The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions

Erin Murphy
New York University School of Law

Follow this and additional works at: https://repository.law.umich.edu/mlr

Part of the Fourth Amendment Commons, Law Enforcement and Corrections Commons, Legislation Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://repository.law.umich.edu/mlr/vol111/iss4/1

This Article is brought to you for free and open access by the Michigan Law Review at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.
When criminal justice scholars think of privacy, they think of the Fourth Amendment. But lately its domain has become far less absolute. The United States Code currently contains over twenty separate statutes that restrict both the acquisition and release of covered information. Largely enacted in the latter part of the twentieth century, these statutes address matters vital to modern existence. They control police access to driver’s licenses, educational records, health histories, telephone calls, email messages, and even video rentals. They conform to no common template, but rather enlist a variety of procedural tools to serve as safeguards—ranging from warrants and court orders to subpoenas and demand letters. But across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms.

Despite the appearance of law enforcement exemptions in every generally applicable privacy statute on the federal books, they have garnered virtually no scholarly attention. Privacy scholars have primarily busied themselves with mainstream consumer interests, while criminal justice scholars have chiefly focused on the Fourth Amendment. As a result, these exemptions have gone largely unexamined even as scholars and courts increasingly look to statutory resolutions of Fourth Amendment questions. For example, at least four Supreme Court justices recently suggested in United States v. Jones that the proper scope of some privacy protection might be a topic better left to legislatures than courts.

In response to these concerns, this Article examines, comprehensively and in depth, the operation of privacy statutes with specific regard to law enforcement. In its most elemental form, this Article answers the following questions: what does the federal statutory approach to regulating privacy from the police look like, and in what ways does it mimic, overlap with, or
differ from the Fourth Amendment constitutional approach? In answering these questions, this Article also engages the deeper democratic debate over constitutional versus statutory approaches to controlling the police, using the lessons garnered from examining existing privacy regulations to better inform the secondary argument about who does it best.

**Table of Contents**

**Introduction** .......................................................................................................................... 486

I. Statutory Privacy: Methodology and Observations... 491
   A. Methodology.................................................................................492
   B. Things We Already Know: Federal Statutory Privacy Is Recent and Patchwork.........................493
      1. Statutory Privacy Is a Late Twentieth-Century Invention .........................................................493
      2. Statutory Privacy Protection Is Piecemeal, Sectoral, and Reactive.............................................495
   C. Statutes Tend to Address Technology-Based Concerns..... 499
   D. Law Enforcement Interests Dominate ........................................... 503
   E. Protection Focuses on Individuals, Not Entities, and Especially Members of the Economic Mainstream ...... 507
      1. Individuals, Not Entities ................................................................507
      2. The Poor................................................................................... 508
   F. Law Enforcement Access Provisions Preference Subpoenas over Warrants, and Regulate Not Just Acquisition but Also Use .................................................... 515
   G. Available Remedies in the Event of Violation Differ from the Constitutional Standard of Evidentiary Exclusion ............................................................................. 522
   H. Accountability and Transparency Mechanisms May Be More Readily Available ......................... 525
   I. Federal Privacy Statutes Tend to Set Floors, Rather than Ceilings.................................................. 528
   J. Relative Flexibility of Statutory Enactments ................................................................................. 533

II. Lessons ......................................................................................................................... 534
   A. Myths Dispelled............................................................................ 534
   B. Rethinking the Processes of Privacy .............................................. 537

Conclusion ........................................................................................................................... 545

Appendix ............................................................................................................................ 546

**Introduction**

When we think of privacy protection in the criminal justice system, we think of the Fourth Amendment.¹ But lately its domain has become less ab-

---

¹. See, e.g., RONALD JAY ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 337 (3d ed. 2011) (describing the Fourth Amendment as “the law’s chief source of privacy protec-
solute. The United States Code currently contains over twenty separate statutes that restrict both the acquisition and release of covered information. As might be expected, these statutes were largely enacted in the last third of the twentieth century, and they address matters vital to modern existence—including driver’s licenses, education records, health histories, telephone calls, email messages, and even video rentals. They conform to no common template, but rather enlist a variety of procedural tools to serve as safeguards—ranging from warrants and court orders to subpoenas and demand letters. Yet across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms.

