

DO WE NEED A NEW FOURTH AMENDMENT?

*Orin S. Kerr**

PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT. By *Christopher Slobogin*. Chicago and London: The University of Chicago Press. 2007. Pp. xi, 306. \$37.50.

INTRODUCTION

Imagine the year is 2035. The election of Barack Obama in 2008 triggered a quarter century of Democratic Party dominance in American politics. Over time, Reagan and Bush appointees to the Supreme Court retired and were replaced by much more liberal successors. The new Supreme Court majority, led by Chief Justice Harold Koh, is now eager to make some waves. The Justices have set their eyes on the Fourth Amendment: They want to design a new Fourth Amendment that will match their civil libertarian privacy preferences. They aim to restore what they see as the Court's rightful place at the center of American privacy law, and they are looking for a method that combines some traditional principles with a new set of innovations.

In *Privacy at Risk*, Christopher Slobogin¹ proposes a new approach to the Fourth Amendment designed to appeal to such a Court. Slobogin argues that the government should have to justify all types of surveillance with at least some sort of cause. In particular, the Constitution should require the government to justify all investigatory tactics with a sufficient basis to think the tactic will work in light of its perceived intrusiveness. Slobogin calls this the proportionality principle: The more the public views a particular technique as intrusive, the more proof the government must have that the technique will actually yield evidence in order to justify its use in a particular case. *Privacy at Risk* specifically targets two surveillance techniques currently unregulated by the Fourth Amendment: public surveillance, such as closed circuit TV ("CCTV"); and transactional surveillance, such as access to bank, telephone, and other business records. Slobogin explains that under his new approach, public and transactional surveillance would be subject to considerable constitutional regulation. Slobogin then applies his framework to both techniques and proposes a complex set of Fourth Amendment rules for each.

Should the liberal Supreme Court of 2035 adopt Slobogin's proposal? And more broadly, does Slobogin's approach offer a conceptual improvement over the Fourth Amendment we have now? In my view, the answer is

* Professor, George Washington University Law School. Thanks to Professor Slobogin and Jerry Israel for their comments on an earlier draft.

1. Professor of Law, Vanderbilt University Law School.

“no.” Slobogin provides an interesting thought experiment, but I think his approach suffers from two significant flaws. First, his method does not accurately weigh the interests it claims to weigh. Although Slobogin presents his approach as an effort to balance privacy and security interests, neither public perceptions of intrusiveness nor the likelihood that a tactic will yield evidence accurately measures those interests. As a result, the proportionality principle that seems unobjectionable in theory turns out to be rather artificial in application. Second, Slobogin’s results could be reached more easily in other ways. Slobogin’s method is surprisingly complicated. In many cases, it requires courts to master the intricacies of public opinion surveys to determine public perceptions of intrusiveness. It also requires courts to generate a complex set of Fourth Amendment rules to govern different surveillance practices.

For these reasons, Slobogin’s book raises interesting questions but fails to provide useful tools to guide a future rejuvenation of the Fourth Amendment. If a future Supreme Court wants to reconsider privacy rules to extend protection beyond current law, it can find approaches that are more direct and less cumbersome than the one Slobogin has offered.

I. A NEW FOURTH AMENDMENT?

A. Overview

Slobogin's book offers a new conceptualization of the Fourth Amendment rooted in what he calls the proportionality principle: An investigative technique should be permitted under the Constitution only if the strength of the government’s justification for the technique is roughly proportionate to the level of intrusion it causes (p. 21). Slobogin roots this principle in *Terry v. Ohio*² and its pragmatic balancing of law-enforcement and privacy interests. To determine how much justification the Fourth Amendment requires, Slobogin argues, courts should assess the intrusiveness of the investigatory technique and then set a proportionate threshold of proof that the government must show (p. 17). The more intrusive the technique, the higher must be the degree of *ex ante* certainty established before the technique can be used. Moderately intrusive steps might be permitted with a court order merely establishing relevance, while more intrusive steps might be allowed only with probable cause. This case-by-case balancing of interests should replace the bifurcated design of existing Fourth Amendment law that leaves some practices entirely unregulated by the Fourth Amendment and then requires warrants based on probable cause for others (pp. 205–14).

