

2010

Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire

Christopher Slobogin

Follow this and additional works at: <https://scholarship.law.umn.edu/mlr>

Part of the [Law Commons](#)

Recommended Citation

Slobogin, Christopher, "Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire" (2010). *Minnesota Law Review*. 509.
<https://scholarship.law.umn.edu/mlr/509>

This Article is brought to you for free and open access by the University of Minnesota Law School. It has been accepted for inclusion in Minnesota Law Review collection by an authorized administrator of the Scholarship Repository. For more information, please contact lenzx009@umn.edu.

Article

Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire

Christopher Slobogin[†]

In 2007, I published *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*.¹ The immediate trigger for the book was the recent upsurge in government use of technology to monitor public and private behavior, and more particularly the tremendous increase in government surveillance after 9/11 using techniques such as data mining, phone and computer intercepts, and public camera systems. The primary analytical target of the book, however, was more general: Supreme Court case law that, read broadly, permits much of this technological surveillance to take place without impinging on any constitutional interests.² In an effort to counteract this tendency, the book constructs a Fourth Amendment framework—meant to apply to every type of government investigative technique, technologically enhanced or not—that is both more faithful to precedent and more attentive to the empirical reality of how the techniques affect individual interests and meet law enforcement needs.

The principal component of this framework is the idea that the justification for a government search or seizure ought to be roughly proportionate to the invasiveness of the search or seizure.³ This proportionality principle is a simple but powerful concept found throughout American jurisprudence, including a number of the Supreme Court's Fourth Amendment cases.⁴

[†] Milton Underwood Professor of Law, Vanderbilt University Law School. Copyright © 2010 by Christopher Slobogin.

1. CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* (2007).

2. See *infra* text accompanying notes 23–25 (describing cases).

3. SLOBOGIN, *supra* note 1, at 21–48.

4. *Id.* at 21, 28–30 (describing proportionality reasoning in *Terry v. Ohio*, 392 U.S. 1 (1968), and in various other settings in connection with standards of proof, equal protection law, and tort law).

But, as noted above, the Court's specific Fourth Amendment holdings leave a wide array of surveillance techniques unregulated. Relying in part on surveys measuring the public's attitudes toward surveillance, *Privacy at Risk* argues to the contrary that most types of surveillance are sufficiently intrusive to require justification, albeit not always at the probable cause level.⁵

Two well-known scholars who have reviewed the book are Orin Kerr and Peter Swire. Professor Kerr is much more comfortable with the Court's current position on the Fourth Amendment than I am, and disagrees with my attempt to constitutionalize and empiricize regulation of government surveillance.⁶ Professor Swire is willing to contemplate my proposals, but wishes that I had devoted more attention to national security issues and to transnational law that is consistent with my approach.⁷ This Symposium⁸ provides an opportunity to respond to these reviews and, in the process, elaborate on some of the arguments made in *Privacy at Risk*. On the latter score, I rely on two works published after *Privacy at Risk*. The first, David Faigman's *Constitutional Fictions*, emphasizes the importance of empirical findings to constitutional adjudication.⁹ The second, Richard Worf's article on general suspicionless searches and seizures,¹⁰ bolsters my brief observations in *Privacy at Risk* about the relevance of political-process theory to efforts at justifying surveillance of groups.¹¹

I. THE THESIS OF *PRIVACY AT RISK*

Professor Kerr calls the proportionality principle that I advance in *Privacy at Risk* "a new approach to the Fourth Amendment."¹² But proportionality reasoning in Fourth Amendment cases is not my invention. Much of the Supreme

5. SLOBOGIN, *supra* note 1, at 18–19.

6. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 966 (2009).

7. Peter P. Swire, *Proportionality for High-Tech Searches*, 6 OHIO ST. J. CRIM. L. 751, 751 (2009).

8. Symposium, *Cyberspace and the Law: Privacy, Property, and Crime in the Virtual Frontier*, 94 MINN. L. REV. 1303 (2010).

9. See DAVID L. FAIGMAN, CONSTITUTIONAL FICTIONS: A UNIFIED THEORY OF CONSTITUTIONAL FACTS 162 (2008).

10. Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 TOURO L. REV. 93 (2007).

11. See SLOBOGIN, *supra* note 1, at 18.

12. See Kerr, *supra* note 6, at 951.

Court's search and seizure jurisprudence is consistent with the idea that the more privacy-invading or autonomy-limiting a police action is, the more justification the government must show before it may be carried out. Thus, while most searches of houses and most arrests are only permissible if the police have probable cause,¹³ lesser searches, such as pat-downs, and lesser seizures, such as field stops, only require reasonable suspicion.¹⁴ For brief seizures at sobriety and illegal-immigrant roadblocks no individualized justification is necessary.¹⁵

Admittedly, in some "special needs" situations, such as drug testing of employees or school children, the Court has allowed seemingly serious intrusions on virtually no suspicion, and thus appears to have departed from the proportionality idea.¹⁶ Those situations, however, usually involve searches of groups rather than individuals, a situation that requires a different mode of analysis.¹⁷ In most of its Fourth Amendment cases, the Court has adhered, consciously or not, to the notion expressed in 1967 in *Terry v. Ohio* that "there is 'no ready test

13. See, e.g., *Payton v. New York*, 445 U.S. 573, 588–90 (1980) (holding that the nonexigent entry of a home to effect an arrest or search requires a warrant based on probable cause because the Fourth Amendment "unequivocally establishes the proposition that '[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion'" (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961))).

14. *Terry v. Ohio*, 392 U.S. 1, 26 (1968) (permitting a frisk for weapons and the predicate stop on less than probable cause because it only "constitutes a brief, though far from inconsiderable, intrusion upon the sanctity of the person").

15. See *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (upholding suspicionless stops at sobriety checkpoints, given "the balance of the State's interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped"); *United States v. Martinez-Fuerte*, 428 U.S. 543, 562 (1976) (upholding suspicionless checkpoints to detect illegal immigrants because "the reasonableness of the procedures followed in making these checkpoint stops makes the resulting intrusion on the interests of motorists minimal").

16. See, e.g., *Bd. of Educ. v. Earls*, 536 U.S. 822, 829 (2002) (upholding suspicionless drug testing of students involved in extracurricular activities, stating that "[i]t is true that we generally determine the reasonableness of a search by balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests [but] in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable" (internal quotation marks omitted)).

17. See *infra* text accompanying notes 146–57.

for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails.”¹⁸

The problem with the Court’s post-*Terry* cases is not their adoption of a balancing framework but their willingness to make blithe assumptions about the “invasiveness” of the government actions and to treat legislative and executive allegations of law enforcement “need” as givens. Instead, I argue, the Court should engage in strict scrutiny analysis of government efforts to obtain evidence of wrongdoing.¹⁹ *Privacy at Risk* elaborates on this argument by focusing on two different types of government surveillance, “physical surveillance” and “transaction surveillance.” Physical surveillance refers to real-time observation of physical behavior with the naked eye or with technology such as binoculars, night scopes, tracking devices, and surveillance cameras.²⁰ Transaction surveillance involves obtaining information about transactions from third-party record-holders, such as banks, credit card agencies and Internet service providers (ISPs).²¹ With the help of technology, both types of surveillance have increased exponentially in the past decade.²²

Yet the Court’s construal of the Fourth Amendment has left these investigative techniques entirely unregulated as a constitutional matter. *Katz v. United States*’ definition of “search”—to wit, any government action that infringes “[an] expectation [of privacy] that society is prepared to recognize as reasonable”²³—seems expansive. But since *Katz* was decided in 1967 the Court has been extremely grudging in its approach to the Fourth Amendment’s threshold. According to the Court’s post-*Katz* case law, it is not reasonable to expect privacy in connection with any activity, including activity that takes place inside the home, that can *conceivably* be seen from a lawful vantage point with the naked eye or with technology that is in general public use, such as binoculars.²⁴ Even more incredibly,

18. 392 U.S. at 21 (citing *Camara v. Mun. Court*, 387 U.S. 523, 536–37 (1967)).

19. See SLOBOGIN, *supra* note 1, at 17.

20. See *id.* at 6–9 (defining physical surveillance).

21. See *id.* at 9–13 (defining transaction surveillance).

22. See *id.* at 3.

23. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

24. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (strongly suggesting that no search occurs “where . . . Government uses a device that

the Court has held that the public “assumes the risk” that personal information surrendered to third parties such as banks and phone companies will be disclosed to the government upon demand, and thus can expect no privacy in that context either.²⁵

In *Privacy at Risk*, I argue that this series of decisions by the Court is conceptually bankrupt, principally because of the Court’s refusal to recognize that expectations of privacy can only be gauged through some real world referent, such as positive law governing ordinary citizens or the considered views of the population.²⁶ Neither source provides much support for the Court’s holdings. In many jurisdictions, it is often a crime, or at least a tort, for private citizens to engage in “peeping Tomism” of the home.²⁷ And various federal and state statutes guarantee the confidentiality of records maintained by hospitals, banks, schools, and other institutions, and penalize breach of this confidentiality with civil and even criminal penalties.²⁸ Yet the Court’s Fourth Amendment jurisprudence declares that the American public can expect no privacy vis-à-vis government voyeurism or perusal of our transactions.

