure law more determinate and less dependent on judicial whim. They have the additional attraction, for scholars, of giving central importance to something enjoyable to research. But they are blind alleys.

The opening clause of the Fourth Amendment could hardly be more open-ended. It protects "[t]he right of the people to be

---

[70] See ECP Hearing, 99th Cong, 1st Sess at 58 (cited in note 69) (prepared statement of Deputy Assistant Attorney General James Knapp).

[71] See *Electronic Communications Privacy Act of 1986*, HR Rep No 99-647, 99th Cong, 2d Sess 30–31 (1986).

[72] Electronic Communications Privacy Act of 1986 § 3122(b)(2), Pub L No 99-508, 100 Stat 1869, codified at 18 USC § 3122(b)(2).

[73] See, for example, Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 Harv L Rev 691, 697–98 (2014).

secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[74] One can perhaps extract from this language the traditional rule exempting searches of open fields from constitutional protection,[75] but not much else. The second clause of the Fourth Amendment bans general warrants, and the first clause *could* be read simply as a roundabout way of saying what the second clause says explicitly,[76] but that is a strained interpretation.[77] Alternatively, the phrase "unreasonable searches and seizures" could be read as a term of art for searches prohibited at common law, but that, too, is an awkward reading with little to recommend it.[78] By far the most straightforward interpretation of the Fourth Amendment is: don't search or seize people, their homes, their writings, or their stuff in ways that are excessive or unjustified, and in particular don't issue any general warrants.[79]

That interpretation poses a challenge, though, which is to figure out what makes a search or seizure excessive or unjustified. One possible approach is to try to determine what kinds of searches and seizures were thought "unreasonable" by some group of people associated with the adoption of the Fourth Amendment: its drafters or its advocates or the people who voted for it.[80] The problems with this approach (aside from deciding whose views should count) are well-known, although they bear repeating. First, the search-and-seizure practices that generate controversy today usually lack any close parallels in the late eighteenth century, not just because technology has advanced but because institutional and social contexts have changed too. The Framers didn't know about GPS, obviously, but neither were they familiar with modern police departments,[81] let alone the NSA or "crimmigration." Second, it's not clear why we

---

74 US Const Amend IV.

75 See *Oliver v United States*, 466 US 170, 181–84 (1984); *Hester v United States*, 265 US 57, 59 (1924).

76 See Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich L Rev 547, 692–93, 736 (1999).

77 See David A. Sklansky, *The Fourth Amendment and Common Law*, 100 Colum L Rev 1739, 1779 n 248 (2000).

78 For an extended argument, see id at 1774–1813.

79 Regarding the meaning of the term "unreasonable" in the late eighteenth century, see id at 1780–81.

80 See, for example, Davies, 98 Mich L Rev at 693–724 (cited in note 76).

81 See Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850–1940*, 62 Rutgers L Rev 447, 449–59 (2010); Carol S. Steiker, *Second Thoughts about First Principles*, 107 Harv L Rev 820, 830–38 (1994).

should feel bound by eighteenth-century judgments about which particular searches and seizures are unreasonable,[82] or even whether that is what the Framers or adopters of the Fourth Amendment would have wanted or anticipated.[83]

Partly to avoid these difficulties, a different way is sometimes suggested to anchor the Fourth Amendment in the past. Instead of banning particular practices that were thought unreasonable in the eighteenth century, the Fourth Amendment could be read to require preservation of the level of privacy people had when the Bill of Rights was adopted, or perhaps at some other time. Once again, Professor Kerr has given this suggestion a particularly thoughtful articulation. "When new tools and new practices threaten to expand or contract police power," he suggests, courts can and do "adjust the level of Fourth Amendment protection to try to restore the prior equilibrium . . . of privacy protection"[84] and "maintain a balance of police power over time."[85] But the idea neither started nor ended with Kerr, as he would be the first to acknowledge: his account is explicitly descriptive as well as normative. Kerr's "equilibrium-adjustment theory" is essentially a generalized version of what Professor Geoffrey Stone called, forty years ago, "the principle of conservation of privacy."[86] The idea, Stone explained, is that "we strive to maintain a cumulative level of privacy comparable to that existing at the time the [Fourth Amendment] was drafted."[87] Stone's principle has since been explicitly adopted by the Supreme Court, which committed itself, at least twice in recent years, to "assur[ing] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[88]

---

82 See Christopher Slobogin, *An Original Take on Originalism*, 125 Harv L Rev F 14, 18–21 (2011).

83 See Paul Brest, *The Misconceived Quest for the Original Understanding*, 60 BU L Rev 204, 216–17 (1980); Mark D. Greenberg and Harry Litman, *The Meaning of Original Meaning*, 86 Georgetown L J 569, 584–86 (1998); Sklansky, 100 Colum L Rev at 1791 (cited in note 77).