Surprisingly, these law enforcement exceptions, which appear in every generally applicable privacy statute on the federal books, have garnered virtually no scholarly attention. Perhaps this is because so many laws have sprouted up, each addressing atomistic areas of concern, that it is hard enough to consider them collectively, much less focus comprehensively on their relevance to policing. Indeed, federal statutory privacy law today is notoriously “sectoral,” an umbrella under which consumer, corporate, criminal justice, and myriad other interests mingle. Or perhaps the scholarly


indifference reflects an assumption that law enforcement must be accorded some way around otherwise generally applicable protections. After all, the notion that the Fourth Amendment might occasionally wholly bar government access to information has seemingly been abandoned, having instead yielded to the Court’s clear constitutional preference for procedural over substantive rules.4

But these statutes are important. It is no secret that the nature of criminal evidence is changing. Information is less and less likely to be found in physical forms (like a day planner or printed photographs found in the home) than in more abstract places where the strictures of the Constitution play a less defined role (like the bits and bytes of an iPhone, Flickr account, or Gmail calendar server). For this reason, the Fourth Amendment threshold “reasonable expectation of privacy”5 test has been roundly criticized as insufficiently adapted to a world in which our experience of privacy comes packaged in unconventional ways6—whether through the settings of a Facebook feed,7 the anonymity of an urban landscape, or even the mechanical sophistication of scientific diagnostic tools.8

Federal privacy statutes prove interesting for a second reason: they often cooperate with or supplant judicial decisions about the Fourth Amendment, and thus serve as natural subjects for studying institutional design questions.9 That is, some criminal justice scholars commenced, in parallel to questions raised about the impact of technology on criminal procedure, a broader conversation about the allocation of power among the branches. The groundbreaking work of Bill Stuntz critiqued theconstitutionalization of police practices in the Warren Court era as having generated unanticipated and counterproductive consequences, thereby fueling a cavalcade of arguments about the proper reach of courts.10 By thinking of criminal justice as a


5. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). In the wake of Jones v. United States, it is now also clear that the Fourth Amendment applies to any police action that violates a property interest, at least an interest recognizable at the time of the Founding. 132 S. Ct. 945 (2012).


system of interlocking institutions and players, Professor Stuntz also reignited separation of powers and federalism debates about the most legitimate, just, or efficient way to restrain government power.\footnote{11}{See, e.g., David Alan Sklansky, Response, Killer Seatbelts and Criminal Procedure, 119 Harv. L. Rev. F. 56 (2006), 119 HVLRF 56 (Westlaw); Robert Weisberg, Response, First Causes and the Dynamics of Criminal Justice, 119 Harv. L. Rev. F. 131 (2006), 119 HVLRF 131 (Westlaw). For an early entry in this conversation, see Louis Fisher, Congress and the Fourth Amendment, 21 Ga. L. Rev. 107, 165–70 (1986).}

With respect to innovative investigative methods, Orin Kerr has persuasively argued that technological change is best regulated by legislative, not constitutional, pronouncements.\footnote{12}{See id. at 857–87. Professor Kerr’s analysis was most directly addressed in Daniel J. Solove, Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 748, 760–77 (2005), but a handful of other scholars have also weighed in on specific aspects of this debate. E.g., Christopher Slobogin, Privacy at Risk 169–80, 201–03 (2007); Patricia L. Bellia, Designing Surveillance Law, 43 Ariz. St. L.J. 293 (2011); Christopher Slobogin, Government Dragnets, Law & Contemp. Probs., Summer 2010, at 107, 131.} Focusing on the evolution of wiretapping law as a case study, Professor Kerr first observed that courts tend to meet new technological advances with a “relatively modest and deferential Fourth Amendment.”\footnote{13}{See Kerr, supra note 12, at 867–87; supra note 10 (collecting works by William J. Stuntz).}