Where legislation governing surveillance by the private sector does not exist (usually because, as with public camera surveillance, there is no private-surveillance analogy) or does not provide an indication of *how* private particular types of activities or records are, *Privacy at Risk* argues that surveys of the population should be considered relevant to Fourth

is . . . in general public use, to explore details of the home . . . without physical intrusion”); *California v. Ciraolo*, 476 U.S. 207, 213–14 (1986) (holding that the viewing of a backyard from an airplane in navigable airspace was not a search because “[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed”).

25. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (“This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); *United States v. Miller*, 425 U.S. 435, 443 (1976) (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”).

26. SLOBOGIN, *supra* note 1, at 108–10. The Court itself has recognized this point in the abstract. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.”). In practice, however, the Court has ignored it.

27. *See* SLOBOGIN, *supra* note 1, at 68–69.

28. *Id.* at 157–58.

Amendment analysis.²⁹ Over the past fifteen years I have conducted three such surveys, usually relying on jury pools to assure a diverse, randomly selected sample.³⁰ Each sample received a number of scenarios, most taken from Supreme Court cases, depicting various types of government investigative techniques, and was asked to rate the “intrusiveness” of the techniques on a scale of 1 to 100, with 100 being the most intrusive.³¹

My findings with respect to the various surveillance scenarios can be summarized as follows: virtually all forms of transaction surveillance as well as overt public camera surveillance are viewed, on average, as more intrusive than a roadblock, and government efforts to access records from websites, ISPs, pharmacies, and banks are perceived to be as intrusive as a search of a car.³² If these results are replicated by other studies, they could be said to describe the relative privacy “reasonable people” expect vis-à-vis these types of government intrusion. Further, a proportionality analysis based on these results would hold that establishment of a public camera system requires at least as much justification as the erection of a roadblock, and that government attempts to obtain records of many types of transactions require the same level of justification as the search of a car—probable cause.

Further description of *Privacy at Risk* will be incorporated into my responses to the comments by Professors Kerr and Swire. Most of this discussion will focus on Professor Kerr’s comments because they are more critical of the book. Following the organization Professor Kerr adopts in his review, the response to the Kerr and Swire critiques will focus on the two

29. *Id.* at 113–16.

30. The surveys, all of which are discussed in *Privacy at Risk*, first appeared in Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 (2008) [hereinafter, Slobogin, *Data Mining*]; Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 277 (2002); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727, 738 (1993).

31. See, e.g., SLOBOGIN, *supra* note 1, at 111.

32. See *id.* at 112 (showing a mean intrusiveness rating (MIR) of 35 for roadblock scenario and of 53 for overt camera scenario in which tapes are destroyed); see also *id.* at 184 (showing MIRs for scenarios involving obtaining information from websites, ISPs, pharmacies, and banks between 74.4 and 78.0).

sides of the proportionality inquiry: intrusiveness and justification.³³

II. THE NATURE OF INTRUSIVENESS

As both Professor Kerr and Professor Swire point out, crucial to application of the proportionality principle that I propose in *Privacy at Risk* is an assessment of intrusiveness. Professor Swire finds “useful” my proposal that the government’s justification for a search or seizure bear a relationship to its intrusiveness, and he “particularly like[d]” the reliance on empirical surveys as a means of informing the courts about reasonable expectations of privacy.³⁴ Professor Kerr reacts quite differently. He argues that asking people to rate police actions on an “intrusiveness” scale does not accurately capture privacy expectations, that even if it did courts would have great difficulty knowing how to use such empirical results, and that even if courts could carry out the latter role they should not do so, because ultimately assessment of societal expectations of privacy is not very important for Fourth Amendment purposes. I will address each of these points in turn.

A. INTRUSIVENESS AS THE MEASURE OF FOURTH AMENDMENT INTERESTS

Professor Kerr believes that “measuring intrusiveness does not actually measure how much a technique infringes on civil liberties,” and thus that my intrusiveness surveys are misleading on that score.³⁵ The word “intrusiveness” undoubtedly does

33. This focus means that this Article (like Professor Kerr’s review) neglects several aspects of *Privacy at Risk*. Kerr’s review looks only at the discussion of the proportionality principle in Chapter 2 and three later chapters (Chapters 4, 5, and 7) describing how that principle would apply to surveillance of public activities and to transaction surveillance. See Kerr, *supra* note 6, at 952. Chapter 2 also develops the “exigency” principle (which requires ex ante review of nonemergency searches and seizures) and critiques other Fourth Amendment theories. SLOBOGIN, *supra* note 1. Also not discussed here or in Kerr’s review are Chapter 3, which is devoted to technological surveillance of the home; Chapter 6, which provides an historical analysis of subpoena law (an analysis that is crucial to understanding how we ended up without any constitutional regulation of transaction surveillance); and Chapter 8, which is a concluding discussion of how the “liberal” view of the Fourth Amendment—requiring individualized probable cause for all searches and exclusion as a remedy—has inadvertently and ironically resulted in a much smaller Fourth Amendment than we would have if liberals had been a little less greedy. *Id.*

34. Swire, *supra* note 7, at 757.

35. Kerr, *supra* note 6, at 959.

not capture all of privacy's dimensions. Nonetheless, directly asking people whether they expect "privacy" in a given situation is not a productive means of assessing their views on the privacy interests affected by police actions, for a variety of reasons.³⁶ More importantly, the Supreme Court itself often uses "intrusiveness" or "invasiveness" as a proxy for analyzing the individual interests at stake in Fourth Amendment cases; indeed, well over 200 of the Supreme Court's Fourth Amendment opinions rely on one or both phrases for this purpose.³⁷ Thus, for instance, in *Scott v. Harris*, decided two terms ago, the Court stated, "[i]n determining the reasonableness of the manner in which a seizure is effected, '[w]e must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'"³⁸ In the Court's search cases as well, ranging from *Terry* to the more recent string of "special needs" cases, the conclusion that a particular technique is relatively unintrusive is usually crucial in holdings favoring relaxation of Fourth Amendment strictures.³⁹

Nonetheless, Professor Kerr argues that use of the word "intrusiveness" skewed my survey results. To him, the word

36. One reason, of course, is precisely the fact that the concept of privacy is open to so many interpretations. See generally Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) (exploring the multiple meanings of privacy). Additionally, framing the survey in terms of privacy expectations would have signaled the purpose of the survey to those who know Fourth Amendment law, would not have permitted sensible answers to scenarios involving seizures rather than searches, and would have in essence asked the intrusiveness question in any event, with a question sounding something like: "On a scale of 1 to 100, how significant is the privacy invasion in the following scenarios?" A further advantage of using the word "intrusion" without reference to privacy is that it minimizes the effect of foreknowledge about the law: one might feel intruded upon despite a subjective recognition that the law does not consider the intrusion to be an invasion of privacy.

37. See generally Chart Prepared by Andrew Cunningham, Student, Vanderbilt University Law School (2009) (on file with author) (depicting holdings in 227 U.S. Supreme Court Fourth Amendment cases in which "intrusion" or "invasion" or some variant thereof was used in describing the Court's reasoning).

38. *Scott v. Harris*, 127 S. Ct. 1769, 1778 (2007) (quoting *United States v. Place*, 462 U.S. 696, 703 (1983)).

39. See *supra* notes 13–16; see also *Delaware v. Prouse*, 440 U.S. 648, 653–54 (1979) ("The essential purpose of the proscriptions in the Fourth Amendment is to impose a standard of reasonableness upon the exercise of discretion by government officials, including law enforcement agents, in order to safeguard the privacy and security of individuals against arbitrary invasions" (internal quotation marks omitted)).

“intrusive” means “interference with the status quo,” so that “police techniques that are uncommon, unexpected, or high-profile will tend to be seen as intrusive.”⁴⁰ Thus, he argues, my survey participants may have indicated that a surveillance technique such as use of video cameras arrayed along a public street is relatively intrusive because it is not yet pervasive, not because people sense that their civil liberties would be infringed by the practice.⁴¹

A first response to this observation is that, if unexpectedness were correlated with intrusiveness as Professor Kerr suggests, then my survey participants should have arrived at different rankings than they did. For instance, they should have ranked scenarios such as those involving covert video surveillance and data mining as very intrusive, because their occurrence is rare, whereas searches of cars and pat-downs should have been seen as relatively unintrusive, since these are daily and well-understood events. Yet I obtained precisely the opposite results.⁴² More fundamentally, if it turned out that unexpectedness did have a high correlation with intrusiveness in some types of cases, it is not clear why that is a problem; after all, the Court’s test speaks of “expectations” of privacy. If we discount the public’s belief that an investigative technique is intrusive when that technique is new or unusual, we move in the direction of granting Fourth Amendment immunity to the type of innovative technological surveillance that became commonplace in Orwell’s society of 1984.⁴³

This comment leads directly to another criticism that Professor Kerr makes about the intrusiveness construct. He states that the public cannot accurately evaluate the invasiveness of physical and transaction surveillance because the media (irresponsibly) associates these techniques with “Big Brother.”⁴⁴ But if the public is reacting to surveillance in a media-driven, knee-jerk fashion, my survey participants presumably would not have ranked covert cameras lower than both searching a jun-

40. Kerr, *supra* note 6, at 958.

41. *Id.* at 959.

