Articles

Standing Up for Mr. Nesbitt

By Stephen Wm. Smith*

MR. NESBITT OF HARLOW NEW TOWN near London has a problem—he does not wish to be seen. He refuses to stand up even when requested to do so by local authorities. However, he has chosen a very obvious piece of cover, hiding behind a lone bush in the middle of a clearing near a wood. The bush soon explodes and a scream is heard. The video telling his sad story and others like it is available online.[1]

Although Mr. Nesbitt is a fictional character in a Monty Python sketch, I cited this video in a footnote of a recent opinion[2] for several reasons. Partly it was to see how many people actually read footnotes in legal opinions. But the footnote also illustrates a sobering point: If the government wants to find you, it will find you. Even with very generalized cell phone tower data, the government can easily combine that with other available information—your Facebook page, employer's location, girlfriend's address, a credit card purchase—to figure out exactly where you are at any given time.[3] This is true even if, like the unfortunate Mr. Nesbitt, you don't want to be seen and refuse to stand up when asked.

---

* United States Magistrate Judge, Southern District of Texas, Houston Division. This paper is an extended version of remarks presented by the author at the University of San Francisco Law Review Symposium entitled "Big Brother in the 21st Century" on February 24, 2012.

1. *Monty Python's Flying Circus: How Not to be Seen* (BBC television broadcast Dec. 8, 1970), *available at* http://www.youtube.com/watch?v=zekiZYSVdeQ.

2. *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 837 n.69 (S.D. Tex. 2010).

3. *See generally* Nat'l Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment (2008), *available at* http://iis-db.stanford.edu/pubs/22285/Protecting_Individual_Privacy.pdf; Press Release, ACLU, FBI Data Mining and Collection Programs Threaten Privacy of Innocent Americans (Sept. 24, 2009), *available at* www.aclu.org/national-security-technology-and-liberty/fbi-data-mining-and-collection-programs-threaten-privacy-in.

This raises a question worth exploring. If Mr. Nesbitt cannot afford to stand up for himself, who *does* stand up for him and all the other Nesbitts in the world? That is, who stands between ordinary citizens like us and an increasingly surveillance-happy state?

I am the first to admit that some Nesbitts are dangerous and probably deserve to be watched. If Mr. Nesbitt heads up a drug cartel, runs a mortgage fraud scam, or commits a series of axe-murders, he should surely be found and brought to justice. But what about all the other Nesbitts who are law abiding: the soccer moms, the Sunday school teachers, the law school professors, the newspaper reporters?

You may say that's not a big concern because the government would not bother to target them unless they were committing a crime. But you would probably be wrong, at least if the government's response to a 2008 Freedom of Information Act suit is accurate. Asked to furnish docket information about all criminal cases brought against individuals who had been subject to warrantless cell phone tracking since 2001, the Department of Justice identified a total of just 255 criminal prosecutions.[4] This works out to about thirty-eight cases a year. Given that the federal government obtains tens of thousands of these orders every year,[5] this data suggests that the government spends more time chasing the innocent Nesbitts than the black sheep and ne'er-do-wells.[6]

And so I return to my question: Who stands up for the good Mr. Nesbitt? Consider the possible options. There is the executive branch itself—which is chiefly responsible for law enforcement—whose vital functions are carried out by many dedicated and hard-working professionals. Can't we just trust them to do the right thing? After all, they each take an oath to support and defend the U.S. Constitution. Yet that very same document contains a litany of limits on law enforcement, particularly in the Bill of Rights. If "Trust us, we're U.S. marshals" had been good enough for the founders, the Fourth Amendment would never have seen print.

4. ACLU v. U.S. Dep't of Justice, 655 F.3d 1, 4 (D.C. Cir. 2011).

5. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 322 (2012). While it is true that many courts now require a probable cause warrant as a prerequisite to such tracking, the first opinion doing so was not issued until 2005. *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber &/or Cell Site Info., 396 F. Supp. 2d 294, 295 (E.D.N.Y. 2005).

6. *See* Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1 (noting that eight cell phone companies reported that they responded to 1.3 million requests for subscriber information in 2011 from law enforcement agencies seeking text messages, caller locations, and other information in the course of investigations).

