Fordham Law Review

Volume 74 | Issue 2 Article 15

2005

Congress, the Courts, and New Technologies: A Response to Professor Solove

Orin S. Kerr

Congress, the Courts, and New Technologies: A Response to Professor Solove

Cover Page Footnote

Associate Professor, George Washington University Law School. I wish to thank Daniel Solove for his friendship and the many interesting discussions we have had about the subject of this article.

CONGRESS, THE COURTS, AND NEW TECHNOLOGIES: A RESPONSE TO PROFESSOR SOLOVE

*Orin S. Kerr**

INTRODUCTION

In an Article in this issue, my friend and colleague Professor Daniel J. Solove offers an interesting and thoughtful response[1] to a recent article of mine, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution* ("*Constitutional Myths*").[2] In that article, I identified and attempted to explain a growing bifurcation of search and seizure law. Search and seizure law involving traditional facts and stable technologies remains predominantly a matter of constitutional law. As every student of criminal procedure knows, the law emerges in a case-by-case fashion via Fourth Amendment rulings handed down by the U.S. Supreme Court. Fewer realize that the law governing new and rapidly changing technologies has become predominantly statutory. Congress has created what is in effect a parallel Fourth Amendment to regulate many areas of privacy when technology is in flux.

The question is, why does this bifurcated regime exist? *Constitutional Myths* attempted to identify and explain the doctrinal, historical, and functional underpinnings of this growing reality. The first section explained why the bifurcated regime has coexisted with current Fourth Amendment doctrine, and contended that Fourth Amendment rules have remained surprisingly tied to property law.[3] The second section looked at the canonical historical example of wiretapping law, and explained that,

---

* Associate Professor, George Washington University Law School. I wish to thank Daniel Solove for his friendship and the many interesting discussions we have had about the subject of this article.

1. *See* Daniel J. Solove, *Fourth Amendment Codification: A Critique of Professor Kerr's Case for Judicial Restraint*, 74 Fordham L. Rev. 747 (2005).

2. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004) [hereinafter *Constitutional Myths*]. I also wrote a brief reply article to responses from Professors Sherry Colb and Peter Swire, all of which appeared in the same issue. The response articles are Peter P. Swire, Katz *is Dead. Long Live* Katz., 102 Mich. L. Rev. 904 (2004), and Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 Mich. L. Rev. 889, 890 (2004). My short reply article is Orin S. Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 Mich. L. Rev. 933 (2004).

3. *See* Kerr, *Constitutional Myths*, *supra* note 2, at 808-38.

contrary to the common wisdom, wiretapping may be constitutional in theory but remains mostly statutory in fact.[4] The third section considered the relative institutional competence of Congress and the courts in creating rules of criminal procedure when technology is in flux. It contended that Congress's capacity for ex ante rulemaking, expert input, and its freedom from the case or controversy requirement gives it a considerable institutional advantage in this context relative to courts.[5] In light of the institutional competence of legislatures when technology is in flux, I suggested, the bifurcation of criminal procedure may not be a bad thing. Indeed, the former may be the cause of the latter.

In his response, Professor Solove agrees with me that "we are witnessing a codification of the Fourth Amendment"[6] with respect to changing technologies. Despite our agreement on the descriptive question, we diverge on the normative one. While *Constitutional Myths* made the case that the bifurcated regime may be desirable, counseling judicial caution when technology is changing, Solove urges courts to assume "a bold role . . . not a cautious one."[7] He is skeptical that institutional competence is relevant, but claims that, to the extent we accept institutional competence as a factor in normative policymaking, my article fails to make the case that Congress is better suited than the courts to generate balanced and clear protections in this area.[8] According to Solove, courts are just as well suited to generate rules as is Congress.[9] He further claims that courts can play a special role by reviewing statutory privacy laws to determine whether they are sufficiently privacy protective.[10]