42. See SLOBOGIN, *supra* note 1, at 112 (indicating an MIR of 35 for covert video surveillance and an MIR of 68 for a patdown); *id.* at 184 (showing MIRs of 32.4, 34.1, and 38.5 for various types of data mining and an MIR of 74.6 for a car search).

43. See GEORGE ORWELL, 1984, at 5 (Signet Classics 1981) (1949) (describing an omnipresent government-monitored “telescreen”).

44. Kerr, *supra* note 6, at 960 (calling some media depictions of surveillance techniques “comically incorrect”).

kyard or overt use of cameras, nor would they have ranked data mining of airplane passenger lists much lower than pat-downs or data mining of phone records.⁴⁵ The subjects in my surveys appear to make an earnest effort to rank the various scenarios according to how intrusive they think each is; they are not lumping all the surveillance techniques into one Big Brother category.

A final criticism Professor Kerr makes of the way in which the surveys were conducted focuses on the fact that I told participants to assume the targets of the police were innocent.⁴⁶ I did so because the Supreme Court has held that the innocent target is the appropriate perspective for determining when a seizure has occurred for Fourth Amendment purposes.⁴⁷ Although Professor Kerr correctly points out that the Court has never said that the same perspective applies to analysis of searches,⁴⁸ I can think of no good reason for distinguishing the two situations.

But Professor Kerr is apparently making a larger point than a mere quibble over the explicit holdings of the Court. He states, “[a] technique used exclusively to target the guilty would be much less intrusive than one often used to target the innocent. As a result, any assessment of the civil liberties threat posed by a particular investigative technique must account for the settings in which the police employ the technique.”⁴⁹ Professor Kerr seems to be saying that since my “innocent target” assumption applied to all the scenarios, ranging from those usually aimed at highly suspicious people (such as bedroom searches and requests for bank records) to those targeting primarily innocent people (such as roadblocks and data mining), it somehow tainted the results.

If Professor Kerr is arguing that intrusiveness ratings change depending on the perceived guilt of the target, he is probably right. But results from my first study, which are brief-

45. See SLOBOGIN, *supra* note 1, at 112 (showing an MIR of 42 for covert camera surveillance, of 51 for search of a junkyard, and of 53 for overt camera use); *id.* at 184 (showing an MIR of 32.4 for data mining of passenger lists, 71.5 for a patdown, and 74.1 for data mining of phone records).

46. Kerr, *supra* note 6, at 959.

47. See *Florida v. Bostick*, 501 U.S. 429, 438 (1991) (“[T]he potential intrusiveness of the officers’ conduct must be judged from the viewpoint of an innocent person in [his] position.” (quoting *Florida v. Royer*, 460 U.S. 491, 519 n.4 (1983) (Blackmun, J., dissenting))).

48. Kerr, *supra* note 6, at 961.

49. *Id.* at 960.

ly noted in *Privacy at Risk*,⁵⁰ should allay any concern that this dynamic diminished the value of the survey results. In that study, conducted with Joseph Schumacher, we admittedly did find that subjects' ratings of intrusiveness usually dropped when we varied the scenarios by including a description of the specific evidence sought (e.g., search of a bedroom versus search of a bedroom for drugs).⁵¹ We also found that the seriousness of the crime under investigation correlated inversely with intrusiveness ratings; thus, for instance, the scenario involving a pat-down for evidence of terrorism was seen as much less intrusive than the pat-down scenario that did not specify the evidence sought.⁵² However, we further found that the intrusiveness *hierarchy* stayed relatively intact regardless of the crime or context involved.⁵³ For instance, holding the seriousness of the crime or the police's suspicions constant, frisks are always seen as less intrusive than perusal of bank records, and roadblocks are always seen as less intrusive than technological physical surveillance of private property.⁵⁴ If the object of a search or the guilt of the target affects intrusiveness ratings, it affects all of them roughly equally.

Professor Kerr might instead be arguing that, regardless of how survey participants responded, conclusions about intrusiveness should differ *in each case* depending upon the sus-

50. SLOBOGIN, *supra* note 1, at 33.

51. Slobogin & Schumacher, *supra* note 30, at 759. More specifically, we found that when a scenario both described the target as the survey participant (rather than some third party) and described the evidence being sought (as opposed to not mentioning any evidence), the combined mean for all fifty scenarios was fifteen points lower (48.93 compared to 63.19). *Id.* Dr. Schumacher is a Ph.D. psychologist who assisted in the empirical analysis.

52. *Id.* at 764 tbl.4; *see also id.* at 767 (describing "dangerousness theory" of intrusiveness, to the effect that if the subject believes the target of the search is dangerous, the perceived intrusiveness of a police action will be lower).

53. *Id.* at 764, 767–68 (finding consistency between the scenarios at the top and bottom of the rankings, and significant inconsistencies only with respect to ten scenarios, perhaps explainable by the extent to which subjects viewed the target of the search to be dangerous); *see also* Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 349–50 (2009) (finding "high correlations between overall intrusiveness ratings of stimuli in samples with and without context"—context meaning a description of what the police were looking for—but noting variations upon closer examination of particular contexts).

54. Slobogin & Schumacher, *supra* note 30, at 762–63 tbl.3 (showing, across all conditions, a pat-down rated as 19, 21, 27, and 9; perusal of bank records rated as 36, 40, 38, and 36; roadblocks rated as 9, 16, 15, and 13; and viewing a backyard with binoculars rated as 34, 33, 35, and 29).

pected guilt of the target or the nature of the crime. If so, he is conflating the intrusiveness inquiry with the justification inquiry, which is based on how certain the police are that they will find the evidence they seek. Only after the intrusiveness of a technique *in general* is determined should the analysis move to the circumstances under which it may take place. More is said about that issue below.

B. THE COURTS' CAPACITY TO USE EMPIRICAL RESULTS

Professor Kerr next argues that even if intrusiveness surveys are relevant to expectation of privacy analysis, a requirement that courts rely on them would create nightmares for judges. He writes:

What if the people Slobogin queried have unrepresentative views? What if public opinion varies by state or region or age or race? Can the Court create a constitutional rule based on survey results without even knowing the actual questions asked? And what if public opinion changes over time—should the courts change the rule when public opinion changes, such as after a terrorist attack or the release of an influential movie about surveillance? How would judges know when public opinion has changed? And how should courts reconcile dueling surveys? . . . Slobogin's method requires courts to have answers to all of these questions.⁵⁵

These are great objections, and worthy of answers. In *Privacy at Risk*, I emphasized that before courts rely on survey results, those results must be replicated (as has already occurred with respect to my first study).⁵⁶ Unless and until robust results are achieved, constitutional doctrine should not change. But if, as seems increasingly likely, surveys indicate that most people perceive transaction surveillance of financial, medical, and other records to be as intrusive as a search of a car, and systemic public surveillance to be more intrusive than a roadblock, then courts purporting to apply the societal expectation of privacy test should not be able to ignore these results simply because evaluating empirical information is difficult. Courts deal with survey data in many different contexts. Professor Swire notes, for instance, that consumer surveys routinely in-

55. Kerr, *supra* note 6, at 964.

56. Using a more sophisticated methodology, Professors Blumenthal, Adya, and Mogle conducted a study that relied on the same scenarios used in our study and found that their “[data] are quite consistent with [Slobogin and Schumacher’s] results; each of our samples correlated highly with their overall data.” See Blumenthal et al., *supra* note 53, at 345. However, they also found that context affected their results. See *id.* at 348–51.

fluence trademark cases.⁵⁷ Courts are capable of sorting through data about intrusiveness as well.⁵⁸

As to Professor Kerr's important queries about how the courts should deal with changes in public attitudes, several responses are worth making. I suggested in *Privacy at Risk* that society's views about relative intrusiveness are unlikely to budge once the Court sets them as the Fourth Amendment standard.⁵⁹ The Court's pronouncements would not only reinforce those views but also inhibit the introduction of techniques that courts have declared intrusive, and thus make public inurement to them less likely. That is not to deny the validity of Professor Kerr's supposition that a terrorist attack might affect public attitudes about intrusiveness. My second and third studies, conducted after September 11, 2001, found reduced intrusiveness ratings compared to those assigned to similar scenarios in the first, pre-9/11 study, probably because post-9/11 participants were willing to give up civil liberties in exchange for more security.⁶⁰ But, again, the hierarchy stayed the same: almost *all* scenarios received lower intrusiveness ratings in the later studies, meaning that the findings most relevant to proportionality analysis remained stable.⁶¹

I do not mean to suggest by this discussion that societal views about relative privacy could never change (the younger generation's flirtation with exhibiting their personal lives on phone video and Facebook suggests as much).⁶² But if these

57. Swire, *supra* note 7, at 757.

58. Much of the empirical information could be provided in briefs. See John Monahan & Laurens Walker, *Social Authority: Obtaining, Evaluating, and Establishing Social Science in Law*, 134 U. PA. L. REV. 477, 496 (1986) ("If the research is more analogous to law than to fact, the parties should present the research to the court in the same manner that they would offer legal precedents, that is, in written briefs rather than by oral testimony."). Moreover, indeterminate empirical results are not necessarily irrelevant. As Professor Faigman has noted, "[t]he empirical uncertainties of factual statements are as important as the statements themselves and should be part of the legal calculus." FAIGMAN, *supra* note 9, at 162.