How about the legislative branch, the one most directly accountable to the electorate? Justice Alito, concurring in *United States v. Jones*,[7] suggested that the "best solution to privacy concerns may be legislative."[8] Alito's concurrence reflects an ongoing academic debate, in which the question is often re-framed as follows: Which branch of government, legislative or judicial, is best suited to rein in executive surveillance powers?[9]

Undoubtedly each branch brings certain institutional advantages (and disadvantages) to bear on the problem, but neither can legitimately claim outright superiority. As one scholar writes of the Supreme Court, it seems "scary to have major issues of policy determined by nine relatively uninformed people assisted by thirty-odd twenty-somethings surfing the Web."[10] At the same time, he writes, Congress is not much better:

> Legislation is as often based on anecdote as analysis, interest group influence in legislative determinations is rampant, staff influence is considerable, and legislative hearings are typically performances rather than attempts by the legislature or one of its committees to obtain information. Although romantic glorification of the judicial process may be the characteristic pathology of many lawyers and most American law professors, correcting for this by unwarranted glorification of the legislative process is no more justified.[11]

Moreover, this debate has an artificial, even metaphysical whiff about it. It's really a false choice—almost like asking which oar of a rowboat is the best, or which part of an airplane is your favorite: the left wing or the right. After all, the legislative and judicial branches do co-exist and operate side by side every day in every state in our nation. More than that, both branches need each other and cannot effectively do their jobs without the other. It is idle to pretend that either branch should twiddle their thumbs on the sidelines while the other plays the game. Like rowboats and airplanes, the rule of law maintains a true course only when opposing sides of government play their necessary

7. 132 S. Ct. 945 (2012).

8. *Id.* at 964. "Let this cup pass" is a familiar refrain by the Court when confronting new surveillance technology. *See* Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional restraints."); United States v. N.Y. Tel. Co., 434 U.S. 159, 179 (1977) (Stevens, J., dissenting) ("[I]n these areas, the Court's rush to achieve a logical result must await congressional deliberation.").

9. Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 295 (2011).

10. Frederick Schauer, *The Dilemma of Ignorance:* PGA Tour, Inc. v. Casey Martin, 2001 SUP. CT. REV. 267, 289 (2001).

11. *Id.* (footnotes omitted).

roles: one co-equal branch counter-balances another; no branch is dispensable. So the proper answer to the question—which branch of government, legislative or judicial, should oversee executive surveillance power—is both of them.

This is not to say that either branch has always lived up to its responsibilities. Take the legislative branch, the one most directly accountable to the people. As Justice Alito says, Congress "is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety"[12] however it sees fit. But how often does it see fit? The Electronic Communications Privacy Act of 1986 ("ECPA"),[13] the law governing most electronic surveillance, was passed in 1986, long before the advent of smart phones, Google, or even the World Wide Web.[14] The basic architecture remains in place,[15] but the edifice is showing its age, and the need for major renovation has been obvious for some time.[16] One of the biggest holes in the ECPA roof is geolocation monitoring.[17] Like an absentee landlord, Congress has all but ignored this widening breach since the problem first came to its attention in 1994.[18] Occasional bills have been introduced to patch this hole, but none have passed and several now languish in committee.[19] In the meantime, magistrate judges, with no congressional guidance about the governing legal standard, have issued hundreds of thousands of orders giving law enforcement

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

13. Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

14. *See Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited October 30, 2012); Smith, *supra* note 5, at 313.

15. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 92 (2010) (statement of Hon. Stephen Wm. Smith, U.S. Mag. J., S.D. Tex.).

16. *See* Harley Geiger, *Sen. Akaka Introduces Privacy Act Update*, CENTER FOR DEMOCRACY & TECH. (Oct. 28, 2011), https://www.cdt.org/blogs/harley-geiger/2810sen-akaka-introduces-privacy-act-update.

17. *See* Ulka Ghanta, *Competing Interests: Enforcing Cybersecurity and Protecting Privacy*, LAW PRAC. TODAY (March 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/competing-interests-enforcing-cybersecurity-and-protecting-privacy.html.

18. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103(a)(2)(B), 108 Stat. 4279, 4281 (1994) (codified at 47 U.S.C. § 1002(a)(2)) (forbidding the use of pen registers to obtain phone location data).

19. *See, e.g.*, ECPA Amendments Act of 2011, S. 1011, 112th Cong. (2011); Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011); Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011).

access to cell phone location data.[20] This gap in surveillance law has now persisted for *eighteen years*.