In this brief Essay, I hope to defend my claim against Solove's critique. In my view, Solove's response misses the mark in two ways. First, it improperly compares statutory rules as they are with Fourth Amendment rules as Solove wishes them to be. The switch from the descriptive to the normative stacks the deck in favor of judicial rules, diverting attention from the more helpful analytical question. Second, I think Professor Solove under-appreciates the institutional limitations of judicial rulemaking. When technology is changing rapidly, the framework of judicial rulemaking in the context of criminal procedure places courts at a significant informational disadvantage. I conclude by considering Solove's suggestion that courts should subject statutory privacy regimes to a type of facial challenge under the Fourth Amendment. The proposal is an interesting one, but it would force courts to grapple with a long list of quite difficult conceptual problems. Solove may have a solution to these problems, but we would

4. *See id.* at 839-56.
5. *See id.* at 857-86.
6. Solove, *supra* note 1, at 747.
7. *See id.* at 776.
8. *See id.* at 773.
9. *See id.*
10. *See id.*

need to work through them more thoroughly before I could be more optimistic about Solove's proposed solution.

I. NORMATIVE AND DESCRIPTIVE CLAIMS

My primary difficulty with Solove's critique is that his institutional comparison contrasts statutory rules as they are with constitutional rules as he wishes them to be. The critique compares existing statutory law with a hypothetical regime in which the courts "applied" the Fourth Amendment. The catch is that, in Solove's usage, "applying" the Fourth Amendment has a specific meaning: It means labeling all government action a Fourth Amendment search or seizure.[11] To Solove, Supreme Court cases declining to find a reasonable expectation of privacy do not apply the Fourth Amendment and find it imposes no restrictions on police conduct. Rather, such cases reflect a "failure to apply the Fourth Amendment."[12] In Solove's critique, "applying the Fourth Amendment" means imposing a broad warrant requirement. The government must obtain a warrant or fit within a narrow exception to the warrant requirement at essentially every step of every investigation.

A reader familiar with Solove's scholarship knows that this legal framework matches his normative policy preferences. In a recent article, *Reconstructing Electronic Surveillance Law*,[13] Solove offered what he termed a "rather radical"[14] proposal for Congress to enact: "Warrants supported by probable cause should be required [by statute] for most uses of electronic surveillance."[15] He explained that "[t]his should be the general rule, with specific exceptions authorizing access under less strict standards enumerated in the statute"[16] when the invasion of privacy is de minimis.[17] "Additionally," he writes, "all violations should be enforced by an exclusionary rule."[18] Solove justified this approach on a number of policy grounds. He claimed that a broad warrant rule provides the right check on executive power,[19] protects against sweeping dragnet

11. *See id.* at 750 ("'Applicability' refers to those particular law enforcement activities that the Fourth Amendment covers. The Fourth Amendment applies to a law enforcement activity whenever there is a 'search' or a 'seizure.'").

12. *Id.* at 754 ("Some of the federal statutes were enacted in response to the Court's failure to apply the Fourth Amendment to particular situations."). Solove repeatedly describes the holdings of such cases as being "that the Fourth Amendment did not apply" in those circumstances. *Id.* at 752-53 (describing the Court's holding in *Smith v. Maryland*, 442 U.S. 735 (1979); *id.* 752 (describing the Court's holding in *United States v. Miller*, 425 U.S. 435 (1976); *id.* at 750 (describing the holding of *Olmstead v. United States*, 277 U.S. 438 (1928)).

13. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264 (2004).

14. *See id.* at 1266.

15. *Id.*

16. *Id.* at 1299.

17. *Id.* at 1300.

18. *Id.* at 1299.