The notion of intrusiveness is central to Slobogin’s proposed reworking of the Fourth Amendment. Slobogin does not define the term, but he argues that intrusiveness should be based heavily on public opinion: Courts should measure intrusiveness based on what the citizenry believes is intrusive (pp. 32–33). Slobogin then suggests two ways for courts to assess societal

2. 392 U.S. 1 (1968).

attitudes toward intrusiveness. First, courts should look to positive law such as property, contract, and tort doctrine for “clues as to what we think is private” (p. 33). When “positive law is ambiguous or does not [directly] address a particular situation,” courts should next turn to surveys and public opinion surveys (p. 33). If public opinion surveys reveal that the public sees a technique as intrusive, then courts should require the government to establish *ex ante* a high degree of probability (such as probable cause) before permitting investigators to conduct that step.³ In some cases the government would need a court order from a judge; in other cases the government would need the appropriate cause but no court order would be required.

Slobogin’s reconceptualization would also restructure Fourth Amendment remedies. Slobogin falls short of flatly rejecting the exclusionary rule, but he argues that a system of civil damages should become the leading remedy for Fourth Amendment violations (p. 216). Because the exclusionary rule ensures that Fourth Amendment issues arise with mostly guilty defendants, judges are more likely to construe the Fourth Amendment narrowly to keep guilty defendants in jail. In contrast, a strong system of civil damages would encourage judges to construe the Fourth Amendment in an appropriately broad way that reflects the real societal costs of pro-government rulings (p. 215). Slobogin suggests a range of reforms to encourage Fourth Amendment civil suits, including liquidated damages, rules against indemnification for reckless violations, and free lawyers for plaintiffs (p. 215).

With this conceptual framework in place, Slobogin applies it to two types of surveillance to build the case for greater legal regulation of those practices. He first considers public surveillance and, in particular, the use of CCTV cameras in public areas. He then considers transactional surveillance such as government access to account records for telephones, banks, and credit cards.

B. Public Surveillance

Existing law offers few if any restrictions on public surveillance such as CCTV. The Fourth Amendment does not apply to surveillance in public, and legislatures have not enacted any meaningful regulation of such surveillance (pp. 89–90). This is misguided, Slobogin contends. Courts should recognize a constitutional right to public anonymity because lack of public anonymity “promotes conformity and an oppressive society” (p. 92). Governmental power to watch us in public can chill our speech, discourage our free spiritedness, and infringe upon our capacity for self-definition (pp. 90–108).

Slobogin then applies his proposed framework to make the case for significant Fourth Amendment regulation of public surveillance. He first looks to positive law to establish the intrusiveness of public surveillance in general and CCTV in particular. Slobogin concludes that the absence of existing legal regulation “probably says little” about public assessments of intrusiveness

3. See pp. 34–35.

(p. 109). The difficulty is that “[n]o entity other than the government engages in concerted, overt surveillance of the public streets using cameras” (p. 109). The lack of legal regulation probably just reflects the fact that such surveillance is rare and has not triggered public outcry. As a result, positive law cannot provide a source for measuring the intrusiveness of public surveillance.

Slobogin next reports on public assessments of intrusiveness by presenting results of a survey he conducted for his book. In the survey, 190 people called for jury duty in Gainesville, Florida were asked to imagine that the government was conducting an investigation of a person who was actually innocent. They were then asked to rate the intrusiveness of a range of different types of investigative techniques used to investigate that innocent person and rank the intrusiveness on a scale from 1 (least intrusive) to 100 (most intrusive) (p. 111). Slobogin took twenty of the twenty-five most relevant scenarios and ranked the different techniques based on their average intrusiveness as reported by the survey participants.

Here is the average intrusiveness of the different techniques, ranked from the least intrusive to the most, with their associated confidence intervals (p. 112):

FIGURE 1
PUBLIC SURVEILLANCE

1. Looking in foliage in park	8 +/-4
2. Conducting health and safety inspection of factory	14 +/-4
3. Monitoring cameras at national monuments	20 +/-7
4. Monitoring cameras at government buildings, airports, train stations	20 +/-7
5. Inspecting a coal mine	25 +/-5
6. Monitoring cameras at stores	26 +/-8
7. Stopping drivers at roadblock for fifteen seconds	35 +/-5
8. Monitoring covert street cameras that have zoom capacity	42 +/-9
9. Flying helicopter 400 feet over backyard	50 +/-5
10. Conspicuously following person down street	50 +/-5
11. Going through garbage cans at curbside	51 +/-5
12. Searching a junkyard	51 +/-5
13. Monitoring overt street cameras; tapes destroyed after ninety-six hours	53 +/-8
14. Monitoring a beeper on a car for three days	63 +/-5
15. Using a device that can see through clothing to detect outline of items	67 +/-5
16. Conducting a pat down of outer clothing; feeling for weapons	68 +/-5
17. Using a video camera to overhear a conversation on the street	70 +/-5
18. Same as 13 above, but tapes not destroyed	73 +/-8
19. Searching body cavities at border	75 +/-5
20. Searching a bedroom	76 +/-5

