Michigan Law Review

Volume 102 | Issue 5

2004

Technology, Privacy, and the Courts: A Reply to Colb and Swire

Orin S. Kerr
George Washington University Law School

TECHNOLOGY, PRIVACY, AND THE COURTS: A REPLY TO COLB AND SWIRE

*Orin S. Kerr**

TABLE OF CONTENTS

I. REPLY TO PROFESSOR COLB 933
II. REPLY TO PROFESSOR SWIRE 936
CONCLUSION 943

I thank Sherry Colb and Peter Swire for devoting their time and considerable talents to responding to my article, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*. I will conclude with a few comments.

I. REPLY TO PROFESSOR COLB

I very much enjoyed reading Professor Colb's response, although I think at times it misunderstands my article. To clarify, my article does not present a defense of the physical-trespass test in Fourth Amendment law; it does not answer how the Fourth Amendment should apply to a hypothetical brain-wave recorder; it does not argue that the use of property principles is proper in light of originalist or other theories of constitutional interpretation; and it does not claim that there should be no role for the Fourth Amendment in cases that involve developing technologies.[1] My article does not endorse any particular Fourth Amendment test, and has nothing positive to say about the pre-*Jones* physical-trespass approach. I do note that property concepts appear with surprising regularity when judges

* Associate Professor of Law, George Washington University Law School. B.S.E. 1993, Princeton University; M.S. 1994, Stanford University; J.D. 1997, Harvard Law School. — Ed. I thank the editors of the *Michigan Law Review* for giving me the opportunity to reply.

1. *But see* 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. 888, 890 (2004) ("The appropriate question is whether courts have (and whether they ought to have) an obligation to apply the Fourth Amendment to new technologies that could invade privacy without physically trespassing on anyone's private property. Kerr answers this question no . . . ."); *id.* at 888-89 (arguing that my analysis would find no constitutional limitations on the use of a hypothetical "brain wave recorder"); *id.* at 893-94 (arguing that an originalist should interpret the Fourth Amendment as protecting privacy instead of property); *id.* at 901 (describing my normative position as "Kerr's argument that Congress alone should be entrusted with protecting privacy").

interpret the Fourth Amendment. Even when purporting to protect privacy, judges have proven reluctant to deviate from rules based on principles of property law. I make this argument not to endorse property law as a specific normative principle of interpretation, but rather to show how courts have interpreted the post-*Katz* Fourth Amendment in a narrow way with important ramifications for the Fourth Amendment in new technologies. We can debate why this is so: my own suspicion is that judges understand property concepts, but have no common framework for assessing and evaluating privacy claims.[2] Whatever the reason, I have no necessary sympathy for the property approach. I argue that judicial modesty has important virtues in this area, but such modesty can be achieved under a privacy approach as well.[3]

More broadly, my article presents a pragmatic case for judicial caution in the face of rapid technological change, not a defense of property law as a guide for interpreting the Fourth Amendment. It attempts to bring about a greater awareness of the role of statutory privacy laws and the gap between the perception and reality of where privacy rights governing new technologies originate. While scholars focus on the Constitution, the primary privacy protections regulating new technologies have come from Congress. To be sure, this may be the kind of technical and arcane issue that only a law professor could find interesting; as Professor Colb notes, most people care about whether their privacy is protected, not what branch of government confers that protection.[4] But for readers concerned with the structure and contour of privacy laws, I offer a pragmatist case for why we should focus more on statutory protections and less on developing theories of constitutional protection. Fourth Amendment history, doctrine, and the institutional limitations of the courts suggest that the

---

2. Nor do privacy law scholars, for that matter. A rather large percentage of scholarship in the area of privacy law is focused on trying to determine the meaning of privacy. *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) (reviewing the many different understandings of privacy and offering another understanding of what privacy means).