19. *Id.*

investigations,[20] prevents hindsight bias,[21] and imposes a clear and appropriately flexible standard for law enforcement.[22]

Solove's normative proposal has now reemerged, and forms the basis of his institutional comparison. Solove compares the imperfect statutory law that exists today with a hypothetical legal framework that he greatly admires:

> The current status quo reveals areas where the courts refused to apply the Fourth Amendment and where legislatures became involved. I aim to ask, are we better off with the void as filled by the legislative rules or would we be better off had the Fourth Amendment been interpreted to encompass a particular law enforcement activity? I believe in many instances, the latter would be better.[23]

Unsurprisingly, the existing regime of statutory law fails to measure up to Solove's normative ideal.[24] Existing law contains a number of gaps, Solove explains;[25] it does not offer enough protection[26] and its remedial schemes are inadequate to protect privacy.[27]

I agree with a number of these criticisms, and, as Solove notes, have written articles making similar points.[28] But the imperfections of existing statutory law shed little light on the relative institutional competence of Congress and the courts. To be sure, a comparison of existing statutory and constitutional rules at a particular moment in time could shed some light, if only as a momentary glimpse of the kind of output that statutory versus constitutional regimes are likely to produce in areas of technological change. But Solove does not offer such a comparison. While he laments the withering away of the Fourth Amendment in the first half of his article, the institutional comparison in the second half is limited to contrasting existing statutory law with an idealized model of what he believes the Fourth Amendment should protect.[29]

In my view, the more useful comparison is the one I make in *Constitutional Myths*: a comparison between the institutional ability of Congress and the institutional ability of the courts to generate clear and balanced criminal procedure rules when technology is in rapid flux. The question is not whether any regime is perfect—no laws are—but whether courts or Congress are likely to be in a position to generate better rules of

---

20. *Id.* at 1300.
21. *Id.*
22. *Id.* at 1301.
23. Solove, *supra* note 1, at 762 n.124.
24. *See id.* at 764-66. Solove notes that "[g]iven a choice, it seems that a better balance between privacy interests and law enforcement needs could have been reached if the courts had held that the Fourth Amendment covered a particular law enforcement activity." *Id.* at 766.
25. *Id.* at 763.
26. *Id.* at 765.
27. *See id.* at 763.
28. *See id.* at 767.
29. *See id.* at 751-53.

criminal procedure when technology is changing rapidly. Here, the advantage lies with Congress. When technology is changing quickly, it is ideal for the law to change quickly along with it. Congress can legislate comprehensively, updating rules when technology changes.[30] Congress can enact much clearer rules, soliciting expert input and acting when the technology is still current.[31] The absence of a case and controversy requirement allows Congress to set the best rule for current technology; in contrast, judicial efforts to hit a moving target force the courts to keep the law uncertain to maintain flexibility for future technological change.[32]

II. JUDICIAL INFORMATION DEFICITS

In *Constitutional Myths*, I contended that the richer information environment is one of the several advantages of congressional rulemaking when technology is in flux. Judges generally reach decisions by reading focused legal briefs and cases, picking a side, and then writing up the case based on the record and the arguments of the parties. If the court misunderstands the technology, the court usually will not know that until after the opinion is released and has become binding law. In contrast, Congress can reach decisions by seeking expert input, holding hearings, and receiving responses concerning proposed bills and statutory text. Proposed bills can be scrutinized, commented on, and debated at length from a wide range of perspectives before being passed into law. To borrow from computer software circles, the difference between the two environments is something like the difference between open-source and closed-source software.[33] Judges follow a closed-source model, in which they ask for briefs, hold a short oral argument, and then work in secrecy to produce the outcome. Legislatures follow an open-source model, in which the language and procedure is open to the public.

In my earlier article, I argued that these differences give Congress a considerable advantage when technology is changing:

> Judges struggle to understand even the basic facts of such technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension. Judges generally will not know whether those metaphors are accurate, or whether the facts before them are typical or atypical given the technology of the past or the present. These dynamics make it easy for judges to misunderstand the context of their decisions and their likely effect when technology is in flux. Judges who attempt to use the Fourth Amendment to craft broad regulatory rules covering new technologies run an unusually high risk of crafting rules based on incorrect assumptions of

30. *See* Kerr, *Constitutional Myths*, *supra* note 2, at 871-75.

31. *See id.* at 875-82.

32. *See id.* at 873-74.

33. *See generally* Michael J. Madison, *Reconstructing the Software License*, 35 Loy. U. Chi. L.J. 275, 280-85 (2003) (providing background information on open-source and-closed source software).