Consider next the judicial branch, and more specifically the Supreme Court, which after all is the ultimate arbiter of constitutional rights in our system. Has it done much better? The Supreme Court has decided a total of *two* ECPA cases[21] in the quarter century since that statute was passed, and in the most recent case decided in 2010, *City of Ontario v. Quon*,[22] the Supreme Court expressed the worry that maybe they were moving too fast. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[23] And what was the emerging technology they were so hesitant to consider in *Quon*? Pagers. Alphanumeric pagers. The pager's role in society is pretty clear now—nobody has one.[24]

To be fair, by the time the Court was writing its opinion in *Quon,* the underlying factual record was already eight years old—practically an eternity in the digital era. Even had the Court fully embraced the opportunity to comprehensively expound Fourth Amendment principles as applied to electronic communications in government workplaces, the record facts may have been useful only as a historical jumping-off point.

Another disadvantage faced by the *Quon* Court is the relative paucity of cases involving electronic surveillance under ECPA. The selection pool for the Supreme Court docket generally comes from the courts of appeal, where ECPA cases are in short supply. Take our topic for today—cell phone location tracking. So far, only one federal appellate court has ever addressed the question of the proper legal standard for government access to cell phone tracking records from a phone company, and that decision raised as many questions as it answered.[25]

---

20. *See* Smith, *supra* note 5, at 322.

21. City of Ontario v. Quon, 130 S. Ct. 2619 (2010); Bartnicki v. Vopper, 532 U.S. 514 (2001).

22. 130 S. Ct. 2619 (2010).

23. *Id.* at 2629.

24. This is not quite literally true, although total U.S. revenues for the paging industry did drop by approximately one-third from 2004 to 2008. Bob Cook, *Twilight of the beeper: Today's technology offers other ways of keeping connected*, Am. Med. News (June 9, 2008), http://www.ama-assn.org/amednews/2008/06/09/bisa0609.htm.

25. *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011).

Ordinarily, one might expect that the relative frequency of cases at the appellate level is indicative of their frequency at the district court level, hence the relative need for appellate guidance. But that is plainly not true of ECPA-related cases; every year the government files tens of thousands of applications for electronic surveillance orders under that statutory regime.[26] For reasons I have explained elsewhere,[27] almost none of these decisions are appealed. So despite a pressing need for appellate court guidance to magistrate judges deluged with these requests on a daily basis, almost none has been given.

Let's put this in perspective. Every year 15,000 employment discrimination cases are filed in federal court,[28] and based on innumerable Supreme Court and circuit precedents, every trial court knows what the plaintiff's burden of proof is. Inconceivable that it could be otherwise, most would agree. Yet, every year more than twice that number of electronic surveillance cases are filed and decided,[29] with literally no binding precedent[30] to specify the government's burden of proof when tracking your cell phone location. How is that conceivable?

Almost by default, then, these matters have been left to the lowest limb of the judicial branch: the magistrate judge. Unlike the Supreme Court, magistrate judges don't have the luxury of picking and choosing cases, of waiting until various appellate courts have weighed in with their considered judgment on difficult or novel issues of law. Magistrate judges are on the front lines, grappling hand to hand with the various, novel, and creative surveillance technologies deployed by law enforcement.[31] As a result, there is no danger of their decisions becoming technologically obsolete the moment they are issued.

That said, the ex parte nature of ECPA applications does present a major procedural challenge for magistrate judges. These are not adversary proceedings with opposing counsel present to argue the constitutional, statutory, or procedural rights of Mr. Nesbitt or the other targeted parties. To the contrary, the entire process is sealed away from public view, cordoned off by gag orders forbidding the elec-

26. Smith, *supra* note 5, at 321.

27. *Id.* at 328.

28. *See* Admin. Office of the U.S. Courts, 2006 Annual Report of the Director: JUDICIAL BUSINESS OF THE UNITED STATES COURTS 168 tbl.C–2 (2007), *available at* http://www.uscourts.gov/uscourts/Statistics/JudicialBusiness/2006/front/completejudicialbusiness.pdf.

29. *See* Smith, *supra* note 5, at 322.

30. *See id.* at 326–31.

31. *See, e.g.*, *In re* U.S. *ex rel.* Order Pursuant to 18 U.S.C. § 2703(d), C.R. No. C–12–670M, 2012 WL 4717778 (S.D. Tex. Sept. 26, 2012).

tronic service provider from telling customers that their cell phone or email records have been turned over to the government.[32] Under these circumstances, it necessarily falls to the magistrate judge to ensure that the target's legal rights are respected. Her role is not that of an umpire calling balls and strikes, but more like a referee in a one-sided soccer match forced to play goalie for the missing side.