Slobogin concludes from the survey that CCTV should be subject to some kind of Fourth Amendment regulation (pp. 112–13). He reasons that some kinds of public surveillance by cameras registered a higher level of intrusiveness than some techniques that the Fourth Amendment already regulates (pp. 112–13). For example, the Fourth Amendment regulates health and safety inspections at a factory, which measured an average intrusiveness of only fourteen, and inspections at a coal mine, which averaged a rating of twenty-five (p. 112). CCTV was often seen as much more intrusive: Street cameras where the tapes are retained measured an average intrusiveness of seventy-three. Because survey results show that public surveillance is often perceived as quite intrusive, the Fourth Amendment should protect against its use.

Slobogin then proposes a range of requirements that the Fourth Amendment should impose on CCTV, some of which resemble standards offered by an American Bar Association report for which he served as the reporter.⁴ First, government agencies that want to use CCTV cameras must justify the installation of each individual camera (pp. 120–21). Slobogin looks to the Supreme Court's roadblock cases and finds the analogy between roadblocks and CCTV cameras persuasive; as a result, he suggests, public cameras should be authorized only when roadblocks would be authorized (pp. 120–21). In his view, this means that cameras should be allowed only when there is individualized suspicion, other techniques pose a formidable law-enforcement problem, an immediate hazard to life and limb is present, or else there is a need to obtain information about a serious crime (pp. 120–21).

Slobogin next argues that the Fourth Amendment should impose strict requirements on how government agencies use public-surveillance cameras. Once a camera has been installed, individualized suspicion should be required before a camera is focused on an individual in a way that involves "intense scrutiny" (p. 125). All individuals surveilled should receive notice of the monitoring (pp. 126–27). Surveillance should be terminated when no longer needed: Suspicionless surveillance should be terminated after one minute if no cause develops, and if continued beyond a minute, it should be terminated after five to ten minutes unless probable cause develops or extenuating circumstances exist (p. 128). Agencies should be required to disclose their practices to facilitate oversight (pp. 132–33), and there must be penalties, such as suspension or a dock in pay for employees or injunctive relief, for noncompliance (pp. 133–34).

C. Transactional Surveillance

Transactional surveillance receives similar treatment. Once again, the positive law regulating transactional surveillance is very modest. Fourth

4. See AMERICAN BAR ASSOCIATION, ABA STANDARDS FOR CRIMINAL JUSTICE: ELECTRONIC SURVEILLANCE: PART B: TECHNOLOGY-ASSISTED PHYSICAL SURVEILLANCE (3d ed. 1999), available at http://www.abanet.org/crimjust/standards/taps_blk.html.

Amendment protection is nonexistent, and statutory standards remain low. Slobogin contends that this is a mistake: Third party records can have enormous privacy implications and deserve much higher privacy protection than they currently receive (pp. 139–80).

Slobogin then offers an empirical study to bolster the case for greater transactional surveillance (p. 183). Seventy-six participants received written descriptions of twenty-five scenarios involving different investigative techniques, and they were asked to rate the intrusiveness of the techniques on a scale from 1 to 100. Slobogin then ranked the average intrusiveness of the techniques as follows, with the following confidence intervals (p. 184):

FIGURE 2
TRANSACTIONAL SURVEILLANCE

1. Roadblock	30.2 +/-7.5
2. Airplane passenger lists (data mining)	32.4 +/-8
3. Store patron lists (data mining)	34.1 +/-7.5
4. Criminal/traffic records	36.2 +/-7
5. Anonymous phone, credit card, and travel records (data mining)	38.5 +/-7
6. Corporate records	40.6 +/-7
7. Real estate records	45.5 +/-8
8. ID check and questioning during brief stop	49.1 +/-8
9. Club membership records	49.5 +/-8
10. Phone records (data mining)	50.0 +/-8
11. Electricity records	57.5 +/-8
12. High school records	58.3 +/-9
13. Phone, credit card, and travel records (data mining)	59.7 +/-8
14. Record of specific phone call	59.8 +/-7.5
15. List of food purchases	65.3 +/-7.5
16. Pat down	71.5 +/-7.5
17. Phone records	74.1 +/-7.5
18. Web sites visited	74.4 +/-8
19. Search of car	74.6 +/-7
20. Credit card records	75.3 +/-7.5
21. E-mail addresses sent to and received from	77.1 +/-8
22. Pharmacy records	78.0 +/-7.5
23. Use of snoopware to target subject	79.0 +/-8
24. Bank records	80.3 +/-7.5
25. Bedroom search	81.2 +/-6.5

Slobogin concludes from the survey that transactional surveillance should be subject to Fourth Amendment regulation. Many of the respondents viewed transactional surveillance as more intrusive than roadblocks, patdowns, and searches of cars, all of which are currently regulated by the Fourth Amendment (pp. 183–84). Fourth Amendment law should recognize

these societal attitudes and should regulate transactional surveillance as well (p. 185).