59. SLOBOGIN, *supra* note 1, at 114.

60. For instance, the roadblock scenario received an MIR of 46 and a body cavity search at the border an MIR of 90 in the 1993 study, compared to an MIR of 35 for the roadblock and a 75 for the body cavity search in the 2002 study. Compare Slobogin & Schumacher, *supra* note 30, at 738–39, with SLOBOGIN, *supra* note 1, at 112.

61. Compare SLOBOGIN, *supra* note 1, at 112, 184, with Slobogin & Schumacher, *supra* note 30, at 738–39 (showing pre-9/11 and post-9/11 scenario hierarchies that are very similar).

62. See, e.g., Janet Kornblum, *Privacy: That's Old-School: Internet Gener-*

views do undergo a metamorphosis, an intrusiveness-driven Fourth Amendment should (and will be able to) accommodate them. As I stated in *Privacy at Risk*, if society's views did "change substantially—for instance, if twenty years from now, government-run CCTV is seen as much less intrusive than searching foliage in a public park or much more intrusive than a frisk—then Fourth Amendment analysis should probably change with them."⁶³ The next section further explicates this point.

C. THE SOCIETAL EXPECTATION TEST

Even if the various methodological and implementation objections to intrusiveness surveys can be dismissed, Professor Kerr does not think such surveys should govern Fourth Amendment analysis.⁶⁴ He points out that the Supreme Court explicitly relies on the societal expectations of privacy test only in connection with determining when a government action is a search, not when it is establishing the appropriate justification for conduct that has already been denominated a search.⁶⁵ And even in connection with the Fourth Amendment's threshold question, Professor Kerr argues that the analysis should consist of "normative assessments of the costs and benefits of subjecting a legal technique to constitutional regulation," not an assessment of societal expectations of privacy.⁶⁶

On its face, Kerr's proposal ignores precedent—*Katz's* expectation of privacy test—much more forthrightly than Professor Kerr claims that I do.⁶⁷ In any event, privacy cannot be eva-

ation Views Openness in a New Way, USA TODAY, Oct. 23, 2007, at D1 (noting that people today have less concern about privacy in some respects because of familiarity with new technologies).

63. SLOBOGIN, *supra* note 1, at 114. Certainly the Court's views on intrusiveness, and probably society's views as well, have changed in the past, in both directions. Compare *Katz v. United States*, 389 U.S. 347, 353 (1967) (declaring bugging of a phone booth a search), with *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (declaring wiretapping of a phone not a search); compare *Warden v. Hayden*, 387 U.S. 294, 301–02 (1967) (holding seizure of mere evidence permissible), with *Gouled v. United States*, 255 U.S. 298, 309 (1921) (holding seizure of mere evidence not permissible); compare *Hale v. Henkel*, 201 U.S. 43 (1906) (permitting subpoena for business papers), with *Boyd v. United States*, 116 U.S. 616 (1886) (prohibiting seizure of business papers).

64. See Kerr, *supra* note 6, at 960–61.

65. *Id.* at 961.

66. *Id.* at 961 n.14.

67. At one point, Professor Kerr states that my approach would require "a dramatic revision of current doctrine" and then asserts that "[i]t is difficult to justify a revision of current doctrine on the ground that some aspects of cur-

luated “normatively” without inquiring into what people think about it. Reliance on surveys of the type I carried out to establish Fourth Amendment norms does smack of putting search and seizure law up for a vote, which runs against the constitutional grain.⁶⁸ But some sort of mechanism for measuring public attitudes about the invasiveness of government attempts to pry into our lives is crucial if privacy is the appropriate metric. As Robert Post has explained (in a statement I quote in *Privacy at Risk*), the only way to get a sense of what privacy means in this context is to look at “social forms of respect that we owe each other as members of a common community.”⁶⁹ Thus, Post concludes, “there can ultimately be no other measure of privacy than the social norms that actually exist in our civilization.”⁷⁰ We need to be careful about how we measure those norms, but we must measure them if we care about privacy.

Professor Kerr might respond that the Court does not mean what it says when it states that the threshold of the Fourth Amendment is determined by “expectations of privacy.” Rather, this phrase is code that the Justices use to refer to their own balancing of individual interests against the government’s need for evidence of crime.⁷¹ If that is so, on what basis is the Court determining the scope of individual interests at stake in Fourth Amendment cases?

In other work, Professor Kerr has identified three relevant “models” that he says the Court has used to operationalize the *Katz* test.⁷² The “private facts” model, which “asks whether the

rent doctrine require it.” *Id.* at 961. I have to confess I do not understand this argument. First, by investigating society’s expectations of privacy, I am adhering to *Katz*’s original formulation. See SLOBOGIN, *supra* note 1, at 68–69 (quoting Court language that confirms this formulation). Although I am obviously arguing for a different interpretation of that formulation than subsequent Court opinions have given it, scholars routinely argue that the Court is misconstruing its own doctrine, whether the issue is *Miranda*, equal protection, or prior restraint. I am not clear why that is “difficult.”

68. See, e.g., *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 638 (1943) (“One’s right to life, liberty, and property, to free speech, a free press, freedom of worship and assembly, and other fundamental rights may not be submitted to vote; they depend on the outcome of no elections.”).

69. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092 (2001).

70. *Id.* at 2094.

71. Kerr, *supra* note 6, at 961 n.14 (“[T]he Court’s applications [of the expectation of privacy test] generally rely on normative assessments of the costs and benefits of subjecting a legal technique to constitutional regulation.”).

72. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507–19 (2007). Kerr also identifies a fourth model, the “policy

government's conduct reveals particularly private and personal information deserving of protection," is the one that most closely relates to my intrusiveness inquiry.⁷³ Professor Kerr's second model is based on "positive law," to which I have also already alluded as an occasionally good proxy for assessing societal expectations.⁷⁴ Finally, Professor Kerr describes a "probabilistic model," which focuses on the risks of disclosure to others as we go about our daily business.⁷⁵ This model is quite frequently invoked by the Court, in cases stating or implying that when people walk on the public streets, putter about in their yards, engage in activities near their windows, or conduct transactions through banks, they assume the risk that other people, including those who work for law enforcement, will take note.⁷⁶

Although Professor Kerr treats these as three separate models, they all focus on the same metric: intrusiveness. Professor Kerr recognizes this point, albeit inadvertently, in his discussion of each of the three models. For instance, in discussing the private-facts model he states, "[t]he nature of the information obtained by the government is obviously a critical aspect of its invasiveness and need for legal regulation."⁷⁷ Regarding the positive-law model he writes, "[t]he selection of the positive-law model in physical entry cases makes sense: it provides clear and familiar ex ante guidance for police, and in this context it resonates with our intuitions as to what kind of investigative steps are only modestly invasive and what steps are highly invasive."⁷⁸ And in reference to the probabilistic model he states, "social practice will tend to reflect the invasiveness of a particular technique relatively directly: if an unusual technique leads to the discovery of evidence, it is likely that the technique was also unusually invasive."⁷⁹

Just as importantly, all three models—not just the private-facts model—require resort to empirical reality of the sort ob-

model," wherein "[j]udges must consider the consequences of regulating a particular type of government activity, weigh privacy and security interests, and opt for the better rule." *Id.* at 519. This way of looking at the *Katz* test conflates justification with intrusion and so is not discussed here, but rather is addressed (implicitly) in Part III.

73. *Id.* at 506.

74. *Id.*; see *supra* note 26–28 and accompanying text.

75. Kerr, *supra* note 72, at 506.

76. See *supra* note 25 and accompanying text.

77. Kerr, *supra* note 72, at 534.

78. *Id.* at 544.