3. Peter Swire's article provides a helpful reminder that a privacy-focused regime does not necessarily lead to a more protective Fourth Amendment regime than a property-focused regime. *See* Peter P. Swire, *Katz* is Dead. Long Live *Katz*., MICH. L. REV. 904, 910 (2004) (arguing that "courts have clung to the property approach to assist the government" and elsewhere has used "[t]he end of the property regime . . . [as] a sword for the government, not a shield of personal privacy"); *see also* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a 'Reasonable Expectation of Privacy?'*, 33 CONN. L. REV. 503, 512-13 (2001) (noting that rights-based conceptions of the Fourth Amendment can lead to broader protections than privacy-based conceptions of the Fourth Amendment). I mostly disagree with the examples Swire relies upon — in particular, I see third-party conveyance cases such as *United States v. Miller*, 425 U.S. 435 (1976), as property cases — but the key point survives that it is possible to have a low-protection privacy regime.

4. *See* Colb, *supra* note 1, at 890.

vital work of protecting privacy in response to technological change will come more from Congress than from the courts.

Colb makes two interesting practical arguments against judicial caution. First, she suggests that judicial deference is unnecessary because even broad judicial privacy protection would not overprotect privacy interests.[5] I understand Colb's argument as one of substantive preference: Colb greatly values privacy, and she calculates that within the set of feasible outcomes more privacy will always be better. Because the courts are unlikely to interpret the Fourth Amendment in a way that provides more privacy than Colb would want, there is no harm if the courts interpret the Fourth Amendment broadly.[6] In my view, the problem with this argument is that it overlooks the difficulties judges face when they craft privacy rules regulating developing technologies. Colb may be right that most judges will not intentionally create rules that are more privacy protecting than she would want. But attempts to protect privacy can backfire, and the context of judicial rulemaking makes missteps particularly likely. As a result, judicially crafted rules are particularly likely to have unintended consequences that even a privacy-valuing observer would dislike. Consider Judge Magnuson's holding in *United States v. Bach*[7] that the Fourth Amendment requires a law-enforcement officer be physically present whenever an internet service provider ("ISP") responds to a search warrant for information on its servers.[8] Judge Magnuson believed that his rule would protect privacy, but his failure to understand the relevant technology created a mismatch between his values and the effect of the resulting rule. If the Eighth Circuit had not overturned his decision, Magnuson's rule either would have slowed investigations considerably without any benefit to privacy or else required police officers to be stationed permanently at ISPs. It is hard to see how either outcome would achieve the goal of protecting privacy.

Colb also argues that Congress may be unable to protect privacy adequately because it may lack the constitutional authority to do so.[9] I think her concern is overstated. Colb's analysis overlooks the expansive reach of the modern Commerce Clause, which provides broad authority to regulate the use of developing technologies. The Supreme Court has interpreted the Commerce Clause to give Congress essentially unlimited power over instruments of interstate

5. *See* Colb, *supra* note 1, at 900.

6. *Id.*

7. No. Crim.01-221, 2001 WL 1690055 (D. Minn. Dec. 14, 2001).

8. *See id.* at *3.

9. Colb, *supra* note 1, at 900-01.

commerce such as communications networks.[10] As a practical matter, this means that Congress can regulate anything connected to the Internet.[11] In addition, lower courts for the most part have allowed Congress to regulate the use of technological instruments that have traveled in interstate commerce prior to their use.[12] For example, use of a camera to create images of child pornography can be regulated by Congress if the camera or film has traveled in interstate or international commerce.[13] This theory permits Congress to regulate the use of nearly every camera and all film. If upheld by the Supreme Court, it would allow Congress to regulate the use of new technologies by state and local governments without any significant limits. Because nearly every technological tool travels across state lines prior to its use, it seems likely based on existing law that Congress can regulate technological instruments under the Commerce Clause.

II. REPLY TO PROFESSOR SWIRE

Professor Swire's thoughtful article offers a series of arguments in support of a strong role for the courts in the protection of privacy involving developing technologies. Swire's first argument is that constitutional privacy protections are necessary because they tend to be stronger than statutory protections. According to Swire, statutory

---

10. Weiss v. United States, 308 U.S. 321 (1939).

11. *See, e.g.*, United States v. Runyan, 290 F.3d 223 (5th Cir. 2002) (finding interstate-commerce element in child-pornography statutes was established when Government linked images to the Internet); United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997) (stating that "[t]ransmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in interstate commerce"); United States v. Thomas, 74 F.3d 701, 706-09 (6th Cir. 1996) (finding interstate-commerce element in obscenity statutes was satisfied where pornographic material sent via the Internet); United States v. Kelly, No. 99-10100-01, 2000 WL 433093, at *2 (D. Kan. Mar. 2, 2000) ("Assuming, as defendant contends, that the facility and means used in this case was a computer with a modem connected via phone lines to the internet, the court concludes that this would clearly be a sufficient nexus to interstate commerce to permit Congress to regulate it.").