> context and technological practice. The context of judicial rulemaking is unusually conducive to high rates of error when technology is in flux.[34]

Professor Solove disagrees. He claims that "[t]here is no reason . . . to assume that the average legislator can better understand technology than the average judge."[35] To Solove, the question boils down to laziness: New technologies are not particularly complex, and any judge or legislator can understand them. My argument in favor of legislative competence is not that legislators are smarter than judges, however, nor that they work harder. Rather, the argument is that the institutional environment of legislative rulemaking will lead to rules that better reflect technology.

To see why, consider the ways in which judges reach decisions in cases with new and developing technologies. For judges and their law clerks, learning a technology is mostly a matter of book learning. They read the parties' briefs, get an idea of some of the technological questions, and then go on Westlaw or Lexis and hunt around for law review articles that discuss the relevant technology. If they find something, they must hope that the information is accurate and still current. It might be, but then it might not be, and judges and clerks are not well positioned to tell the difference. The judge will then write up the opinion in the solitary environment of judicial chambers. The process is solitary and closed.

The legislative process is more open and interactive. Bills are public, and interest groups can track them and comment on them. The press can write stories about proposed bills, drawing public attention and scrutiny to proposed legal rules. Legislative staffers can invite technologists to testify. They can ask for comment from law enforcement and privacy groups, both of which have close connections to technology-savvy advisors. They can float various ideas, and find out which are better and which are worse. Legislatures can also give special significance to the views of particular legislators. A district court judge must reach her decision on her own. In contrast, a large legislative body can allow a few key players to have unusual influence. For example, U.S. Senator Patrick Leahy of Vermont is the most informed voice in the Senate on questions of electronic privacy, and he also tends to be among the most influential. Legislators may recognize Senator Leahy's expertise and defer to his judgment. Reliance on a single group decision may lead to better rules than an individual judgment.

Professor Solove is also unimpressed with the case studies I offer in my article exploring judicial misunderstandings of developing technology that led to counterproductive or unclear rules. My article focused on two cases, *United States v. Bach*[36] and *Trulock v. Freeh*.[37] Solove is unimpressed with *Bach* because the errors in that case were recognized by the appellate court,

34. Kerr, *Constitutional Myths*, *supra* note 2, at 875-76 (footnotes omitted).

35. *Id.*

36. No. CRIM.01-221, 2001 WL 1690055 (D. Minn. Dec. 14, 2001), *rev'd*, 310 F.3d 1063 (8th Cir. 2002).

37. 275 F.3d 391 (4th Cir. 2001).

and the decision was reversed on appeal.[38] Solove suggests that this will happen in most cases, so the risk of judicial error is low. A few more examples can help to illustrate that this is not so. The evidence is anecdotal, of course, but in my view revealing.

One notable case is *United States v. Carey*,[39] in which the U.S. Court of Appeals for the Tenth Circuit created a "special approach" to computer warrants that requires magistrate judges in the Tenth Circuit to approve specific search protocols for searches of computers.[40] If the warrant does not explain the specific search protocols, the evidence is suppressed.[41] The "special approach" is based on an assumption, itself drawn from a 1994 law review article,[42] that it is easy to know ex ante how to minimize the invasiveness of computer searches.[43] Magistrate judges can know the proper protocol, the thinking goes, so they should require them to minimize the invasiveness of the searches. As I detail at length in another article, it turns out that this assumption is false.[44] At least based on current technologies, the computer search process is highly contingent and unpredictable, rendering ex ante protocols largely useless if not counterproductive. Magistrate judges in the Tenth Circuit must include them, however, even though they do not serve the purpose the Tenth Circuit intended. Why? Because one panel read a law review article and reached an incorrect empirical conclusion about the computer forensics process.