Slobogin then uses the empirical study to generate a framework to govern transactional surveillance under the Fourth Amendment. Slobogin's approach distinguishes between two types of surveillance—target-driven surveillance and event-driven surveillance—and among four types of records—corporate records, public records about individuals such as real estate records, quasi-private records such as utility records, and fully private records such as medical records (p. 183–86). He would then recognize four distinct thresholds the government could use to compel transactional information: subpoenas based on relevance, court orders based on relevance, court orders based on reasonable suspicion (what he describes as *Terry* orders), and warrants based on probable cause (pp. 185–86).

Slobogin then argues that the different types of orders to compel should be constitutionally mandated for different types of records as follows:⁵

FIGURE 3
SLOBOGIN'S TRANSACTIONAL SURVEILLANCE PROPOSAL

TRANSACTION	AUTHORIZATION REQUIRED	THRESHOLD
Corporate records	Subpoena	Relevance
Public records about individuals	Court order	Relevance
Quasi-private records obtained through event-driven surveillance	Court order	Relevance
Quasi-private records obtained through target-driven surveillance	<i>Terry</i> order	Reasonable suspicion
Private records obtained through event-driven surveillance	<i>Terry</i> order	Reasonable suspicion
Private records obtained through target-driven surveillance	Warrant	Probable cause

In Slobogin's view, these thresholds reflect the proper balance of the intrusiveness of different techniques and the government interest in using them.

II. A CRITICAL PERSPECTIVE

Let's go back to the future—specifically, to the hypothetical of the liberal Supreme Court in 2035 that opened this Review. Does Slobogin's framework offer the best path for the hypothetical Supreme Court of 2035 to follow? I think the answer is “no” for two primary reasons. First, Slobogin's approach lacks a strong conceptual grounding: It fights against, rather than follows from, a balancing of privacy and security interests. Few would deny

5. P. 186. Unfortunately, a typographical error in the book has led to the authorization required for private records appearing incorrectly in the summary chart on page 186. I have used a corrected version here.

the need to balance privacy interests and security interests in Fourth Amendment law. But Slobogin's version of the balance proves unsatisfying because the two sides of the equation don't measure the interests accurately. "Intrusiveness" provides a weak proxy for privacy interests, and ex ante certainty in court orders provides a poor proxy for security interests.

Second, there are much simpler ways to reach Slobogin's results. Slobogin candidly acknowledges that his framework was drafted with particular results in mind. Slobogin aims to increase privacy protections in the areas of physical and transactional surveillance,⁶ and he is less concerned with how we get there than that we do in fact get there.⁷ But Slobogin's approach is significantly more complicated than it needs to be. Existing law could be tweaked to achieve Slobogin's desired results without requiring such a dramatic reconceptualization of the Fourth Amendment.

A. A Lack of Balance

1. What Does "Intrusiveness" Measure?

Let's start with the notion of intrusiveness, which in many ways forms the heart of Slobogin's approach. Slobogin uses public perceptions of the relative intrusiveness of a technique used against an innocent to measure the technique's threat against privacy interests. The more the public views a technique as intrusive, the greater the privacy interests it implicates. But in my view, this framework is incorrect: Public perceptions of intrusiveness when a technique is used against an innocent person bear only a slight connection to the real civil liberties interests raised by a particular law-enforcement technique.

To see why, think carefully about the word "intrusive." The word intrusive suggests interference with the status quo. The more intrusive something is, the more it alters the world that existed before. As a result, police techniques that are common, are expected, or go unnoticed will tend to seem unintrusive. They don't change the status quo very much, if at all. On the other hand, police techniques that are uncommon, unexpected, or high-profile will tend to be seen as intrusive. In a sense, intrusiveness measures surprise: The more surprising a technique is, the more it jolts the status quo, the more it will upset expectations, and the more intrusive it will appear.

In my view, this understanding of intrusiveness explains the results of Slobogin's public opinion surveys. Consider Figure 1, the chart of survey responses involving physical surveillance and video cameras. At the top of the chart, the six least-intrusive scenarios (numbers 1–6) all involve surveillance that is expected and common. We expect safety inspectors to check

6. P. 5 ("The principal thesis of this book is that . . . physical and transaction surveillance techniques must be regulated more extensively than they currently are.")