12. *See, e.g.*, United States v. Rodia, 194 F.3d 465 (3d Cir. 1999) (upholding 18 U.S.C. § 2252(a)(4)(B) under the Commerce Clause). 18 U.S.C. § 2252(a)(4)(B) (2000) makes it a felony crime to

> knowingly possess[] 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or *which was produced using materials which have been mailed or so shipped or transported*, by any means including by computer, if —
>
> **(i)** the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> **(ii)** such visual depiction is of such conduct . . . .

Id. (emphasis added).

13. *See Rodia*, 194 F.3d at 479 (upholding the statute under the Commerce Clause). *But see* United States v. McCoy, 323 F.3d 1114, 1121 (9th Cir. 2003) (rejecting this theory).

privacy protections are weak and constantly shrinking because the Justice Department controls the legislative process.[14] In contrast, constitutional protections once established remain stable and strong.[15] As a descriptive matter, however, I am not convinced that this is true.

It seems to me that both statutory and constitutional privacy protections on average tend toward a middle ground. Supreme Court decisions establishing strong Fourth Amendment protection tend to be followed by other decisions that temper the initial rule. For example, the Supreme Court's expansion of the exclusionary rule to the States in *Mapp v. Ohio*[16] was followed by a series of decisions minimizing the scope of exclusion, both through good-faith exceptions for warrants[17] and new exceptions to the warrant requirement.[18] Perhaps *Katz* itself is an example: the promise of broad protection in *Katz* was followed by a series of cases construing it narrowly. Through repeated case-by-case decisions, the courts eventually work their way toward some sort of middle ground level of protection.

Contrary to Swire's suggestion, I think that statutory protections also tend to reach a middle ground. If there is a general trend toward lesser statutory protection over time, it is not clear to me. Swire focuses on the fact that Congress did not act on an Internet privacy bill that the House Judiciary Committee approved in 2000, but then passed the USA Patriot Act in 2001. To Swire, this suggests that the legislative process is broken: Congress passed (bad) pro-government legislation but not (good) pro-privacy legislation, leading to less privacy.[19] I find it difficult to draw a lesson from this example. It is worth noting, however, that in Swire's own example the legislative process rejected FBI and DOJ proposals and instead attempted to push the law in a strongly pro-privacy direction. Then, when Congress passed some of the proposals a few years later, it did so only under remarkable circumstances and even then only subject to a sunset provision.[20] If Swire's example is supposed to show a trend toward

---

14. Swire, *supra* note 3, at 919-20.

15. *Id.* at 916 ("Fourth Amendment cases generally offer a sharp yes/no choice between two positions. If the government action is a 'search,' then there are relatively strict rules. A neutral magistrate must decide whether 'probable cause' has been shown.").

16. 367 U.S. 643 (1961).

17. *See, e.g.*, United States v. Leon, 468 U.S. 897 (1984).

18. *See, e.g.*, United States v. Ross, 456 U.S. 798, 809 (1982).

19. *See* Swire *supra* note 3, at 914-15.

20. The pro-privacy bill that Swire mentions is House Bill 5018, the Electronic Communications Privacy Act of 2000, which began as a Clinton administration initiative to update the Internet privacy laws. At that time, the House Judiciary Committee was controlled by Republican Bob Barr. The House Judiciary Committee under Barr transformed the bill. As Swire acknowledges, the committee "overwhelmingly amended [the proposal] in the direction of greater privacy protections." *See* Swire *supra* note 3, at 915. Indeed, the bill that emerged would have shifted the rules rather dramatically in a pro-

lessening privacy protection over time, then it is at best a mixed signal. More broadly, the privacy/security pendulum swings both ways; while there may be times of crisis when the pendulum swings in favor of law enforcement, there are other periods when the pendulum swings in favor of privacy. I would pose this question to Swire: if there is a systematic tendency toward greater surveillance, in what year was privacy most protected by the legislative process? In 1960, when federal law did not forbid wiretapping? In 1970, before FISA was enacted? In 1980, before Congress passed ECPA?