He then advanced a series of justifications for continued judicial caution, grounded largely in concerns about institutional competence: primarily that legislatures are better poised to gather facts from a wide range of interest groups about emerging technologies and are more adept at amending enactments to keep up with rapid changes, both with respect to a device’s social meaning and its technical specifications.\footnote{14}{See id. at 857–87. Professor Kerr’s analysis was most directly addressed in Daniel J. Solove, Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 748, 760–77 (2005), but a handful of other scholars have also weighed in on specific aspects of this debate. E.g., Christopher Slobogin, Privacy at Risk 169–80, 201–03 (2007); Patricia L. Bellia, Designing Surveillance Law, 43 Ariz. St. L.J. 293 (2011); Christopher Slobogin, Government Dragnets, Law & Contemp. Probs., Summer 2010, at 107, 131.} More generally, critics of expansive constitutionalization of privacy rights have complained that it is, among other things, prone to being antidemocratic, antifederalist, piecemeal, incoherent, impractically opaque, and inflexible (in that precedent is both easy to make and hard to dislodge).\footnote{15}{See, e.g., Donald A. Dripps, Constitutional Theory for Criminal Procedure: Dickerson, Miranda, and the Continuing Quest for Broad-but-Shallow, 43 Wm. & Mary L. Rev. 1, 4}

In contrast, advocates of judicial protection for constitutional interests both dispute the positive claims of legislative superiority and defend the role of the Constitution in safeguarding rights. They note that legislatures have not consistently risen to defend privacy, even in cases where the Constitution has not entered the field or has opened the door to legislative action, pointing to failures in political process.\footnote{16}{See, e.g., Donald A. Dripps, Constitutional Theory for Criminal Procedure: Dickerson, Miranda, and the Continuing Quest for Broad-but-Shallow, 43 Wm. & Mary L. Rev. 1, 4} The reason for legislative
intransigence may vary, and "[j]ust by entering the fray, the Court can make it easier for legislators to stay out." But as David Sklansky has observed, the reason for Congress's failure to act is, in the end, less important than the fact that it does not. Without the Court, important police activities—such as interrogations of suspects—would otherwise go wholly unregulated.

This Article stands at the intersection of these two lines of inquiry—at the juncture between new technology and institutional design. This crossroads has generally been overlooked: perhaps the privacy scholars have simply been too busy with consumer and data privacy to focus specifically on criminal justice, while the criminal justice scholars have been too busy with crime and the Fourth Amendment to focus on general privacy statutes. But the time for greater attention has clearly come.

In United States v. Jones, the Supreme Court confronted its first major technological tool of police investigation in over a decade: a GPS tracking device installed on a private car. Although the plurality opinion—comically, in the minds of some—resolved the issue on the basis of common law ideas of physical trespass, the two concurring opinions both suggested that technological change might require a more nuanced understanding of the scope of the Fourth Amendment.

Given the increasing salience of federal privacy enactments as a primary source of regulation of police investigative activity, it behooves us to look at this body of law more systematically. By comprehensively examining statutory law enforcement exemptions, this Article hopes to enrich our understanding of how legislatures have regulated privacy thus far. In its most elemental form, my questions might roughly be summarized as follows: What does the federal statutory approach to regulating privacy (specifically

---


17. Sklansky, supra note 11, at 64.

18. Peter Swire has argued that rather than spurring legislative activity, a hands-off approach by the courts "would quite likely result in an impoverishment of the legislative debate about privacy and surveillance, and less effective deliberation on what safeguards are appropriate." Swire, supra note 16, at 919–20 (observing that law enforcement views judicial silence as judicial approval, and citing the need for the "moral and political authority of constitutional doctrine").


20. The last major pronouncement along these lines was in Kyllo v. United States, 533 U.S. 27 (2001). But that case, which involved heat sensors used on the exterior of a building, lacked the analogic and rhetorical potential of a case involving GPS trackers, which is more readily likened to a broad range of surveillance technologies.