79. *Id.*

tained through surveys. Positive law is, of course, the result of a survey, albeit one mediated through the democratic process. And the probabilistic model's assertions about risks of exposure—the risk of our banking transactions being seen by unauthorized persons⁸⁰ or the risk that strangers in airplanes will look down and notice activities in the backyard of a home⁸¹—are also statements about reality that can be empirically investigated.⁸²

In short, judgments about the nature of individual interests at stake in Fourth Amendment cases are not “normative” in the legal sense, as Professor Kerr asserts,⁸³ but inevitably based on facts relating to intrusiveness. In his recent book, *Constitutional Fictions: A Unified Theory of Constitutional Facts*, Professor David Faigman demonstrates that a wide range of constitutional jurisprudence—in cases involving school desegregation, abortion, preventive detention, and search and seizure—is replete with factual assumptions.⁸⁴ Unfortunately, courts, like Professor Kerr, do not always admit or recognize that reality.⁸⁵ As Professor Faigman notes, “[f]acts for the Court are a constituent part of the interpretive exercise. They are not so much discovered as created.”⁸⁶

Professor Kerr provides an example of this phenomenon toward the end of his review where he argues that, even if relative intrusiveness is the correct test, there is a much easier way

80. *Cf.* *United States v. Miller*, 425 U.S. 435, 443 (1976) (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

81. *Cf.* *California v. Ciraolo*, 476 U.S. 207, 223 (1986) (Powell, J., dissenting) (“[T]he actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent.”).

82. Indeed, my research suggests that the probabilistic model coincides with the notion of how invasive an investigative technique is perceived to be. For instance, the fact that my survey participants gave an MIR of 80.3 to the perusal of bank records scenario, SLOBOGIN, *supra* note 1, at 184, and an MIR of 50 to helicopter overflights of backyards, *id.* at 112, can be read to indicate that they do not assume such records are routinely made available to third parties or that such flights are common.

83. *See* Kerr, *supra* note 72, at 523 (stating that the private-facts model “requires a normative assessment of the ‘privateness’ of the information”).

84. FAIGMAN, *supra* note 9, at 1–3 (speaking of the “pervasiveness of factual issues in constitutional cases”).

85. *Id.* at xii.

86. *Id.* at 15.

to implement it than through consulting surveys.⁸⁷ In support of that view, he describes a series of opinions from the New Jersey Supreme Court holding that bank, phone, and ISP address records are protected under New Jersey's constitution because they are associated with a reasonable expectation of privacy.⁸⁸ Without endorsing those results, Professor Kerr notes that they are similar to those I might reach, but states the way the court reached it—through assumptions about what people regard as private—is preferable to my empirical method, because it “offers a more direct and simple path”⁸⁹ than reliance on “public opinion surveys that courts are ill suited to apply and interpret.”⁹⁰

The New Jersey Supreme Court's method surely is simpler, but it is the same suspect method on which the Supreme Court has relied in coming to the opposite conclusion: judicial fiat. Other than referring to precedent, the New Jersey court's reasoning in these cases consists of guesses about people's expectations in dealing with banks, ISPs, and phone companies and descriptions of the types of information the government can obtain from their records.⁹¹ Moreover, these guesses appear to be wrong.⁹² The court concluded that these records, although protected by New Jersey's search and seizure provision, can be obtained via a grand jury subpoena simply on a showing of relevance,⁹³ which in New Jersey means that the documents need merely “bear *some* possible relationship, however indirect, to the . . . investigation.”⁹⁴ That conclusion would be inconsistent with proportionality analysis if findings like those I have obtained are replicated. My research indicates that most people

87. Kerr, *supra* note 6, at 964–66.

88. *Id.* at 965–66.

89. *Id.* at 965.

90. *Id.* at 966.

91. See, e.g., *State v. Reid*, 945 A.2d 26, 33 (N.J. 2008) (noting that users of the Web “have reason to expect that their actions are confidential”); *State v. McAllister*, 875 A.2d 866, 874 (N.J. 2005) (“[B]ank customers voluntarily provide their information to banks, but they do so with the understanding that it will remain confidential.”); *State v. Hunt*, 450 A.2d 952, 956 (N.J. 1982) (“From the viewpoint of the customer, all the information which he furnishes with respect to a particular call is private.”).

92. See *SLOBOGIN*, *supra* note 1, at 184 (indicating a high MIR for transaction records); see also *infra* note 95 and accompanying text.

93. See *Reid*, 945 A.2d at 35–36.

94. See *In re Grand Jury Subpoena*, 401 A.2d 258, 259 (N.J. Super. Ct. App. Div. 1979) (per curiam) (quoting *In re Grand Jury Subpoenas*, 391 F. Supp. 991, 995 (D.R.I. 1975)).

associate bank, phone, and ISP records with a high degree of privacy, on par with intrusions that the Supreme Court has held require reasonable suspicion or probable cause.⁹⁵

To this conclusion, Professor Kerr might raise his previously noted objection that the Supreme Court has never formally applied societal expectation of privacy analysis to police conduct that has already been designated a search.⁹⁶ While that is technically correct, in fact the Court routinely modulates the degree of justification required for a search based on relative intrusiveness. As mentioned above, scores of Court decisions have done so since *Katz v. United States* established the reasonable expectation test.⁹⁷

The New Jersey Supreme Court's decisions on transaction surveillance provide one further example of that phenomenon. The plaintiffs in that court's most recent transaction surveillance case, involving subscriber information held by ISPs, argued that because previous case law had established that relatively unrevealing utility records could be obtained with an *ex parte* subpoena, something more should be required in order to obtain subscriber information.⁹⁸ The court disagreed, not because it rejected the factual premise that ISP records are more private than utility records, but rather because it had already held that accessing *bank* records only requires a subpoena:

Utility records expose less information about a person's private life than either bank records or subscriber information. But we see no material difference between bank records and ISP subscriber information and decline to treat them differently. They reveal comparably detailed information about one's private affairs and are entitled to comparable protection under our law.⁹⁹

Although I think the court's ultimate holding (allowing the government to obtain ISP information via subpoena)¹⁰⁰ is wrong, the point here is that proportionality analysis based on intrusiveness pervades judicial analysis not only in determining the Fourth Amendment's threshold, but also in determining

95. See SLOBOGIN, *supra* note 1, at 184 (indicating an MIR of 80.3 for bank records, 74.1 for phone records, and 57.5 for electricity records compared to an MIR of 71.5 for a pat-down and 74.6 for search of a car).

96. See Kerr, *supra* note 6, at 951.

97. See *supra* note 37.

98. *Reid*, 945 A.2d at 31; see also *State v. Domicz*, 907 A.2d 395, 404 (N.J. 2006) (requiring a subpoena to obtain utility records).

99. *Reid*, 945 A.2d at 36.

100. *Id.*

how much protection the Fourth Amendment should extend in situations where that threshold is reached.

D. CONCLUDING THOUGHTS ABOUT INTRUSIVENESS

Honest judging would recognize that empirically derived privacy expectations are crucial in determining individual interests in Fourth Amendment cases, at both the threshold level and once conduct has been determined to be a search. On the threshold issue, the Court has adopted a test—based on expectations of privacy that *society* is prepared to recognize as reasonable—that cries out for a factual resolution of the issue, and then has decided that it does not care about the relevant facts. On the issue of how much weight courts should give to individual interests in situations that are clearly searches, once again facts about intrusiveness perceptions should be important, if not dispositive; yet they often are not.

In fairness to the courts and Professor Kerr, these types of facts are not easy to come by. As the New Jersey Supreme Court cases illustrate, it is simpler to be an armchair philosopher than investigate the factual basis of one's assumptions. This is especially true when that investigation requires evaluating scientific evidence, confidence intervals, and measures of statistical significance, an often daunting endeavor for many legally trained individuals.¹⁰¹ There is also the fear of change. As previously noted, if judicial facts are linked to real world perceptions, the basis for judicial decisions can be altered. That changeability threatens the stability of the law.

More cynically, real facts will often get in the way of the results one wants to reach. Professor Faigman conjectures that one reason courts create facts rather than find them is a desire to maintain their power; they believe that allowing empiricists to determine reality would mean surrendering their dominion over the law.¹⁰² In response to this contention, Faigman argues that “fact-finding by fiat” also leads to “the almost certain erosion of the legitimacy of the Court's pronouncements.”¹⁰³ And if,

101. Cf. Joëlle Anne Moreno, *Beyond the Polemic Against Junk Science: Navigating the Oceans that Divide Science and Law with Justice Breyer at the Helm*, 81 B.U. L. REV. 1033, 1081 (2001) (“Legal scholars and practitioners . . . are often confounded by the principles of statistical analysis, risk assessment, probabilistic attribution, and attendant mathematical jargon.”).

102. FAIGMAN, *supra* note 9, at 16 (“An institution that surrenders its authority to define the empirical world loses a considerable amount of its power.”).