More broadly, comparing privacy protections at different times is more difficult than Swire acknowledges. Law, technology, and social practices interact in complicated ways, and changes in law often respond to changes in technology and social practice. Whether you identify a trend in one direction or another depends in part on whether you look primarily to law in isolation or to the interaction of law with social practice and technology. When emerging technologies make surveillance easier and new legal protections are proposed to counter them, those concerned with privacy can look to technology and social practice and identify a decrease in privacy protections. At the same time, those concerned with public safety can look at the law in isolation and argue that the proposed amendments would impose greater restrictions than ever before.[21] The strategies flip when technology makes surveillance harder, and the issue turns to whether the law should change to restore some lost powers. Law enforcement advocates will tend to look at technology and social practice and see a threat to effective investigations, while privacy advocates will tend to focus on the law in isolation and argue that the proposed amendment would give the government unprecedented new authority.[22] This does not mean it is impossible to make overall measurements of how much

---

privacy direction by raising privacy thresholds and imposing suppression remedies in nearly every context of communications-network crime investigations. For example, the law would have imposed a statutory suppression remedy for intercepted Internet communications, *see* H.R. 5018, 106th Cong. § 2(a)-(b) (2000), raised the threshold for obtaining pen register orders, *see* H.R. 5018 § 4, imposed a warrant requirement on cell phone location information, *see* H.R. 5018 § 7, and extended the warrant requirement from only unopened email to protect all email, *see* H.R. 5018 § 13. This change in direction scuttled the bill: privacy advocates were skeptical because the bill contained some pro-government measures and had been supported by the Clinton Administration, and law-enforcement interests opposed the bill because on the whole it represented a substantial shift toward greater regulation of law enforcement.

21. Consider Swire's discussion of how the law should respond to changes in technology as telephone communications are routed over the Internet. Here he focuses on how advancing technology lessens privacy under the assumption of stable legal rules. *See* Swire, *supra* note 3, at 910-15.

22. We have seen this debate in the context of debates over the use of encryption and the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), codified at 47 U.S.C. §§ 1001-1021 (2000). *See* Dan Eggen & Jonathan Krim, *Easier Internet Wiretaps Sought*, N.Y. TIMES March 13, 2004, at A1.

privacy the law provides at different times. But it does mean that effective comparisons across time are difficult to make.

Swire suggests that statutory protections tend to be weak because the Justice Department controls the legislative process, but fails to identify a persuasive reason why legislators should listen to law-enforcement interests beyond the legislators' interest in satisfying public preferences.[23] Swire draws on the insight that concentrated groups can influence legislation more than dispersed groups,[24] but his concern is addressed by the existence of the influential privacy groups that represent privacy interests in legislative debates in Congress. Groups such as the American Civil Liberties Union ("ACLU"), the Center for Democracy and Technology, and the Electronic Privacy Information Center have considerable sway on Capitol Hill. Mainstream press outlets such as the *New York Times* and the *Washington Post* provide extensive coverage of surveillance and privacy issues that on the whole tends to be wary of government claims and sympathetic to privacy concerns.[25] As I have noted elsewhere, law-enforcement groups and privacy groups are the "two important constituencies that exert a significant influence over Congress in this area."[26] As a practical matter, "few changes in [privacy statutes involving new technologies] can pass through Congress without at least the support of one of these sides and the grudging acquiescence of the other."[27]

I don't wish to paint an overly rosy picture of Congress and the legislative process. At the federal level, the constitutional structure gives law-enforcement agencies an important advantage in congressional negotiations in the form of the presidential veto power.[28] Law-enforcement powers are executive-branch powers, and most presidents will be more willing to expand executive-branch powers

---

23. As Williams Stuntz has argued in the context of substantive criminal law, legislators have legitimate reasons to pay attention to law-enforcement interests:

> That natural alliance [of interest between legislators and law-enforcement groups] should make prosecutors (along with police) a very powerful lobby on criminal law issues. If police and prosecutors want some new criminal prohibition, they likely want it because it would advance their goals. Advancing police and prosecutors' goals usually means advancing legislators' goals as well. Thus, legislators have good reason to listen when prosecutors urge some statutory change.