Another interesting example is *United States v. Maxwell*,[45] a decision by the Court of Appeals for the Armed Forces. *Maxwell* was the first case that applied the Fourth Amendment to e-mail, and the opinion tried to offer a careful analysis of the relevant technology and how the Fourth Amendment should apply to it. The court held that an America Online ("AOL") subscriber had a reasonable expectation of privacy in his stored e-mail on AOL's servers. The court's rationale was expressly limited to AOL e-mail, however, on the ground that AOL e-mail was different from "Internet" e-mail:

> AOL differs from other systems, specifically the Internet, in that e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank located in Vienna, Virginia.[46]

---

38. Solove, *supra* note 1, at 772.
39. 172 F.3d 1268 (10th Cir. 1999).
40. *See id.* at 1275 n.7.
41. *See, e.g.*, United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930 (D. Utah Apr. 12, 2001) (suppressing evidence due to the absence of a search protocol).
42. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. & Tech. 75 (1994).
43. *See Carey*, 172 F.3d at 1275 (citing Winick, *supra* note 42).
44. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. (forthcoming 2005).
45. 45 M.J. 406 (C.A.A.F. 1996).
46. *Id.* at 417 (citations omitted).

What does this mean? The court seemed to think that AOL is a "system," and "the Internet" is another "system," justifying treating AOL e-mail differently than Internet e-mail. But in fact no such distinction exists. AOL e-mail is a type of Internet e-mail, and all Internet e-mail is privately stored at a "private" computer server somewhere. It seems that the court simply misunderstood how e-mail works. As a result, the meaning of the court's opinion is quite difficult to understand. Is e-mail protected by the Fourth Amendment? Under *Maxwell*, it depends on whether the e-mail is "Internet" e-mail or some other kind of e-mail.

A final example is the Fourth Circuit's decision in *United States v. Simons*.[47] In *Simons*, government investigators retrieved computer files from the computer of a government employee. The files contained child pornography, leading to criminal prosecution. The defendant appealed his subsequent conviction on the ground that the investigators had violated the Fourth Amendment in accessing his files. Here is how the court's opinion described the relevant facts of the search:

> [F]rom his own workstation, [the investigator] examined [the defendant's] computer to determine whether [the defendant] had downloaded any picture files from the Internet; [the investigator] found over 1,000 such files.[48]

This description is ambiguous about a key question: What is the defendant's "computer"? In most modern work environments, an employee will be assigned a personal computer in his private workspace that is connected to a central server. The employee will save some files on the personal computer, and other files on the central server. Did the investigator in *Simons* examine the machine in the defendant's office, or examine the files stored on the server? We don't know. And it turns out to be a very important distinction for Fourth Amendment purposes: The Fourth Amendment rules for computers on a stand-alone personal computer present a very different set of questions from the Fourth Amendment rules for information stored on a network.[49] While there are several possible explanations for this oversight, one very possible one is the court's failure to understand a basic client-server network.

III. THE TROUBLE WITH FACIAL CHALLENGES

Professor Solove ends his essay by turning briefly to his own proposal for how the courts should apply the Fourth Amendment when technology is in flux. If I understand Solove correctly, he wants courts to subject statutory efforts to regulate privacy in new technologies to a type of facial

47. 206 F.3d 392 (4th Cir. 2000).

48. *Id.* at 396.

49. For an introduction to some of those issues, see Brief for Professor Orin S. Kerr as Amicus Curiae Supporting Appellant, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), *available at* http://www.epic.org/privacy/bach/kerr_amicus.pdf.

challenge.[50] Under his approach, courts should not simply require a warrant in every instance. Rather, courts should examine Congress's handiwork and decide "whether Congress's legislation is adequate to satisfy Fourth Amendment requirements."[51] According to Solove, courts should determine whether the statute minimizes dragnet searches, leads to particularized searches, and controls the executive branch sufficiently. If the statute achieves these goals, akin to the kinds of protection that a warrant requirement should afford, courts should uphold it. If the statute does not achieve those goals, courts should invalidate parts or all of it and make the legislature try again.[52]

Unlike Professor Solove, I do not have a specific approach worked out as to how I think the courts should apply the Fourth Amendment to new technologies. I maintain that caution is quite important as a general principle, for the reasons explored in *Constitutional Myths*. Unfortunately, I am not certain about the specifics beyond that (at least yet). For now, I will limit my response to Solove to a narrow point about Fourth Amendment facial challenges. Whatever their possibilities, such challenges raise a number of considerable headaches. Perhaps courts may go that route: The Supreme Court did review a Fourth Amendment statute under a facial challenge once, in *Berger v. New York*.[53] But facial challenges of Fourth Amendment statutes pose a number of complex and formidable questions. Three of these are general difficulties, and the fourth is specific to the problem of rules governing new technologies.