103. *Id.* at 18.

as Professor Kerr seems to prefer, courts make a normative assessment of the costs of a search even when those costs have been investigated scientifically, then they are taking on the role of philosopher-kings that Justice Scalia, at least, vehemently believes judges should avoid at all costs.¹⁰⁴

Professor Faigman also reminds us that, even in a more empirically based regime, courts will have plenty of power, because they will still play a crucial role in making normative judgments once the correct facts are found.¹⁰⁵ As I stated in *Privacy at Risk*:

Research such as that described here . . . only provides information concerning society's views about *relative* intrusiveness. It does not tell the Court where to position the Fourth Amendment threshold (e.g., at a mean of 15 or 50 on a 100-point intrusiveness scale). The decision as to the level at which privacy expectations are accorded constitutional protection can still be a judicial, normative one that has precedential impact.¹⁰⁶

That judicial assessment would then set the stage, under the proportionality principle, for determining the type of justification the government must proffer.

III. THE JUSTIFICATION INQUIRY

Recall that under the proportionality principle advanced in *Privacy at Risk*, the government's justification for a search or seizure must be roughly proportionate to its intrusiveness, and that the justification inquiry focuses on how certain police are about whether the search or seizure will produce the evidence they seek.¹⁰⁷ Thus, under proportionality reasoning as I define it, the benefits of a search or seizure should be analyzed solely with reference to the extent to which the police action is likely to yield evidence of wrongdoing, measured in terms of certainty

104. See, e.g., *Stanford v. Kentucky*, 492 U.S. 361, 379 (1989) (Scalia, J.), *abrogated by Roper v. Simmons*, 543 U.S. 551 (2005) (stating, while interpreting the Eighth Amendment, that “[t]o say, as the dissent says, that ‘it is for us ultimately to judge whether the Eighth Amendment permits imposition of the death penalty,’ . . . not on the basis of what we perceive the Eighth Amendment originally prohibited, or on the basis of what we perceive the society through its democratic processes now overwhelmingly disapproves, but on the basis of what we think ‘proportionate’ and ‘measurably contributory to acceptable goals of punishment’—to say and mean that, is to replace judges of the law with a committee of philosopher-kings” (quoting *id.* at 391 (Brennan, J., dissenting))).

105. FAIGMAN, *supra* note 9, at 181 (“Enlightened constitutional practice can be neither solely normative nor exclusively empirical.”).

106. SLOBOGIN, *supra* note 1, at 114.

107. For elaboration of this concept, see *id.* at 37–39.

levels such as probable cause, reasonable suspicion, and the like. The more intrusive searches and seizures would require probable cause or perhaps even something more, whereas less intrusive searches and seizures could be justified on reasonable suspicion or relevance grounds or—if the intrusion is truly minimal—would not require any justification at all.

Professor Kerr argues that “[t]his approach doesn’t work because the government’s amount of proof that a technique will yield evidence *ex ante* fails to correlate well with the degree to which the technique furthers government interests”¹⁰⁸ in two ways. First, “the government’s degree of certainty *ex ante* is different from the likelihood of finding evidence *ex post*.”¹⁰⁹ Second, “the degree of confidence that *some* evidence will be found sheds little light on how much will be found or how helpful the evidence will be.”¹¹⁰ This second criticism is echoed, at least indirectly, by Professor Swire.¹¹¹ I will take up these criticisms in turn, and then end with a discussion of a more general concern of Professor Kerr’s, having to do with whether courts or legislatures are better situated to decide the justification issue.

A. MEASURING CERTAINTY

Professor Kerr points out that, outside of the warrant context (where searches frequently produce evidence), little statistical information about the efficacy of searches and seizures exists.¹¹² From this observation, he somewhat mystically concludes that in most search and seizure situations “we cannot rely on *ex ante* thresholds.”¹¹³ This would be news to the courts, which routinely evaluate the validity of a search or seizure from an *ex ante* perspective, as well as to the average police officer, who on a daily basis decides to stop an individual or search a car based on a belief that he has a fair chance of uncovering evidence of crime.¹¹⁴ These assessments may not be

108. Kerr, *supra* note 6, at 962.

109. *Id.*

110. *Id.*

111. *See infra* text accompanying notes 132–37.

112. *See* Kerr, *supra* note 6, at 962 (citing RICHARD VAN DUIZEND ET AL., THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS, AND PRACTICES 138 tbl.6-2 (1983)).

113. *Id.*

114. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 27 (1968) (“[I]n determining whether the officer acted reasonably in such circumstances, due weight must be given, not to his inchoate and unparticularized suspicion or ‘hunch,’ but to

based on mathematically sophisticated calculations, but the entire edifice of Fourth Amendment law is based on the assumption that courts and police can, to use Professor Kerr's word, "rely" on such determinations.¹¹⁵

At the same time, the government should seek data about possible success rates if feasible to do so. When searches or seizures target specific individuals, such data might be hard to produce.¹¹⁶ But when the government engages in searches or seizures of groups, as it does with roadblocks, drug testing programs, camera surveillance, and data mining, some quantitative estimation of a technique's efficacy (i.e., a success rate or "hit rate") will often be possible, based on past experience.¹¹⁷ In *Privacy at Risk*, I argued that just as intrusiveness can be studied empirically, the justification inquiry can sometimes be quantified where group searches are concerned. Specifically, in group search situations the government should be required (1) to produce more than speculative conclusions about the likely hit rate (what I call "generalized suspicion"), and (2) to show that this hit rate is roughly proportionate to the intrusion visited upon the individuals in the group.¹¹⁸ Just as the courts should not be able to rely on gut reactions in making pronouncements about intrusiveness when better information exists, they should not be able to declare, as the Supreme Court has done repeatedly in its special needs cases, that there is a significant crime problem without even seeking concrete evidence to support the assertion.¹¹⁹

the specific reasonable inferences which he is entitled to draw from the facts in light of his experience.").

115. See, e.g., *New Jersey v. T.L.O.*, 469 U.S. 325, 341–42 (1985) ("Under ordinary circumstances, a search . . . will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the [individual] has violated or is violating . . . the law . . .").

116. But see Max Minzner, *Putting Probability Back into Probable Cause*, 87 TEX. L. REV. 913, 915 (2009) (arguing that success rates of individual officers ought to be factored into the ex ante cause determination).

117. See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 662–63 (1995) (describing significant drug activity among student athletes); *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 608 (1989) (recounting that a large number of train accidents and safety incidents over an eight-year period were caused by drug- or alcohol-impaired employees).

118. SLOBOGIN, *supra* note 1, at 39–44 (discussing levels of justification).

119. See, e.g., *Bd. of Educ. v. Earls*, 536 U.S. 822, 836 (2002) ("We reject the Court of Appeals' novel test that 'any district seeking to impose a random suspicionless drug testing policy as a condition to participation in a school activity must demonstrate that there is some identifiable drug abuse problem among a sufficient number of those subject to the testing, such that testing that group

I may be misunderstanding Professor Kerr's complaint about my approach to the justification inquiry, but he seems to be arguing that one reason *ex ante* certainty levels should not be dispositive of that inquiry is because they make solving crime more difficult. That stance ignores the well-accepted proposition that protecting privacy and autonomy through cause requirements necessitates some sacrifice in law enforcement efficiency.¹²⁰ It also opens the door wide to allowing the government to justify suspicionless or virtually suspicionless investigative efforts on easily made (and made-up) assertions about crime problems, the need for deterrence, and the difficulty of pursuing its goals in any other way.

B. CONTEXT

It is precisely the latter sort of assertion that Professor Kerr thinks *should* be the focus of justification analysis under the Fourth Amendment. The correct measure of the benefits that derive from a search or seizure is not, he says, the extent to which evidence of wrongdoing will be obtained, but rather the more capacious inquiry into "how much the technique helps the government catch and successfully prosecute bad guys in light of how much that successful prosecution deters future wrongdoing, incapacitates wrongdoers, and furthers justice."¹²¹ Elsewhere Professor Kerr states that the proportionality approach is deficient because it "generally does not factor in how much the surveillance solves crime, the seriousness of the crimes that it solves, how much it succeeds compared to alternatives, and how often it targets guilty suspects instead of innocent ones."¹²²

These are all important factors for law enforcement authorities to consider in choosing between constitutionally legitimate law enforcement options. But Professor Kerr is in es-

of students will actually redress its drug problem."); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453-54 (1990) ("[T]he choice among such reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers.").

120. Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) ("In times of unrest, whether caused by crime or racial conflict or fear of internal subversion, this basic law [requiring probable cause for most searches and seizures] and the values that it represents may appear unrealistic or 'extravagant' to some. But the values were those of the authors of our fundamental constitutional concepts.").