Willam J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 534 (2001).

24. *Cf.* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971).

25. *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

26. Orin S. Kerr, *Lifting the 'Fog' of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 837 (2003).

27. *Id.*

28. *See* U.S. CONST. art I, § 7.

than reduce them. This dynamic allows presidents to use threats of vetoes (and in unusual cases, vetoes themselves) as tools to block legislative enactments that law enforcement interests view as threatening. If, over time, the veto threat creates an institutional bias in legislation in favor of law-enforcement interests, that may create an important role for the judiciary to play. In effect, the judicial branch could act as a counter to the executive branch; while a President could use the veto power to nullify legislation that excessively narrows executive power, the courts could use their power of judicial review to nullify legislation that excessively broadens it.

One interesting way in which the courts might respond to this dynamic is through statutory rather than constitutional interpretation. When interpreting statutory text, judges could place a 'thumb on the scale' in favor of privacy interests. The combination of judicial caution in the constitutional area and judicial boldness in the statutory area might lead to an optimal solution. Courts could further Fourth Amendment values by protecting privacy through statutory construction. Judicial pressure in statutory cases would keep Congress on its toes, encouraging Congress to enact clear and carefully articulated statutory standards. At the same time, the courts would rest final authority for the scope of privacy protection (within some constitutional bound) with the governmental body best suited to craft privacy protections in new technologies — the legislature.

There is a history supporting just such an approach. Consider the Supreme Court's pro-privacy reading of the first permanent federal wiretapping statute, Section 605 of the Communications Act of 1934.[29] As a textual matter, Section 605 appears to be only a criminal prohibition on private wiretapping; it says nothing about wiretapping by government agents or remedies beyond criminal punishment. In 1937, however, the Court interpreted the law in *Nardone v. United States*[30] to apply to federal officers and also to serve an evidentiary function: according to the Court, the statute made all wiretapping evidence inadmissible in federal court.[31] The Court relied in part on policy considerations:

> For years controversy has raged with respect to the morality of the practice of wire-tapping by officers to obtain evidence. It has been the view of many that the practice involves a grave wrong. In the light of these circumstances we think another well recognized principle leads to the application of the statute as it is written so as to include within its sweep federal officers as well as others.[32]

---

29. 47 U.S.C. § 605 (2000).

30. 302 U.S. 379 (1937).

31. *Id.* at 384.

32. *Id.*

Three years later, the Court expanded that holding in the second *Nardone v. United States*[33] to require the exclusion of "fruit of the poisonous tree" of illegal wiretapping.[34] The Court relied explicitly on the need to protect privacy: "two opposing concerns must be harmonized: on the one hand, the stern enforcement of the criminal law; on the other, protection of that realm of privacy left free by Constitution and laws but capable of infringement either through zeal or design."[35] Just a decade after the Court declined to regulate wiretapping under the Fourth Amendment in *Olmstead*, it opted for aggressive pro-privacy readings of the statutory wiretapping law in the *Nardone* cases.

Other courts have suggested that statutory privacy laws should be construed broadly. Consider a few excerpts from decided cases on the various federal statutory privacy laws. On the Privacy Act: "[T]he Privacy Act's protection is to be broadly construed."[36] On the Wiretap Act: "When considering a statute designed to protect privacy, a court must be reluctant to give expansive reading to the exceptions."[37] On the Electronic Communications Privacy Act: "In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed."[38] Such examples may not in isolation amount to an existing canon in favor of construing privacy statutes broadly. At the same time, such a canon may permit judges to pursue constitutional values without the institutional difficulties of a judge-based privacy regime when technology is in flux.