21. See, e.g., Jones, 132 S. Ct. at 957 (Alito, J., concurring in the judgment) ("Ironically, the Court has chosen to decide this case based on 18th-century tort law.").

22. Specifically, Justice Alito, writing for himself and three others, effectively endorsed Professor Kerr's approach. See id. at 964 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." (citing Kerr, supra note 12, at 805–06)). Justice Sotomayor, writing separately, did not agree as directly, but did warn against "entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse." Id. at 956 (Sotomayor, J., concurring).
Privacy in the Criminal Justice System

from the police) look like, and in what ways does it mimic, overlap with, or differ from the conventional Fourth Amendment constitutional approach? Are the supposed advantages of legislative action in fact evident from the historical record? Are there disadvantages to a judicial approach? What lessons might we take away from a study of federal privacy law to inform how each institutional actor—courts and Congress—ought to approach regulation of policing in the twenty-first century?

To answer these questions, Part I draws on comprehensive research analyzing the salient features of the major privacy enactments. In sum, this Part proffers a series of observations about the nature and character of these statutes and their law enforcement exemptions: 1) they emerged entirely in the late twentieth century; 2) they are sectoral rather than comprehensive in scope; 3) they are largely motivated by technological developments; 4) they primarily protect the privacy of individuals, especially those in the socioeconomic mainstream; 5) they universally provide for law enforcement access to covered material, relying chiefly on more complex devices than a warrant and probable cause; 6) they strongly disfavor the exclusionary rule remedy; 7) they demonstrate no particular commitment to federalist principles; and 8) they show no particular proclivity for keeping current with changing technological conditions.

Part II then tenders an analytic critique of constitutional versus statutory privacy regulation as regards criminal justice and locates that critique within the larger debate over institutional preferences for legal regulation. Among other things, I argue that the variety of procedural tools typically found in statutory regimes, as well as the capacity for legislative enactments to impose more sensitive accountability metrics, suggests that what seems on the surface to be diminished statutory protection for constitutional rights—because such laws typically do not require warrants or application of the exclusionary rule remedy—may mask the actual degree of meaningful protection. The Article closes with some of my own intuitions about the ideal regulatory model for the future.

I. STATUTORY PRIVACY: METHODOLOGY AND OBSERVATIONS

Because close study of twenty-odd federal statutes would make for incredibly dull reading, I do not attempt to replicate my research here. In brief, I examined each statute, including its legislative history and application, through judicial and administrative records. To provide an inkling of some of the major enactments that my research covered, consider the statutes, which are listed in full in the Appendix, of the 1970s, like FCRA (credit records), FERPA (educational records), the Internal Revenue Code ("IRS Code") (tax records), RFPA (bank records), and the Privacy Act (federal government records); the 1980s, like the PPA (journalist notes), CCPA (cable records), SCA/ECPA (electronic records), the Pen Register Act (dialed phone numbers), VPPA (video rental records), and CMPPA (data-mined information); and the 1990s, like DPPA (driver's licensing records), the DNA ID Act (genetic information), HIPAA (health records), COPPA
(records from children’s online activity), VVA (“upskirt” photos), and CDA (online activity). This Part therefore analyzes fifty years of experience with privacy legislation in order to test out some of the theses propounded above. Before beginning, however, a word about my methodology.

A. Methodology

In embarking on this project, I first had to determine which of innumerable statutes should qualify for my study. After all, defining the concept of “privacy” is notoriously difficult, and combing through a code one can find a “privacy” dimension to many enactments. Accordingly, I found it necessary to hone my inquiry in ways that merit brief mention here.

First, I elected to focus exclusively on federal enactments. Much of that decision was pragmatic: there is simply too much state variation to undertake a thorough assessment. I do acknowledge that state privacy practices can vary considerably and may touch on important issues ignored here. But it is also the case that, although some states have acted as first movers in statutory privacy, many states have simply mirrored or even copied federal statutory analogues. Nevertheless, my primary interest is in federal forms of regulating privacy, with their power to preempt or shape state laws and practices, particularly given my secondary interest in federal legislative power as an alternative to constitutional pronouncements.