Ex parte proceedings obviously preclude the sort of adjudicative fact-finding that is the hallmark of an adversarial hearing in our judicial system. Even so, there are other extra-record sources of information available to the court. Data from these sources are commonly referred to as "legislative facts," as opposed to the facts to be adjudicated in a particular case.[33] Although the terms "legislative" and "adjudicative" facts were coined by Professor Kenneth Davis in a landmark 1942 article,[34] they describe a distinction rooted in the common law.[35] Adjudicative facts typically concern what happened between the parties. They usually answer the questions of who did what, where, when, how, why, and with what motive or intent and are resolved under the rules of evidence.[36] On the other hand, "legislative facts" are not the facts of the particular case but more generalized facts about the world.[37] As one scholar has recently explained:

> A legislative fact gets its name not necessarily because it is found by a legislature, but because it relates to the "legislative function" or policy-making function of a court. The central feature of a legislative fact is that it "transcend[s] the particular dispute," and provides descriptive information about the world which judges use as foundational "building blocks" to form and apply legal rules.[38]

This distinction is neither novel nor controversial; it was incorporated into the Federal Rules of Evidence more than thirty years ago.[39] Legislative facts come to the court's attention by various means: testimony or documentary evidence offered by parties at the trial level;

32. *See* Smith, *supra* note 5, at 322–26.

33. Allison Orr Larsen, *Confronting Supreme Court Fact Finding*, 98 VA. L. REV. 1255, 1258–59 (2012).

34. Kenneth Culp Davis, *An Approach to Problems of Evidence in the Administrative Process,* 55 HARV. L. REV. 364, 402 (1942).

35. *See* 2 RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 940, 948–49 (5th ed. 2010).

36. 2 KENNETH CULP DAVIS, ADMINISTRATIVE LAW TREATISE § 15.03, at 353 (1st ed. 1958).

37. Larsen, *supra* note 32, at 1255.

38. *Id.* at 1256–57 (footnotes omitted) (alteration in original).

39. FED. R. EVID. 201.

briefing by parties and amici on appeal; or, when the efforts of the parties are deemed insufficient, in-house research by the court itself.[40]

Legislative facts are especially common in deciding constitutional questions, including the application of the Fourth Amendment to evolving surveillance technology.[41] For example, in *Berger v. New York*,[42] the Court declared unconstitutional a New York statute authorizing electronic eavesdropping without a probable cause warrant.[43] The Court's opinion roamed freely beyond the factual record,[44] which was summarized in a couple of short paragraphs at the beginning of the opinion and hardly ever mentioned again. The Court traced the history of eavesdropping from the days of Blackstone, to its 19th century transformation into "wiretapping" by the invention of the telegraph and telephone, and finally to its modern incarnation as sophisticated electronic devices: miniature bugs, fountain pen and cufflink microphones, electronic rays beamed at walls, mirror transmitters, off-premise parabolic microphones, etc.[45] The cited source for this "eavesdropping catalogue of horrors,"[46] as the dissent mockingly called it, was a law review article published after the trial.[47] Other extra-record citations included testimony at a Senate Judiciary Committee hearing, a report by the President's Commission on Law Enforcement and Administration of Justice, and a reference to a poll of New York prosecutors published eight years previously in a book titled "The Eavesdroppers."[48] That poll was especially significant because its numbers were used to refute the government's claim that outlawing electronic eavesdropping would severely cripple crime detection.[49]

Another Supreme Court case resting heavily on legislative facts is *Smith v. Maryland*,[50] where the Court ruled that installation and use of a pen register is not a search protected by the Fourth Amendment.[51] Again, the Court reached out to extra-record sources to explain the

40. Larsen, *supra* note 32, at 1257–58.

41. DAVID L. FAIGMAN, CONSTITUTIONAL FICTIONS: A UNIFIED THEORY OF CONSTITUTIONAL FACTS 44 (2008).

42. 388 U.S. 41 (1967).

43. *Id.* at 44.

44. *Id.* at 44–45 (petitioner was convicted of conspiracy to bribe a public official to obtain a liquor license).

45. *Id.* at 45–47.

46. *Id.* at 82 (Black, J., dissenting).

47. *Id.* at 47 (citing Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003, 1005–10 (1966)).