121. Kerr, *supra* note 6, at 962.

122. *Id.* at 963.

sence arguing that a highly intrusive search (say, of a house) should be permitted on less than probable cause if it is a particularly effective method of solving serious crime and only affects an unspecified number of innocent people. That type of argument is a recipe for government dragnets and general searches, which is precisely what the Fourth Amendment was meant to prevent.¹²³

Professor Kerr is particularly concerned about the impact the imposition of *ex ante* certainty requirements would have in solving serious crime. For instance, he suggests that the cause required to search a house for evidence of a minor crime should be lower than the cause required to search a house for evidence of a planned terrorist attack.¹²⁴ Based on this example, he concludes that “[t]he government’s interest cannot be measured solely by the chances that some evidence will be discovered; any measurement must consider the importance of the case and how much the evidence will advance that case in light of the alternatives.”¹²⁵

On the precise facts of Professor Kerr’s hypothetical, where government is trying to *prevent* a crime rather than solve one, I agree with him. In *Privacy at Risk*, I explicitly recognized a “danger exception” to proportionality analysis and devote much more attention to it than Professor Kerr suggests in his brief footnote on the topic.¹²⁶ Specifically, the danger exception exists when the government is conducting a search to prevent a significant imminent harm, such as a terrorist act.¹²⁷ This rationale, along with the lesser intrusion idea discussed earlier,¹²⁸ explains the holding in *Terry v. Ohio*, which allowed stops and frisks on reasonable suspicion as a crime prevention measure.¹²⁹ As I suggest in *Privacy at Risk*, this rationale might also justify some of the government’s more aggressive efforts to pro-

123. See *supra* text accompanying notes 1–4.

124. Kerr, *supra* note 6, at 962–63 (elaborating on this example).

125. *Id.* at 963.

126. See *id.* at 963 n.17. But see SLOBOGIN, *supra* note 1, at 26–28, 194, 293 n.99 (elaborating on the danger exception).

127. See SLOBOGIN, *supra* note 1, at 193–95 (discussing the exception in the context of terrorism).

128. See *supra* text accompanying notes 13–18 (explaining the balance between justification and intrusion).

129. *Terry v. Ohio*, 392 U.S. 1, 26–27 (1968) (“[A] perfectly reasonable apprehension of danger may arise long before the officer is possessed of adequate information to justify taking a person into custody for the purpose of prosecuting him for a crime.”).

tect national security¹³⁰—a discussion Professor Swire seems to have missed in indicating that I slight this type of government program.¹³¹

There is a big distinction, however, between reducing certainty requirements because of an imminent danger that needs to be prevented and reducing them because a serious crime has already been committed. Only in the former situation does a true exigency exist. Professor Kerr appears to believe this distinction is not important, since he repeatedly emphasizes the importance of crime seriousness when determining whether a particular search or seizure may take place.¹³² Professor Swire may be making the same point with his suggestion that *Privacy at Risk* should have resorted to the vast literature in this country and in Europe on how proportionality analysis has played out in other constitutional contexts.¹³³ This literature can be read to require, in the search and seizure context, some assessment of the magnitude of the government's interest as well as the probability that it will be achieved.¹³⁴ Thus, Professor Swire may also believe that investigation of a serious crime, outside of the imminent danger context, allows relaxation of the ex ante certainty needed to authorize a search or seizure.

In *Privacy at Risk*, I explicitly dismissed this type of reasoning. First, it ignores Fourth Amendment jurisprudence.¹³⁵ In individual cases, the Supreme Court has rejected the idea

130. SLOBOGIN, *supra* note 1, at 194 (“[C]onsistent with the danger exception described in chapter 2, the showing usually required under proportionality analysis could be relaxed when the government can demonstrate that the data mining is necessary to detect a significant imminent threat [such as terrorist activity].”).

131. Swire, *supra* note 7, at 759 (“Slobogin’s discussion of criminal procedure law does not address the intersection with the growing phenomenon of national security searches and seizures.”).

132. Kerr, *supra* note 6, at 962–63.

133. Swire, *supra* note 7, at 760–63 (“When Slobogin omits reference to the large literature on the Proportionality Principle, he foregoes a major persuasive argument for his proposed reworking of the Fourth Amendment.”). The statement in the text is not meant to deny the validity of Swire’s general point that greater attention to proportionality literature would have improved the book.

134. See, e.g., Vicki C. Jackson, *Being Proportional About Proportionality*, 21 CONST. COMMENT. 803, 807 (2004) (noting that one version of proportionality analysis “turns on an evaluation of the importance of the objective measured against its infringing effects on protected rights”).

135. When the search or seizure is of a group, rather than of an individual suspect, the Court’s analysis is somewhat different. See *infra* text accompanying notes 147–57.

that “the seriousness of the offense under investigation itself creates exigent circumstances of the kind that under the Fourth Amendment justify a warrantless search.”¹³⁶ Second, this doctrine is very good policy. A police raid of a home is not rendered less intrusive simply because the police are looking for evidence of a felony rather than evidence of a misdemeanor.¹³⁷ Professor Kerr’s position (if not Professor Swire’s) is analogous to saying that the government’s burden of proof at trial should be reduced in murder cases because such cases involve serious crime.

C. LEGISLATURES V. COURTS

A third point to consider in discussing the justification side of Fourth Amendment analysis is at least obliquely suggested by Professor Kerr in the beginning of his review, when he states that liberal justices might adopt my approach as a way of restoring “what they see as the Court’s rightful place at the center of American privacy law.”¹³⁸ Here he is referring to the idea—one that he has vigorously advocated¹³⁹—that legislatures are much better situated than courts to regulate investigative techniques, especially when, as is the case with physical and transaction surveillance, complicated technology is involved. In general, Professor Kerr is correct on this matter. That is why I state in several places in *Privacy at Risk* that the courts should abstain from mandating the finer regulatory points, but rather should stick to general principles.¹⁴⁰

136. *Mincey v. Arizona*, 537 U.S. 385, 394 (1978).

137. Note, however, that there is some evidence to suggest that where government efforts are viewed as facilitative rather than adversarial, as with health and safety inspections, entries into the home are viewed as less intrusive. See Slobogin & Schumacher, *supra* note 30, at 768 (describing evidence from the intrusiveness study suggesting that “when the motivation of the searchers seems beneficent, the sense of intrusion is lessened”).

138. Kerr, *supra* note 6, at 951.

139. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (“I contend that the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing.”).

140. SLOBOGIN, *supra* note 1, at 75–78 (discussing a legislative approach to surveillance of the home); *id.* at 118–19 (discussing “constitutional roadmapping” in which courts lay out basic principles with legislatures filling in the details); *id.* at 201–03 (discussing Kerr’s preference for legislative solutions and concluding that, while the courts must provide guidelines, “more detailed rule-making along the lines suggested here might best be left to Congress”).

But Professor Kerr makes clear in another recent article that he does not think the courts should play even the latter role with respect to transaction surveillance (and thus probably not with respect to public physical surveillance either).¹⁴¹ He believes that subconstitutional protections, like subpoena law, sufficiently curb wanton abuse of the wide-ranging authority the Supreme Court has granted to the government through its Fourth Amendment jurisprudence.¹⁴² Thus, he is not disturbed by the fact that, under existing law, subpoenas can be issued on a simple finding of relevance (and sometimes even less) or the fact that many types of subpoenas can only be challenged by the third-party record-holder, which seldom wants to buck the government's investigative efforts.¹⁴³

Whether or not one believes this statutory law is sufficiently protective of privacy interests in personal information, it is important to remember that given the Court's stance that the Fourth Amendment does not apply to transaction surveillance, even these minimal limitations are not *required*.¹⁴⁴ As we have

141. Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 596–600 (2009).

142. *Id.* at 596–97 (describing statutory substitutes and declaring it a “good thing” that they provide less protection than a warrant).

143. See SLOBOGIN, *supra* note 1, at 169–80 (describing current subpoena-like mechanisms and the minimal extent to which third parties contest them). Professor Kerr gives three other reasons for his stance in favor of the Court's current third party doctrine. First, he asserts that regulating transaction surveillance would unfairly disadvantage the government, which before the advent of the phone, the Internet, and other technology could relatively easily figure out with whom we conducted our transactions. Kerr, *supra* note 141, at 573–81. Of course technology has also vastly increased the *government's* ability to acquire transactional information; allowing government to acquire this information without justification would lead to a serious imbalance in the other direction. Second, Professor Kerr argues that we consent to revelation of our transactional information when we give it to institutional third parties. *Id.* at 588–90. That restatement of the Court's assumption-of-risk rationale blinks reality and fails to distinguish between giving information to human third parties, who have an autonomy interest in disclosing information, and institutional third parties, which do not. See SLOBOGIN, *supra* note 1, at 156–60. Third, Professor Kerr argues that any alternative to the Court's third party doctrine would disproportionately harm law enforcement because it will be too onerous or confusing. Kerr, *supra* note 141, at 581–86. I agree with him to the extent we impose the warrant-probable cause template on such searches. One of the advantages of the proportionality approach is that it provides more flexibility, because it permits less intrusive searches and seizures, conducted at early stages of an investigation, on a lesser showing. Professor Kerr's statement that “intermediate standards” are “not possible under the Fourth Amendment,” *id.* at 597, is simply not true.