7. For example, in response to an argument I have made that rule making in this area is best left to Congress rather than courts, Slobogin suggests that congressional rather than constitutional rule making may be acceptable to him if privacy protections are very strong. He writes, "The goal should be meaningful protection of personal information, whatever its source." P. 203.

out factories, we expect stores to have cameras to watch for shoplifting, and we expect the government to have cameras at national monuments. This sort of surveillance is part of our everyday experience. As a result, survey respondents rank it low on the intrusiveness scale.

Moving down the list brings us to techniques that are more uncommon, unexpected, and visible. The techniques in the middle of the chart (numbers 7–13) are generally used at an early stage of an investigation. For example, conspicuously following a person down a street suggests that the government is watching but that it doesn't yet have enough evidence to know exactly what the suspect has done. At the same time, such techniques tend to cast a wide net and don't suggest that the government already believes that the innocent person is guilty. The methods are part of the backdrop of criminal investigations but not part of daily experience. Survey respondents accordingly describe them as moderately intrusive.

The bottom of Figure 1 lists the methods ranked the most intrusive. For the most part, these are techniques that the government uses only after singling out a criminal suspect. For example, everyone knows that the government doesn't search bedrooms of just anyone. Such searches require great effort and target specific individuals rather than large groups. If we posit that the government's target is innocent, as Slobogin required survey respondents to assume, the techniques listed at the bottom of the chart logically become the most intrusive. After all, it is a shocking thing—and we can hope, an uncommon one—for the government to treat an innocent person as a criminal. The same dynamic explains Figure 2, the chart on transactional surveillance: The more unexpected and uncommon the surveillance for an innocent target and the more it wrongly suggests guilt, the more intrusive it becomes to survey respondents.

If I am right about how members of the public gauge intrusiveness, then Slobogin's methodology suffers from an important weakness: Measuring intrusiveness does not actually measure how much a technique infringes on civil liberties. Indeed, whether an investigative technique seems jarring, uncommon, or becomes associated with guilt in the public mind has no obvious connection to the civil liberties threats its use will raise. In general, a technique will threaten civil liberties when it is used in an abusive way by investigators. It might be used in bad faith, such as to monitor political enemies rather than actual crime. Or it might be used when its costs to civil liberties outweigh its benefit to public safety, such as if the police use highly invasive techniques to solve very minor crimes. But these possibilities are only loosely correlated with whether the public sees the technique as jarring.

This is true for three reasons. First, the frequency of a technique simply has no necessary correlation with its threat to civil liberties. Some techniques are uncommon but raise few civil liberties concerns, while others are used widely but are quite troubling to civil liberties. For example, I think roadblocks raise a serious threat to civil liberties: They permit the government to stop travelers and subject travelers to government inspection without any individualized suspicion. Even if they are relatively common,

and do not suggest the guilt of the person stopped, roadblocks nonetheless impose a serious infringement on personal liberty.

Second, public perceptions can be erroneous. Under Slobogin's approach, public perceptions must become enshrined as constitutional law whether they are accurate or not. If the public were to misunderstand the real privacy implications of new technologies, then that's too bad: Their perceptions trump. Even assuming that intrusiveness measures civil liberties interests, Slobogin's approach requires the actual threat of a particular technique to civil liberties to play second fiddle to the public's perception of the threat.

Misunderstandings are particularly likely in the case of technological surveillance like CCTV and transactional surveillance. Most people experience technological surveillance in two settings: first, routine commercial settings that they experience firsthand, and second, nonroutine settings of criminal and terrorism investigations that people read about in news reports. Slobogin's surveys suggest that most people are quite comfortable with the former. People often don't fear what they have experienced firsthand and found harmless. But many people are scared of what they don't understand, and many will find reports of new forms of technological surveillance quite unnerving. Media coverage no doubt fuels this perception. Journalists tend to report every technological surveillance story as the arrival of Big Brother, even if that angle is comically incorrect.⁸ As a result, public perceptions of new technological surveillance can be highly inaccurate.

Third, the civil liberties threat raised by a particular technique is a function of its average intrusiveness, which itself is a byproduct of the kinds of cases in which it is used. 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. However, Slobogin's study avoids this: It measures the intrusiveness of techniques only in the hypothetical case of an innocent suspect, avoiding the contextual inquiry into average intrusiveness. For all of these reasons, Slobogin's effort to measure intrusiveness fails to provide a proxy for the civil liberties that he is attempting to measure.