One difficulty with Fourth Amendment facial challenges is finding an appropriate standard to determine how good is "good enough." Solove wants the courts to measure particularization, control, and minimization, but offers no standard to use to know when these goals are sufficiently satisfied. A second and related challenge is knowing how the statute will work in practice. Solove wants courts to determine whether a statute will protect the values he identifies as central to the Fourth Amendment. But courts looking at a statutory scheme generally have no idea how the statute works in practice. In the case of a new statute, no record will exist of how the statute is working in the real world. How are courts supposed to know whether a statutory scheme offers enough protection?

---

50. The difference between facial and as-applied constitutional challenges is complex and slippery, and remains a relatively unexplored fault line in constitutional adjudication. As a general matter, however, an as-applied challenge claims that the government's conduct as permitted by a statute violated the defendant's rights. The violation is specific to the facts of the defendant's case, and the statute is flawed only to the extent it permitted the government to act in that case. In contrast, a facial challenge claims that the defendant was acted upon pursuant to a statute that itself was constitutionally improper. The harm claimed is not a direct violation of the defendant's constitutional rights, but rather a more abstract claim that the defendant was acted upon pursuant to a statute that has some kind of constitutional defect. *See generally* Richard H. Fallon Jr., *As-Applied and Facial Challenges and Third-Party Standing*, 113 Harv. L. Rev. 1321 (2000).

51. Solove, *supra* note 1, at 774.

52. *Id.*

53. 388 U.S. 41 (1967).

Such problems have led the Supreme Court to strongly disfavor facial challenges in the Fourth Amendment context. The key case is *Sibron v. New York*,[54] decided just a year after *Berger*. In *Sibron*, the defendant tried to bring a facial Fourth Amendment challenge to a New York stop-and-identify statute. In an opinion by Chief Justice Earl Warren, the Court declined to accept the facial challenge. The Court's analysis focused on the practical difficulties of conducting a facial review outside of the specific context of evaluating warrant procedures:

> We decline . . . to be drawn into what we view as the abstract and unproductive exercise of laying the extraordinarily elastic categories of [the statute] next to the categories of the Fourth Amendment in an effort to determine whether the two are in some sense compatible. The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case. In this respect it is quite different from the question of the adequacy of the procedural safeguards written into a statute which purports to authorize the issuance of search warrants in certain circumstances. *See Berger v. New York*, 388 U.S. 41 (1967). No search required to be made under a warrant is valid if the procedure for the issuance of the warrant is inadequate to ensure the sort of neutral contemplation by a magistrate of the grounds for the search and its proposed scope, which lies at the heart of the Fourth Amendment. This Court held last Term in *Berger v. New York*, *supra*, that N.Y. Code Crim Proc. § 813-a, which established a procedure for the issuance of search warrants to permit electronic eavesdropping, failed to embody the safeguards demanded by the Fourth and Fourteenth Amendments.
>
> Section 180-a, unlike § 813-a, deals with the substantive validity of certain types of seizures and searches without warrants. It purports to authorize police officers to "stop" people, "demand" explanations of them and "search [them] for dangerous weapon[s]" in certain circumstances upon "reasonable suspicion" that they are engaged in criminal activity and that they represent a danger to the policeman. The operative categories of § 180-a are not the categories of the Fourth Amendment, and they are susceptible of a wide variety of interpretations.[55]

Path dependency provides a third problem. Let's assume that we have found a way to solve the first two problems: We have agreed on a standard to use to measure how good is good enough, and we know exactly how each phrase in the statute works in practice. Courts could give the statute a single up or down vote, upholding or invalidating it en masse. This may be an inefficient way of going about things, though: If the court strikes down the law, the legislature would have to try again, and the process could go on for many years before it enacts a statute that the courts find constitutional. Alternatively, the courts could uphold parts of the statute and strike down

54. 392 U.S. 40 (1968).
55. *Id.* at 59-60 (citations omitted).

other parts. But how can they chose which parts of the statute should be retained or struck down?