I am less persuaded by some of the other arguments that Professor Swire makes. For example, Swire argues that the courts should interpret the Fourth Amendment expansively because a strong Fourth Amendment will facilitate the public debate over statutory privacy laws. While congressional debates may sometimes be inspired by constitutional discourse, I doubt that this inspiration hinges on the actual scope of the privacy protection the courts establish or the precise tests that they endorse. After all, Brandeis and Warren's "right to be let alone" is justly celebrated and oft-cited in legislative debates

33. 308 U.S. 338, 341 (1939).

34. *Id.* at 341. This case introduced the "fruit of the poisonous tree" doctrine later adopted in the Fourth Amendment context: "[T]he trial judge must give opportunity, however closely confined, to the accused to prove that a substantial portion of the case against him was a fruit of the poisonous tree." *Id.*

35. *Id.* at 340.

36. Martin v. United States, 1 Cl. Ct. 775, 780 (Fed. Cl. 1983).

37. Jandak v. Village of Brookfield, 520 F. Supp. 815, 820 (N.D. Ill. 1981).

38. McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998).

in favor of increased privacy protections, but no one seems to remember or care that the Supreme Court rejected this approach in *Katz v. United States*.[39]

Similarly, Swire agrees that decisions rejecting Fourth Amendment protection have inspired congressional action in the past, but argues that this is unlikley to occur again in the future.[40] According to Swire, "[t]he triumph of the jurisprudence of *United States v. Miller* and *Smith v. Maryland* suggests little room for new decisions by the Supreme Court that would prompt congressional action."[41] I disagree. *Smith* and *Miller* are hotly contested cases, and even when read broadly they concern only the narrow question of whether third-party possession eliminates Fourth Amendment protection. There are good reasons not to read these cases broadly, among them the recent decision in *Kyllo*.[42] Given this, I think it likely that lower courts will divide on how the Fourth Amendment applies to emerging technologies ranging from computer files to cell phone communications, and that the Supreme Court will eventually address at least some of them. Supreme Court decisions involving any of these technologies will trigger vigorous legislative activity.

Swire is also too quick to dismiss the judiciary's lack of expertise. According to Swire, judges can overcome their institutional difficulties through the use of expert testimony, review of opinion polls, and a close study of relevant statutory privacy laws.[43] None are likely to be helpful. To the extent that Swire imagines judges trying to identify and match constitutional protections to majoritarian preferences, it is unclear why we cannot leave such matters to the elected branches. Expert testimony is unlikely to help much because most Fourth Amendment questions arise in the context of a motion to suppress, rather than a civil trial between well-financed adversaries. Defense attorneys will only rarely find it worthwhile to educate a judge about a technology, and judges will only rarely think that they need to be so educated. Finally, many of the relevant questions are beyond even an expert's knowledge. Such questions include: How will the use of a given technology evolve over time? What would be the consequences of a particular rule? These are not the types of questions that technical experts are well equipped to answer.

---

39. 389 U.S. 347, 350-51 (1967).

40. Swire, *supra* note 3, at 917.

41. *Id.* (citations omitted).

42. Kyllo v. United States, 533 U.S. 27 (2001); *see, e.g.*, Brief of Amicus Curiae Orin S. Kerr, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), *at* http://www.epic.org/privacy/bach/kerr_amicus.pdf (exploring precedents in support of both high Fourth Amendment protection and low Fourth Amendment protection for stored email held by an Internet service provider).

43. *See* Swire, *supra* note 3, at 924.

CONCLUSION

In my article, I predict that we may be moving toward a bifurcated regime in which privacy rights in traditional cases are constitutional but rights in developing technologies are largely statutory. This is an easy prediction to make in some ways, for it is a fairly accurate description of the law today. Professors Swire and Colb each want the courts to reinvigorate the Fourth Amendment, and argue that the courts must and can assume a vigorous role regulating the use of emerging technologies. Whether the courts follow a bold or more modest path, I hope both Colb and Swire will agree that in the foreseeable future Congress will continue to play an essential role. Whatever balance is struck between constitutional and statutory privacy, we should recognize that statutory laws should not remain an afterthought. If scholars wish to remain relevant to the law in action, we should focus on Congress and appreciate the possibilities of statutory law as a source of privacy protection in new technologies.