Unfortunately, Slobogin's response to these methodological concerns is only hinted at in the book.⁹ The defense rests largely on the requirements of existing Fourth Amendment doctrine. First, the Supreme Court has mentioned the role of "understandings that are recognized and permitted by

8. A helpful example is the FBI surveillance tool popularly known as Carnivore, which the FBI created to protect privacy when it had obtained court orders from federal judges authorizing surveillance. Of course, the press didn't report it that way. See Posting of Orin Kerr to The Volokh Conspiracy, <http://volokh.com/posts/1106113372.shtml> (Jan. 18, 2005, 23:49 EST).

9. Slobogin's perspective on the methodological issues receives fuller treatment in his 1993 article with Joseph Schumacher that introduced his methodology. See 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, 743-51 (1993).

society” when applying the reasonable-expectation-of-privacy test.¹⁰ According to Slobogin, this reference requires a study of what society understands as intrusive.¹¹ Second, the Supreme Court has suggested that the test for when a person is seized—when a reasonable person in the suspect’s position would not feel free to terminate an encounter with the police—should be measured from the perspective of an innocent suspect rather than a guilty one.¹² According to Slobogin, this means that the Fourth Amendment is properly viewed from the perspective of innocent persons rather than guilty ones.¹³

I find Slobogin’s justification unpersuasive. The first problem is that his proposal itself advocates a dramatic revision of current doctrine. It is difficult to justify a revision of current doctrine on the ground that some aspects of current doctrine require it. Either existing Supreme Court doctrine is binding authority or it is not. And if it is helpful authority in some instances but not others, then some theory is needed to account for when it is helpful. If existing doctrine can impose requirements, why doesn’t it also forbid the revision? Given the policy-driven nature of Slobogin’s proposal, reliance on snippets of existing law to justify a particular approach to reform seems notably out of place.

The second problem is that Slobogin appears to use that existing law out of context. While the Supreme Court has mentioned “understandings that are recognized and permitted by society,” it has done so only in the course of determining what constitutes a Fourth Amendment search.¹⁴ Under Slobogin’s method, however, essentially everything is a search; the real question becomes how serious a search it is, and thus whether it counts as constitutionally reasonable or unreasonable. Similarly, the Supreme Court has applied the perspective of an innocent suspect only in the course of determining when a person is seized. The difference is very important in that setting, as an innocent person is much less likely than a guilty person to feel like a target of police arrest. But why should the distinction carry over to the very different question of whether a Fourth Amendment search is constitutionally reasonable? If the doctrine is to jump from one box to the other, some theory (or at least some argument) is needed to explain why.

10. Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978).

11. Slobogin & Schumacher, *supra* note 9, at 743–51.

12. See Florida v. Bostick, 501 U.S. 429, 438 (1991).

13. See p. 111 (“[The assumption that the target is innocent] is consistent with the Supreme Court’s definition of search and seizure for Fourth Amendment purposes.” (citing *Bostick*, 501 U.S. at 438)).

14. To be clear, I think the Court’s doctrine generally does *not* rely directly on societal standards in applying the reasonable-expectation-of-privacy test. As I have detailed elsewhere, the Court’s applications generally rely on normative assessments of the costs and benefits of subjecting a legal technique to constitutional regulation. See generally Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

2. What Do Certainty Thresholds Measure?

I have similar difficulties with Slobogin's assessment of government interests. In my view, Slobogin's approach does not accurately measure what it purports to measure. Recall that Slobogin argues that the government must justify invasions of autonomy and privacy interests by showing a competing interest in solving crime. Under his approach, the government's interest is established by *ex ante* evidence that the technique will be successful and evidence will be found. A greater invasion of privacy must be justified by a greater showing of evidence: Highly invasive techniques must be justified by probable cause, less invasive techniques by reasonable suspicion, and the least invasive techniques by mere relevance to an investigation (pp. 37–44). The government's degree of certainty serves as a proxy for the degree of the government's interest.

This 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. To see why, consider the government's interests in a criminal investigation. The goal of the criminal justice system is to further the retributive and utilitarian ends of the criminal law.¹⁵ By gathering evidence and catching the bad guy, the government can impose punishment that deters future wrongdoing and furthers the ends of justice. As a result, the proper measure of how much an investigative method furthers the government's interests is 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.

The amount of proof the government has *ex ante* reveals only a very small part of this picture. First, the government's degree of certainty *ex ante* is different from the likelihood of finding evidence *ex post*. For example, studies have indicated that the level of certainty required to obtain a search warrant is different from the likelihood that warrants actually recover evidence.¹⁶ The gap between *ex ante* probability and *ex post* results suggests that we cannot rely on *ex ante* thresholds without some sense of how they actually translate to likelihood of finding evidence. As far as I know, however, no studies have explored this dynamic outside the warrant context.