84 Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv L Rev 476, 480 (2011).

85 Id at 527. See also Kerr, 111 Mich L Rev at 352–53 (cited in note 50).

86 Geoffrey R. Stone, *The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers*, 1976 Am Bar Found Rsrch J 1193, 1216 (1976).

87 Id.

88 *Jones*, 133 S Ct at 950, quoting *Kyllo*, 533 US at 34.

Unlike Stone and unlike the Court, Kerr argues that "Year Zero" need not be 1791.[89] But there is no other obvious reference point.[90] And regardless of the starting date, the basic appeal of this approach remains the same. It avoids the circularity of defining "reasonable expectations of privacy" by reference to the limits that courts and legislatures place on surveillance, and it skirts the slippery slope of allowing "reasonable expectations of privacy" to depend on what people actually have come to expect. A preexisting balance is fixed and objective. You can hold onto it.[91] "Equilibrium adjustment" therefore can appeal even to people who think privacy is the wrong hook for the Fourth Amendment. Professor Paul Ohm, for example, thinks search-and-seizure law needs to adapt to a "world without privacy."[92] Borrowing from Kerr, though, he proposes that, as technology advances, courts should continually adjust Fourth Amendment burdens on law enforcement, sometimes tightening them and sometimes loosening them, in order "to preserve a level playing field between the police and criminals."[93]

The argument against this kind of approach to the Fourth Amendment can be simply stated. It is the same objection, more or less, that can be raised about originalism. First, other than determinacy, it has little to recommend it. And second, it doesn't offer much in the way of determinacy.

To begin with, why would anyone want to "maintain a balance of police power" or "preserve a level playing field between the police and criminals"? The police and criminals are not

---

89 Orin S. Kerr, *Defending Equilibrium-Adjustment*, 125 Harv L Rev F 84, 85–86 (2011). Kerr takes pains to make clear that he is not an originalist. He explains that "[e]quilibrium-adjustment . . . is a theory of maintaining the status quo balance of power, not an effort to restore eighteenth-century rules." Id at 84.

90 Kerr argues that the reference point can be any date before the technological development that has required recalibrating privacy rules. See id at 85. He also has explained to me that he believes that equilibrium adjustment aims to restore the balance struck by a particular rule, not the level of privacy in a particular era. But if we are trying to devise rules for, say, searches of e-mail, it isn't clear why the goal should be to restore the level of privacy that happened to exist just before e-mail was invented, or the balance struck by a particular, pre–e-mail statute. Unless, that is, we think that, through a long series of recalibrations, we can trace that level of privacy or that particular balance back to something that existed at the time the Constitution was adopted—or to some other set of arrangements with constitutional stature.

91 See Kerr, 125 Harv L Rev at 526 (cited in note 84) (arguing that "equilibrium-adjustment maximizes legal stability").

92 Paul Ohm, *The Fourth Amendment in a World without Privacy*, 81 Miss L J 1309, 1320 (2012).

93 Id at 1312.

athletic teams, or separate branches of government that we hope will keep each other in check. It is not as though there was some Goldilocks Era when we had just the right amount of crime. It may seem more plausible to say that there was a time when a particularly attractive balance—or a balance endorsed by the Constitution—was struck between the interests of law enforcement on the one hand and the interests of privacy and liberty on the other. Maybe, in fact, that is how the drafters and adopters of the Fourth Amendment thought about their own time—minus, of course, general warrants and writs of assistance.

Maybe, but there is little evidence of it. It is hard to find anyone in the eighteenth century singing praises to the exquisite balance the common law had struck between privacy and law enforcement. The revolutionary generation often spoke reverentially of the common law, but not in *that* manner. They extolled the *protections* of the common law, not the compromises that it struck or the social conditions that it fostered.[94] There is scant reason to think that the Fourth Amendment was intended or originally understood to be a coded instruction to preserve eighteenth-century levels of privacy, or—even less plausibly—the eighteenth-century balance of power between criminals and the forces of the state. Nor does that seem an attractive goal to constitutionalize.

The only reason why it *might* be attractive has to do with determinacy. Even if there is nothing especially wonderful about the eighteenth-century balance between privacy and the interests of law enforcement, perhaps it gives us something to hold on to—something that will help us avoid making constitutional protections dependent on what judges happen to find unreasonable, and that will help us to ensure that Fourth Amendment protections do not dwindle as people come to expect less privacy.