Imagine that a statute has ten sections, each of which has a particular impact on privacy that depends in part on the impact on privacy of the other sections. The total number of combinations of different sections of the statute that could be upheld would be expressed mathematically as two to the tenth power, or 1024 different combinations. Let's imagine a court concludes that only two percent of the available combinations will lead to a privacy regime that is sufficiently protective of privacy to satisfy the Fourth Amendment standard. That two percent translates into twenty different combinations. Are courts supposed to list all twenty combinations that may work, and then instruct the legislature to pick which combination it wants? Or should the Supreme Court just pick the one it likes the best among the twenty combinations? If the latter, how are the Justices supposed to decide?

A final reason to be skeptical about facial challenges is specific to changing technologies. As technology shifts, the implications of different legal rules change. A rule that is protective today may not be protective tomorrow, which means that the facial constitutionality of a statute may change over time. If we accept Professor Solove's approach, a statute may be facially constitutional one year, unconstitutional the next, and then constitutional again a year later. Whether a particular law should be upheld would hinge on the precise timing of when the Supreme Court decided to hear the case, and no one would know whether a Supreme Court decision from the past was still binding on legislatures of the present.

Consider the following example. Imagine that the year is 1985, and Congress rewrites the telephone privacy laws from scratch. Congress enacts a new law, the Super Privacy Protection Act ("SPPA"), which creates extremely strong privacy protection for all landline phone communications. Given the state of technology of the day, however, the law does not offer any protection for cordless or cellular phone communications. The Federal Bureau of Investigation can almost never wiretap landline phones, offering very strong privacy protection. In 1985, Justice Daniel Solove would vote to uphold the statute. At that time, cordless and cellular technologies are in their infancy, and the overwhelming proportion of telephone calls are between two landline phones. The SPPA would be seen as broad and privacy protective.

Now fast-forward to the year 2005. Cellular phones have taken over; most people spend as much or more time talking on cell phones than regular phones, and landline phones seem a bit quaint. By 2005, the SPPA no longer seems so super. The statute now exempts half or more communications from its coverage. Is the SPPA facially constitutional? In 1985, Justice Daniel Solove voted to uphold the statute; by 2005, however, Solove will have to change his vote. The statute that was facially constitutional in 1985 will have become facially unconstitutional by 2005, as the number and popularity of cordless and cellular phones increased. At

some point between 1985 and 2005, social practices concerning the use of different types of telephones will have reached the tipping point, rendering the constitutional unconstitutional. Of course, it could tip back: Perhaps a company will introduce a new type of landline phone in 2008 that will become extremely popular, and the SPPA will become constitutional again. So is the SPPA facially constitutional? It depends on when the question is asked.

For all of these reasons, tasking the courts with conducting a rigorous facial review of statutory privacy laws seems quite difficult. It may be possible, but it is a surprisingly complex task. To the extent Solove's proposal is based in part on facial review of privacy statutes, I am skeptical that courts have the capacity to review such statutes in a coherent and principled way.

CONCLUSION

While Professor Solove and I disagree on the normative question of institutional competence, I am delighted that he agrees with my basic descriptive claim. Scholars of criminal procedure tend to think of the field as a branch of constitutional law. To learn the law, we look to the opinions of the Supreme Court that interpret the Fourth, Fifth, and Sixth Amendments. In recent years, however, a statutory equivalent to that regime has begun to emerge. The new law is found more in the United States Code than the United States Reports. For better or worse, statutory law has become a very important source of privacy protection in criminal investigations involving new technologies.