Second, in selecting which federal enactments to study, I essentially asked whether the statute covered material likely to be of interest to a law enforcement investigation. My standard was not high; if material seemed to plausibly relate to police investigation, I included the statute. At first glance this standard may appear circular—would we not expect law enforcement exemptions in statutes that cover information useful to law enforcement? Maybe. But there are no routine exemptions for persons with interests we might deem equally as compelling—such as journalists or public health officials. And the statutes themselves cover a broad range of subjects, many of which are not obviously candidates for automatic law enforcement exemption. More importantly, there are lessons to be learned from both the variety and uniformity in the exemptions, as this Article illustrates.

Third, it is worth underscoring that my purpose in examining these statutes is to think about them with regard to ordinary domestic criminal justice. I therefore deliberately ignored those statutes tailored entirely to national

23. For example, states have enacted omnibus data-breach-notification provisions, state privacy torts, trade secrets provisions, rape shield laws, and so forth, none of which are addressed in this Article. California, in particular, has been considered a leader in the area of state privacy legislation. John R. Forbush, Comment, Regulating the Use and Sharing of Energy Consumption Data: Assessing California’s SB 1476 Smart Meter Privacy Statute, 75 ALB. L. REV. 341, 353–54 (2011–12) (“California is the first state to have an office dedicated solely to protecting consumer privacy and the state has been a leader in passing privacy protection statutes that go beyond the minimum ‘floor’ protections set out in various federal laws.”).

24. See infra notes 236–240 (discussing, in the context of federalism questions, the related debate over whether states have aggressively pursued privacy policies).
security, such as the Foreign Intelligence Surveillance Act, as well as provisions in general privacy statutes that pertained exclusively to national security investigations.25

Finally, this enterprise is admittedly imprecise. Although I have tried to be cautious in generalizing from such a richly textured set of materials, the assessment here is qualitative and evaluative, not quantitative and exacting. Nevertheless, clear general principles can be extracted from the study of federal statutory privacy, and to that end I believe I have set forth relatively uncontroversial observations about their operation.

B. Things We Already Know:
Federal Statutory Privacy Is Recent and Patchwork

There are two universal truths about privacy statutes that should be acknowledged by way of background. The first is that federal privacy statutes represent a relatively recent phenomenon, and the second is that they are sectoral rather than universal in character.

1. Statutory Privacy Is a Late Twentieth-Century Invention

As might be expected, federal statutes dedicated to privacy are largely the product of the final quarter of the twentieth century. Notions of personal privacy precede this period, but this early interest focused primarily on intrusions by private actors, not the government. For example, most scholars attribute the “birth of privacy” to the seminal article The Right to Privacy, published in 1890 by Samuel Warren and Louis Brandeis in the Harvard Law Review.26 That article launched privacy as a doctrinal area principally concerned not with governmental intrusions but rather with the emergence of a media culture interested in prurient gossip.27 Accordingly, the new torts focused largely on the commercial exploitation of private information, rather than on corporate espionage or government abuse.28

Even the earliest communication privacy statutes were aimed more at the “protection of . . . property, not the safeguarding of the individual’s

25. Although national security is, of course, a form of “law enforcement” (and concededly, one that often interfaces with domestic law enforcement), I find that the peculiarities of both law and policy with regard to national security are difficult to see beyond once they are introduced. Therefore, I have omitted those provisions in order to bring the purely domestic issues into unobstructed view.
27. Id. at 195–96 (focusing on commercial rather than governmental invasions of privacy). Reviewing the law of privacy in 1960, Professor Prosser identified four distinct torts, each having more to do with popular publicity than with law enforcement encroachments. See William Prosser, Privacy, 48 CALIF. L. REV. 383 (1960).
28. See id. at 217; see also DANIEL J. SOLove & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 11 (4th ed. 2011).
Nevertheless, with the rise of Prohibition, law enforcement interception of private communication became a more salient issue. While the Attorney General and the Federal Bureau of Investigation ("FBI") disavowed wiretaps as "unethical," the Treasury Department embraced them. By 1932, Congress had considered and rejected eight bills prohibiting wiretapping. A rider along those lines briefly passed in 1933, but the enactment of section 605 of the Federal Communications Commission Act marked the critical point for wiretapping law. Despite strong evidence that the provision was intended only to transfer jurisdiction from the Federal Radio Commission to the newly created Federal Communications Commission ("FCC"), the provision's wording launched a series of challenges aimed at interpreting the section as a wholesale ban on wiretaps.