But it doesn't, really. The degree of privacy against government that existed when the Fourth Amendment was adopted—or at some other point in the past—sounds fixed and objective, but on closer inspection it proves wildly indeterminate. The problem is that privacy is neither unidimensional nor evenly distributed. There are different kinds of privacy, and different people possess each to different degrees. It is close to meaningless to refer to the "amount," "degree," or "level" of privacy that existed in 1791 without specifying what is meant by "privacy"

94 See Sklansky, 100 Colum L Rev at 1784–93 (cited in note 77).

and whose privacy is at issue. (To avoid complications, I will focus in the argument that follows on the particular version of "equilibrium adjustment" endorsed by the Supreme Court: maintaining the level of privacy from state intrusions that existed in 1791. But the basic problems of indeterminacy would remain the same if a different "Year Zero" were selected, or if we sought to preserve a "balance of police power" rather than a level of privacy.)

To preserve the amount of privacy people had in 1791, we would need to know what privacy is, or at least roughly how to measure it. It is a commonplace of modern privacy scholarship, though, that "[t]here is no such thing as privacy *as such*";[95] rather, privacy is "a plurality of different things,"[96] lacking any "'essential' or 'core' characteristics."[97] I find that unconvincing, but I am in the minority, and even in my view there are at least two competing conceptions of privacy: a dominant conception of privacy as control over the dissemination and use of personal information, and a different understanding, which I favor, that privacy has to do with respect for a zone of personal refuge.[98] Nor would choosing one of these two views end the difficulty, because infringements on an individual's right to informational control are not all mutually commensurable, and neither are violations of a person's zone of refuge. So figuring out whether we have the same level of privacy today as in the past is not just difficult; it is impossible. The inquiry is incoherent.

Try comparing, for example, the amount of privacy today with the amount in 1791. And to keep things simple, focus for the moment just on the privacy of communications. There were no telephones or computers back then, so no one was susceptible to wiretapping or e-mail monitoring. And there were no electronic listening devices, either, so if you were alone with someone in your home or in the secluded corner of a public house, you could be pretty sure no one would overhear your conversation. There were no video cameras, and telescopes were bulkier and less

---

95 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 Yale L J 1151, 1221 (2004).

96 Solove, *Nothing to Hide* at 24 (cited in note 29).

97 Daniel J. Solove, *Understanding Privacy* 8 (Harvard 2008). See also Peter Galison and Martha Minow, *Our Privacy, Ourselves in the Age of Technological Intrusions*, in Richard Ashby Wilson, ed, *Human Rights in the 'War on Terror'* 258, 269 (Cambridge 2005) (describing "privacy" as a term that "evokes a cluster of ideas, rather than a sharply chiseled concept").

98 See Sklansky, 102 Cal L Rev at 1078–79, 1113 (cited in note 1).

powerful, so with some care you might be able to know that no one was watching you, either. On the other hand, precisely because communication technologies were so primitive, there was no way to speak with anyone without seeing them face-to-face, and for many people, much of the time, visits of this kind were difficult to keep secret, especially in communities where people knew their neighbors. Nor was it always possible to find places to speak without being overheard. Not every pub had a secluded corner, and not every person had a spacious home. Telecommunications have opened up new modes of surveillance, but they have also created new possibilities for discreet interactions. The same has been true, more recently, of social media, which, despite their "public" nature, allow adolescents "a measure of privacy and autonomy that is not possible at home where parents and siblings are often listening in."[99] Even if we focus just on privacy from the government, it is not clear whether teenagers, say, have more or less of it because of social media. Yes, the police can search online records, but they can question parents and siblings, too, and in some ways that can feel more intrusive. So is there more privacy today than in 1791, less, or about the same? It depends how you think about it. And that is without even considering the privacy of matters other than interpersonal communications: the privacy of one's medical condition, say, or the range of intimate behavior that is considered no one else's business.

What makes things still more complicated is that privacy is distributed unevenly, and any particular kind of intrusion is likely to matter more to some people than to others.[100] Searches of homes are of greatest concern to people with homes that are large, comfortable, uncrowded, and free of domestic violence; other people tend to carry out less of their lives at home. Searches of cars disproportionately impact people who drive a lot and people who use their cars for storage. Monitoring of online activity affects people more if they use computers or smartphones heavily, especially if they live with their parents. Street searches are a particular concern for young men of color, because the police stop-and-frisk them so often. Airport searches matter mostly to people who fly, and especially to people—like men of

---

[99] Danah Boyd, *It's Complicated: The Social Lives of Networked Teens* 19 (Yale 2014).