144. See *supra* text accompanying notes 23–26 (criticizing the limited protection under Fourth Amendment precedent).

seen with National Security Letters, which permitted FBI agents to obtain records without any judicial or prosecutorial check, even the limitations that Professor Kerr is willing to adopt can disappear at the first moral panic—precisely because they are not constitutionally based.¹⁴⁵ Courts and the Fourth Amendment have to provide a legal backstop against these types of circumstances.

In *Privacy at Risk*, I did briefly mention one significant caveat to this position, a caveat that might also alleviate some of Professor Kerr's concern about basing justification solely on certainty levels. Based on an article by Richard Worf,¹⁴⁶ I noted that, where searches and seizures of *groups* are involved—stops at roadblocks, school-wide drug testing programs, data mining, and public camera surveillance—political-process theory might cede authority to the legislature even where no *ex ante* hit rate evidence is adduced.¹⁴⁷ I suggested that, so long as the affected group has access to the political process (i.e., is not a discreet and insular minority) and the authorizing legislation puts sufficient limitations on executive discretion (e.g., requires a search of everyone in the group) rationality review might suffice.¹⁴⁸

In a forthcoming work entitled *Government Dragnets in a Technological Age*, I elaborate on this position, again relying heavily on Worf's work.¹⁴⁹ I acknowledge that legislation, which avoids the process flaws of disparate treatment and overdelegation, deserves deference for two reasons. First, the group affected has had an opportunity to influence the law. Second, legislative bodies are better at figuring out the welfare-maximization questions that arise in determining the deterrent and detection effects of group searches and seizures and alternative methods of controlling crime.¹⁵⁰ At the same time, as po-

145. See SLOBOGIN, *supra* note 1, at 177–79 (describing abuses of National Security Letters). Cindy Cohn has said that National Security Letters should simply be called “letters” because they are often used to obtain information having nothing to do with national security. Cindy Cohn, Legal Dir., Elec. Frontier Found., Panel at the DePaul Law School Conference: Cyberlaw 2.0: Legal Challenges of an Evolving Internet (Oct. 15, 2009).

146. Worf, *supra* note 10, at 119–31 (arguing for deference to legislatures in this area).

147. See SLOBOGIN, *supra* note 1, at 43.

148. *Id.*

149. Christopher Slobogin, *Government Dragnets in a Technological Age*, LAW & CONTEMP. PROBS. (forthcoming 2010) (manuscript at 24–28, on file with author).

150. *Id.* Note also that the primary method of avoiding overdelegation is to

litical-process theory dictates, group searches and seizures that are not authorized by legislation or that are authorized by legislation that is tainted by process flaws should still be subject to strict scrutiny by the courts. I define this scrutiny solely in proportionality/compelling-state-interest terms, without the necessity component that usually accompanies strict scrutiny analysis, not only because proportionality reasoning is focused solely on ex ante certainty levels but because, as Kerr suggests, courts are not good at carrying out the necessity calculus in the criminal context.¹⁵¹

Applying this reasoning to cases the Court has confronted, I conclude in *Government Dragnets* that although some of the group search and seizures the Court has approved (and one it did not)¹⁵² should have been approved, many other programs the Court has sanctioned were defective because they were established either by an executive entity or by legislation that did not impose any meaningful limitations on law enforcement.¹⁵³ Also subject to strict judicial scrutiny would be data mining programs that allow the government to sweep through thousands or millions of records based on vague legislative pronouncements, and public camera systems established at the behest of law enforcement agencies rather than municipal government. Because they are the products of a defective political process, courts should prohibit such investigative techniques unless there is a demonstration of the hit rates required by proportionality analysis.¹⁵⁴

Most importantly for purposes of responding to Professor Kerr's critique, investigative techniques that are not aimed at promoting searches and seizures of groups with political access,

ensure the program applies to all constituents, powerful and disadvantaged alike, which should have an inhibiting effect on casual passage of dragnet programs. See Slobogin, *Data Mining*, *supra* note 30, at 317–38 (describing the near unanimous congressional vote, only two years after 9/11, scaling back the Department of Defense's Total Information Awareness program).

151. Slobogin, *supra* note 149 (manuscript at 30–37).

152. *Chandler v. Miller*, 520 U.S. 305, 308 (1997) (striking down a Georgia statute that required drug testing of all political candidates).

153. See, e.g., *Ferguson v. City of Charleston*, 532 U.S. 67, 76 (2001) (drug-testing program established by local police); *City of Indianapolis v. Edmond*, 531 U.S. 32, 36 (2000) (roadblock policy promulgated by the local police department); *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 447 (1990) (same); *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 608–13 (1989) (drug-testing policy promulgated under statute permitting Secretary of Transportation to “prescribe, as necessary, appropriate rules, regulations, orders, and standards for all areas of railroad safety”).

154. See Slobogin, *supra* note 149 (manuscript at 30–37).

but rather merely facilitate investigation of individuals suspected of crimes, should always be subject to proportionality analysis. That would mean that Professor Kerr's preferred legislation permitting law enforcement access to a suspect's bank or phone records based on a subpoena would not be entitled to rationality review. Rather, they should be analyzed under the proportionality principle.¹⁵⁵

Contrary to Professor Kerr's suggestion, unless political-process theory counsels judicial deference, the mere fact that legislatures are relatively competent at collecting information about technological surveillance (or any other investigative technique) should not immunize their products from constitutional scrutiny. Courts may be relatively poor at constructing complicated legal rules and institutionally ill-equipped to decide how much deterrence is bought with various types of techniques, but they routinely make proportionality assessments in search and seizure contexts.¹⁵⁶ The judiciary is perfectly competent at determining whether the other branches of government have come up with the evidence demanded by the proportionality principle in those situations where it applies.¹⁵⁷

CONCLUSION

Professor Kerr implies throughout his review that the approach advocated in *Privacy at Risk* would be much more appealing to a liberal court than a conservative one because of its insistence that the Fourth Amendment have some impact on surveillance techniques.¹⁵⁸ I am not so sure. Since a proportionality approach would not require probable cause or even reasonable suspicion for minimally intrusive techniques such as brief use of overt public camera surveillance or many types of transaction surveillance, many card-carrying ACLU members may find much to be upset about in my proposals. At the same time, even the "conservative" Justice Scalia has bemoaned intrusive government techniques, like drug testing, that are not

155. *Id.*

156. *See, e.g.,* *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985) (noting that Fourth Amendment analysis requires balancing: "On one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order.>").

157. As Professor Faigman notes, "[w]hile the judiciary may not be as well designed institutionally as the legislative branch to *gather* . . . data, courts are especially well designed to *evaluate* them." FAIGMAN, *supra* note 9, at 133.

158. Kerr, *supra* note 6, at 951, 964 (referring to a future, liberal Court).

justified on some concrete basis.¹⁵⁹ In the original intrusiveness study that I conducted with Joseph Schumacher, we asked participants to indicate where they would place themselves on a due process/crime-control spectrum and found that this designation did not have a significant correlation with intrusiveness ratings.¹⁶⁰ Conservatives as well as liberals are bothered by government intrusions into their privacy.

The moderate approach represented by the proportionality principle has several advantages. As I explained in *Privacy at Risk*, the principle “ameliorate[s] the pressure created by the probable-cause-forever stance without sacrificing the core protection of the Fourth Amendment.”¹⁶¹ Aware that declaring a government action a search would no longer require that probable cause be demonstrated, courts would be more willing to broaden the scope of the Fourth Amendment. Instead of resorting to vacuous “assumption of risk” analysis (Professor Kerr’s “probabilistic model”), they would be more receptive to analyzing search and seizure cases in the terms *Katz* has always stood for: expectations of privacy that society has recognized as reasonable. Along with political-process theory, the proportionality principle would also inhibit suspicionless searches and seizures of groups and thus more effectively counteract pressure, particularly strong since 9/11, to engage in blanket surveillance and other dragnet techniques. But with these caveats, preliminary investigative techniques, including some types of dragnets, could take place in the absence of probable cause, and perhaps even in the absence of reasonable suspicion. To conclude with the same language that ended *Privacy at Risk*: “It is possible to achieve security in our houses, person, papers, and effects from both overweening government officials and those who wish to do us harm.”¹⁶²

159. See, e.g., *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 681 (1989) (Scalia, J., dissenting) (“The Court’s opinion in the present case, however, will be searched in vain for real evidence of a real problem that will be solved by urine testing of Customs Service employees.”).

160. Slobogin & Schumacher, *supra* note 30, at 772–74 (“[C]ontrary to our hypothesis, perceptions of intrusiveness and crime control attitudes were not significantly related.”).

161. SLOBOGIN, *supra* note 1, at 210.

162. *Id.* at 218.