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. Consider a simple example. A police officer may be highly confident that a particular search will uncover marginally relevant evidence in a very minor case. Maybe the officer knows of a 99 percent chance that a search of a target's home will discover evidence (bolstering an already strong case) that the defendant drove his car slightly over the speed limit. Next, imagine the

15. See generally HERBERT L. PACKER, *THE LIMITS OF THE CRIMINAL SANCTION* 35–61 (1968).

16. See RICHARD VAN DUIZEND ET AL., *THE SEARCH WARRANT PROCESS* 120 tbl.6–2 (1983) (reporting that, in the seven jurisdictions studied, the police seized most or all of the items listed in a warrant 64 to 82% of the time for executed and returned warrants).

officer has only a slight reason to think that another particular search will uncover critical evidence that will prove a case of profound importance. Maybe the officer has learned of a 10 percent chance that searching the target's home will uncover a signed and notarized confession to a string of planned terrorist attacks.

In the example, the search for evidence of speeding will almost certainly lead to evidence. At the same time, a 10 percent chance of cracking a major terrorism case serves the public interest in security vastly more than a near certainty of gaining marginally relevant evidence of speeding. The lesson is that the degree of certainty that a technique will yield evidence and the degree to which the technique will advance government interests will often diverge. The 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.

A recurrent theme of my critique is that a true balancing of interests requires context. To know the costs and benefits of using an investigative method, we need to know the overall threat to civil liberties and how much the technique's use will advance government interests *in the contexts in which the technique will actually be used*. Slobogin's approach tends to strip the techniques of their relevant context. The approach 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.¹⁷ In my view, a genuine proportionality principle must take these factors into account.

The difference has particular relevance in cases of public and transactional surveillance. A pragmatist Supreme Court Justice trying to balance privacy and security interests in the setting of public and transactional surveillance would need to consider how these techniques are used, how often they are abused, and what alternative legal regimes such as statutory protections might regulate them absent constitutional protection.¹⁸ That pragmatic Justice would need to consider the administrability of Fourth Amendment rules in areas of technological change and the usefulness of public and transactional surveillance in advancing government investigations.¹⁹ Existing doctrine leaves room for such decisions, as I have argued in several recent

17. Professor Slobogin briefly suggests that the seriousness of the crime under investigation may be relevant in some cases. In particular, he offers a "danger exception" to the proportionality exception: A public safety risk that is "significant" and "imminent" may lower the thresholds at which action should be permissible. *See* p. 28. However, Professor Slobogin does not develop the point except to say that the border of the exception must be "strictly drawn" to avoid gutting the proportionality principle. P. 28.

18. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (arguing that transactional surveillance should not be subject to Fourth Amendment oversight for these reasons).

19. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857–82 (2004).

articles.²⁰ As a result, existing law sometimes leads the courts to conclude that surveillance steps should not be regulated at all under the Fourth Amendment.

Slobogin's approach largely eliminates this option. It ordinarily takes away the category of surveillance permitted without justification, and it avoids looking at the costs and benefits of different rules governing surveillance techniques in the actual contexts in which they are used. While his approach would move the law in a civil libertarian direction, subjecting all surveillance to judicial oversight, it would result in a less accurate balancing of Fourth Amendment interests than current law.

B. *An Easier Way?*

Slobogin's approach also appears unnecessarily complicated. A Supreme Court eager to achieve Slobogin's results could do so more easily with much less doctrinal reform. The complexity results largely from reliance on public opinion surveys. If the Supreme Court must rest constitutional rules on public perceptions of invasiveness, public opinion surveys used to measure those perceptions must be robust. Survey responses can be highly sensitive to the audience, to the phrasing of the question, and to the timing of the survey.²¹ Results of a survey taken one day, with one audience, with questions phrased in a particular way may not match results from another day, another audience, and another set of questions. Before creating a constitutional rule based on public opinion, the Justices must assure themselves that the known surveys accurately and permanently reflect public opinion.

As a result, Slobogin's method requires judges to become skilled at reading surveys, and knowing when public opinion has been accurately measured and for how long that measurement will remain valid. But can judges do this? Consider Slobogin's survey of transactional surveillance (pp. 183–86). We know that Slobogin surveyed seventy-six people and asked them to rank twenty-five scenarios in order of intrusiveness (pp. 183–86). However, we do not know who the seventy-six people were or how they were chosen. Nor do we know the actual scenarios provided to them: Slobogin summarizes the scenarios but does not include the actual language that the survey respondents were asked to consider (pp. 183–86).