[100] See William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 Geo Wash L Rev 1265, 1272 (1999).

Middle Eastern extraction—who are disproportionately the objects of DHS suspicion.[101]

If anything, privacy was even less evenly distributed in the late eighteenth century, which makes it especially hard and especially senseless to try to preserve the level of privacy that existed when the Fourth Amendment was adopted. There was a highly pronounced class tilt to common-law protections against search and seizure. Justice Antonin Scalia has sometimes suggested that a search or seizure should be deemed unconstitutional if "the fiercely proud men who adopted our Fourth Amendment" would not have "allowed themselves to be subjected" to it.[102] But it is difficult to identify *any* kind of government search or seizure to which those "fiercely proud men" willingly would have submitted. Searches and seizures of the poor and the landless, on the other hand, were subject to far fewer restrictions than today.[103]

The revolutionaries objected to searches of *their* homes and *their* persons in part precisely because those searches seemed to them to violate the protocols of class; they complained that the customs officers who invaded their houses were "dirty," "insolent," "impertinent," and "rude."[104] In this regard, as in others, Americans echoed the protests in England against the general warrants executed against John Wilkes and other government critics. On both sides of the Atlantic, the propertied spokesmen for the sanctity of the home had nothing to say about searches and seizures carried out by constables and watchmen—local officials more likely to defer to the gentry, and whose statutory responsibilities, in any event, turned their attention elsewhere.[105] The class bias inherent in the unrestricted arrests of "nightwalkers"[106] typified the eighteenth-century law of search and seizure; the wealthy had little occasion to walk public roads after dark. Sir Edward Coke had warned in the seventeenth century that searches allowed against "poore and base people"

---

101 See generally Ellen Baker, Comment, *Flying While Arab—Racial Profiling and Air Travel Security*, 67 J Air L & Comm 1375 (2002).

102 *Minnesota v Dickerson*, 508 US 366, 381 (1993) (Scalia concurring).

103 See Sklansky, 100 Colum L Rev at 1805–06 (cited in note 77).

104 Id at 1805. See also Davies, 98 Mich L Rev at 577–78 (cited in note 76). The remainder of this paragraph is adapted from Sklansky, 100 Colum L Rev at 1805–06 (cited in note 77).

105 See generally William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning, 602–1791* (Oxford 2009).

106 See Sklansky, 100 Colum L Rev at 1805 (cited in note 77).

might later be exercised against others,[107] but his worry was not widely shared: "English law aimed less at abolishing discretionary intrusions than at confining them within certain social and occupational boundaries."[108] Peers and members of Parliament received special protections against search and seizure, while the homes of the poor were freely inspected for vagrants, poached game, and morals violations.[109] Colonial statutes followed the same pattern and added, in the South, the innovation of the slave patrol: military squads that, operating largely at night, rounded up drifters and ransacked "Negro Houses" and other dwellings that might harbor or provide arms to escaped slaves.[110]

So urging preservation of the amount of privacy that existed in 1791 is doubly ambiguous: privacy is multidimensional, and it is unevenly distributed. Asking whether there is more or less privacy today than in 1791 is close to meaningless without specifying *whose* privacy and what *kind*. And it is hard to see how either of those questions can be answered without some underlying ideas about why privacy is valued and, more specifically, why the Constitution protects privacy. For Fourth Amendment law, the question is how infringements on privacy can make a search or seizure "unreasonable." To decide that, we need a sense of what privacy means and why it matters.

* * *

Each of the ideas I have challenged here—the belief that privacy threats from new technologies are best regulated by legislatures, with minimal judicial involvement, and the notion that the interpretation of the Fourth Amendment should be anchored in the past—can be understood, in part, as an effort to keep courts from having to decide what privacy consists of, why it deserves protection, and how it is threatened. I have my own

---

107 Edward Coke, *The Fourth Part of the Institutes of the Law of England* 177 (Clarke 1817).

108 William Cuddihy and B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 Wm & Mary Q 371, 380 (1980).

109 See id; Cuddihy, *The Fourth Amendment* at 149–50, 164–65 (cited in note 105).

110 See generally Sally E. Hadden, *Slave Patrols: Law and Violence in Virginia and the Carolinas* (Harvard 2001). See also Leonard W. Levy, *Original Intent and the Framers' Constitution* 240 (Macmillan 1988); Cuddihy and Hardy, 37 Wm & Mary Q at 390 (cited in note 108).

ideas about how to answer those questions,[111] but the point I want to make here is in a way more basic; it is that the questions cannot conscientiously be avoided.

[111] See Sklansky, 104 Cal L Rev at 1102–21 (cited in note 1).