48. Berger v. New York, 388 U.S. 41, 60–62 (1967)

49. *Id.* at 61.

50. 442 U.S. 735 (1979).

51. *Id.* at 742.

technology and function of this surveillance device—in particular, two law review articles explaining that pen registers were regularly employed by telephone companies to detect fraud, monitor equipment, prepare customer bills, and identify obscene or annoying phone callers.[52] More striking, perhaps, was the Court's reliance on consumer information said to appear in "[m]ost phone books" to establish that telephone users had no subjective expectation of privacy in the numbers they dial.[53] This prompted a classic sarcastic jibe from the dissent.[54] The Court's affinity for legislative facts was also seen in its refusal to hinge a constitutional ruling on how the particular phone company handling the pen register chose to bill its customers for local calls: "We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation."[55]

A more recent illustration is *Kyllo v. United States*,[56] involving the constitutionality of using thermal-imaging devices to detect relative amounts of heat within the home.[57] The decision turned on the technical capabilities of thermal imagers in general, after pointedly casting aside the findings of an evidentiary hearing on the intrusiveness of the Agema Thermovision 210 model used on Kyllo's house.[58] "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[59] Also relied upon was a Department of Justice website (as last visited a month prior to its opinion) that touted the ability to "see" through walls and other opaque barriers as a scientifically feasible goal of law enforcement research and development.[60] The Court dismissed the significance of the actual videotape

52. *Id.* at 741–42 (citing Victor S. Elgort, Note, *The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028 (1975); William A. Claerhout, *The Pen Register*, 20 DRAKE L. REV. 108 (1970)).

53. *Id.* at 742–43.

54. "Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers . . . I decline to assume general public awareness of how obscene phone calls are traced." *Id.* at 749 n.1 (Marshall, J., dissenting).

55. *Id.* at 745.

56. 533 U.S. 27 (2001).

57. *Id.* at 29.

58. *Id.* at 30–31.

59. *Id.* at 36.

60. *Id.* at 36 n.3 (citing NAT'L L. ENFORCEMENT & CORRECTIONS TECH. CENTER, http://www.nlectc.org/techproj/ (last visited May 3, 2001)). While the originally cited webpage is no longer available, for recent NLECTC updates on surveillance technology see *Sensors &*

of the thermal imaging of the defendant's residence, which had revealed only amorphous images in shades of gray, declaring that the Court must take the "long view" and give "clear specification of those methods of surveillance that require a warrant."[61]

I do not wish to be misunderstood. These cases do not stand for the proposition that adjudicative facts are irrelevant or never important in constitutional litigation. But they do confirm that legislative facts generated outside the adversarial process can be important, and sometimes determinative, in applying the Fourth Amendment to surveillance technology. This means that magistrate judges need not be deterred from ruling on the constitutionality of electronic surveillance requests simply because the process is ex parte, with little or no opportunity for an adversary hearing. A magistrate judge forced to decide such questions as a matter of first impression need not hesitate to use the same tools, extra-record or not, that appellate courts regularly employ for the same task. The digital revolution has made that tool more powerful than ever, with massive amounts of information "just a Google search away."[62]

One commentator has argued that magistrate judges are never permitted, much less forced, to decide constitutional questions unless a statute expressly confers such authority.[63] This seems a very odd proposition given that magistrate judges (and U.S. commissioners before them) have long been entrusted with responsibility for issuing arrest and search warrants,[64] which are nothing other than the flesh and bone of the Fourth Amendment. It is also very odd to imagine Congress appending *Marbury v. Madison*[65] clauses to its legislation, as if to thoughtfully remind the third branch of its powers of judicial review.

Surveillance Technologies, JUSTNET, https://www.justnet.org/sensors/index.html (last visited Nov. 20, 2012).

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

62. Larsen, *supra* note 32, at 1260. The author rightfully points out the potential dangers of this brave new world, such as unreliable or mistaken sources, systematic bias, and notice/legitimacy concerns. Obviously, care should be taken to assure that extra record sources are both credible and reliable.

63. Orin Kerr, *Can Magistrate Judges Rule on How the Fourth Amendment Applies to the Execution of a Court Order At the Time of the Application?*, THE VOLOKH CONSPIRACY (Feb. 28, 2012, 2:33 AM), http://www.volokh.com/2012/02/28/can-magistrate-judges-rule-on-how-the-fourth-amendment-applies-to-the-execution-of-a-court-order-at-the-time-of-the-application/.

64. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948) (explaining that protection of the Fourth Amendment requires a neutral and detached magistrate to issue search warrants).

65. 5 U.S. (1 Cranch) 137 (1803).

The same commentator has also contended that Fourth Amendment issues are not even ripe for consideration by a magistrate judge presented with a government application for electronic surveillance.[66] According to this view, Fourth Amendment issues ought not even be considered until after the search has been carried out, charges filed, and a hearing or trial conducted in the normal adversarial setting, with counsel for both sides free to present their best arguments and evidence.[67] That way the factual record is fixed, with no need for speculation, and the law can be applied retrospectively, firmly grounded in historical facts.[68]

This argument seems profoundly misguided. In the first place, warrant decisions are inherently prospective. Like horse race bets and hurricane predictions, they cannot be made after the anticipated event occurs. What would be the point? They must be made on limited and imperfect information available beforehand, or they won't be made at all. When is a surveillance order ever ripe for determination under the Constitution if not at the time the application is made?

Secondly, the legal issues presented before and after the search are often very different. When a trial court considers whether to suppress evidence or overturn a conviction based on challenged evidence, its decision usually does not turn solely on whether the magistrate judge correctly applied the Fourth Amendment to the government's application.[69] Instead, the court asks whether this particular defendant has standing to challenge the search or seizure;[70] whether the evidence was the fruit of a poisonous tree;[71] whether the defendant timely objected to the evidence or waived objection by opening the door;[72] whether the tainted evidence was admissible for

66. Kerr, *supra* note 62.

67. *See* Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1293 (2010). For a response to Kerr's doctrinal arguments, see Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011), *available at* http://www.virginialawreview.org/inbrief.php?s=inbrief&p=2011/03/20/ohm.

68. Some have criticized this model of case-specific adjudication as reflecting a conventional prejudice not supported by current social science research. *See* Frederick Schauer, *Do Cases Make Bad Law?*, 73 U. CHI. L. REV. 883, 895 (2006) ("when decisionmakers are in the thrall of a highly salient event, that event will so dominate their thinking that they will make aggregate decisions that are overdependent on the particular event and that overestimate the representativeness of that event within some larger array of events").

69. *See generally* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY 378–464 (5th ed. 1996).

70. *See* Rakas v. Illinois, 439 U.S. 128 (1978).

71. *See* Brown v. Illinois, 422 U.S. 590 (1975).

72. *See* Walder v. United States, 347 U.S. 62 (1954).

other purposes such as impeachment;[73] or whether its admission was harmless error.[74] Even if the court finds that the magistrate judge improperly issued the warrant, the evidence need not be excluded where law enforcement has acted in good faith.[75] Finally, it must be remembered that warrant decisions affect the rights of individuals (like our good Mr. Nesbitt) who have not been charged with a crime and thus will never have occasion to file a motion to suppress. A single warrant decision can affect the rights of many besides the accused.

These considerations refute the idea that the warrant decision made by a magistrate judge ex ante is the same as the evidentiary ruling made by a trial court ex post, separated only by time's arrow. In many respects the two decisions are independent of one another, based on differing legal standards and sets of relevant facts. It is misleading to suggest that they are merely two sides of the same legal coin.

In any event, magistrate judges do not have the luxury of retrospective adjudication, of waiting until a suppression motion to evaluate the legality of a search that has already been conducted. Magistrate judges swear an oath to uphold the Constitution—the same oath taken by Article III judges. When a federal agent walks into our chambers to request an electronic surveillance order, there is nobody there but us to make sure the Constitution is followed. If we sign a warrant that, in our considered opinion, violates the Fourth Amendment, then we have violated our solemn oath, and when we conclude that certain types of surveillance orders must be denied because they do not comply with the Constitution, then we owe it to the public and law enforcement to explain our reasons on the record. That way, our conclusions can be challenged and tested not only in the courts of appeals but also in the court of public opinion (including, for what it's worth, blogs and academic journals).

In short, magistrate judges should stand up. And we must stand up even though—or rather precisely because—Congress and the Supreme Court have not. We owe that much to the good Mr. Nesbitt.

73. *See* United States v. Havens, 446 U.S. 620 (1980).
74. *See* Chapman v. California, 386 U.S. 18 (1967).
75. *See* United States v. Leon, 468 U.S. 897, 926 (1984).