Now imagine that the Supreme Court has decided to adopt Slobogin's approach in a case involving transactional surveillance. Can the Court rely on Slobogin's charts? Is a survey taken by seventy-six people enough? 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

20. See Kerr, *supra* note 18; Kerr, *supra* note 19; Kerr, *supra* note 8.

21. See generally Josine Junger-Tas & Ineke Haen Marshall, *The Self-Report Methodology in Crime Research*, 25 CRIME & JUST. 291 (1999).

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? If the constitutional result depends on survey results, can the government simply conduct a new survey, rely on the results, and then insist on new constitutional rules? Slobogin's method requires courts to have answers to all of these questions.

Even if courts can answer such questions, there are much easier ways to reach similar results. The Supreme Court of New Jersey's approach to transactional surveillance offers a helpful illustration: That court has regulated transactional surveillance under the New Jersey Constitution in ways that provide results similar to what Slobogin wants without reliance on public opinion surveys. If the U.S. Supreme Court wants to adopt Slobogin's results, the New Jersey Supreme Court's example would provide a simpler and more direct approach than Slobogin's own.

The New Jersey court regulates transactional surveillance by making two basic moves. First, the court rules that the practice falls under the state constitution. Thus, the New Jersey court has held that government access to bank records,²² phone records,²³ and Internet Service Provider records of IP addresses²⁴ are protected by a reasonable expectation of privacy under New Jersey's version of the Fourth Amendment. This step is straightforward, as it largely tracks the dissents in analogous U.S. Supreme Court cases.²⁵ The second step is more creative. The court applies a balancing test that considers "the type of protection"²⁶ that should be afforded "in the face of legitimate investigative needs"²⁷ that "will arise [and] justify State intrusion upon that interest."²⁸ The inquiry is expressly normative, weighing the public interest in investigative needs against the public interest in privacy in light of then-existing technology. Using this approach, the New Jersey Supreme Court has held that the New Jersey Constitution requires state investigators to obtain a valid grand subpoena for IP addresses and bank records.²⁹

I don't mean to endorse the New Jersey Court's approach as a normative matter. But if a future U.S. Supreme Court were to want to justify Slobogin's results, the method chosen by the New Jersey Supreme Court offers a more direct and simple path. It resembles Slobogin's method at a high level of generality: Like Slobogin's, it regulates what needs to be regulated and does so with as much privacy protection as needed but no more.

22. *State v. McAllister*, 875 A.2d 866 (N.J. 2005).

23. *State v. Hunt*, 450 A.2d 952 (N.J. 1982).

24. *State v. Reid*, 945 A.2d 26 (N.J. 2008).

25. *See, e.g.*, Kerr, *supra* note 18, at 570–71 (detailing the dissenting arguments in the Supreme Court's transactional surveillance cases).

26. *Reid*, 945 A.2d at 35.

27. *Id.*

28. *State v. McAllister*, 875 A.2d 866, 875 (N.J. 2005).

29. *See Reid*, 945 A.2d at 36–37; *McAllister*, 875 A.2d at 875.

But unlike Slobogin's approach, it does not require public opinion surveys that courts are ill suited to apply and interpret.

CONCLUSION

In a revealing passage in *Privacy at Risk*, Slobogin acknowledges that his objections to existing doctrine lie not in the goals of current law but rather in the weighing of interests by recent Justices. "My quarrel with current [Fourth Amendment] law is not with the general approach," he writes, "but with the order and substance" of the specific legal rules that the recent Court has produced (p. 180). The modern Court simply has not valued privacy enough (p. 4). Thus Professor Slobogin's goals are largely results oriented: He aims to "prod"³⁰ courts to "closely watch[]" government surveillance and subject it to more "meaningful regulation" (p. 4).

But if these are Slobogin's goals, his new conceptual framework goes too far. *Privacy at Risk* would do more than simply increase privacy protections: It offers a truly new and original approach to the Fourth Amendment with far-reaching implications. Perhaps a future Court might disagree with the details of existing doctrine. Perhaps that Court might strike a different balance between privacy and security more along Slobogin's preferences. But if so, that Court should proceed cautiously: It should tweak the law, not rework it from first principles. The existing framework of Fourth Amendment protection already offers a more accurate framework to balance privacy and security and is more sensitive to institutional abilities than the new Fourth Amendment that Slobogin proposes. In my view, we are better off with the Fourth Amendment we have now.

30. Univ. of Chi. Press, Christopher Slobogin: Privacy at Risk: Synopsis, <http://www.press.uchicago.edu/presssite/metadata.epl?mode=synopsis&bookkey=236643> (last visited Oct. 20, 2008).