In deciding these cases, the Supreme Court engaged in creative readings of the statute to effectively prohibit wiretapping without overturning its decision in Olmstead v. United States, which had held that wiretapping did not impinge on a Fourth Amendment interest. In this respect, it was actually the Court, rather than Congress, that was the true author of these early communication privacy protections, although the instrument of transmission was statutory interpretation rather than constitutional rulings. Arguably, the Court's interest in privacy continued to outstrip Congress's into the midcentury, when the Court decided a series of substantive due process and First Amendment cases addressing familial, sexual, and associational privacy.

It was not until the 1970s that congressional interest in informational privacy began to blossom. The growing reach of the administrative state, coupled with the increasing sophistication of the commercial sector and the emergence of new data-processing technologies, combined to create a raft of concern over the security of private information. On the one hand, the government increasingly sought information to ensure compliance with legal and administrative regulations, and market entities sought information hoping to reach new consumers. On the other hand, anxiety over growing data collection—both in terms of the kinds of records generated and the frequency with which they were stored and accessed—prompted concerns about

29. *See Jacob W. Landynski, Search and Seizure and the Supreme Court: A Study in Constitutional Interpretation* 199 (1966) (describing early interception statutes as concerned with "malicious injury").
30. *Id.* at 200-01.
31. *Id.* at 205.
32. *See id.* at 206-07.
33. Significantly, this historical interpretation suggests that although it is true that courts historically have not "engage[d] in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies," Kerr, *supra* note 12, at 831, that may in part be because they reserve that creativity for the interpretation of congressional statutes. It is thus difficult to determine exactly which institution to consider the true agent of protection.
threats to personal privacy, and especially the government’s abuse of intimate information.\textsuperscript{35}

Thus, starting in 1970 with the passage of the FCRA, and followed quickly by the passage of the Privacy Act, FERPA, RFPA, and the Foreign Intelligence Surveillance Act, Congress embarked on a course of identifying discrete threatened interests and extending particularized protections via statute. Accordingly, there was a surge of privacy laws passed in the 1970s,\textsuperscript{36} aided in part by the Watergate scandal and publication of the Privacy Protection Study Commission’s report, \textit{Personal Privacy in an Information Society}.\textsuperscript{37} Congress’s interest in statutory privacy endured and, as is evident from the Appendix, five or six pieces of privacy legislation were passed in each of the ensuing decades. In sum, whereas the earliest common law efforts to address privacy were shaped by the fear that private citizens would exploit technology for private gain,\textsuperscript{38} modern federal statutory privacy law is shaped by equally strong concerns about governmental collection and abuse of intimate information.

2. Statutory Privacy Protection Is Piecemeal, Sectoral, and Reactive

Fifty years of federal legislative interest in privacy has resulted in one commonly recognized and often lamented fact: American privacy law is extraordinarily piecemeal. As Paul Schwartz, one of the foremost scholars of consumer privacy, acknowledged, “In contrast to the approach in many other nations, it is unusual in the United States to find any comprehensive privacy laws.”\textsuperscript{39} Whereas Europe has embraced a coherent, comprehensive approach to privacy regulation, the United States has largely relied on independent enactments tailored to particular sectors or interests.\textsuperscript{40} No single
agency is entrusted with supervising privacy in the United States, nor does there appear to be a single guiding principle or theory. The word "patchwork" is often used to describe the statutory protections, and usually as a critique.

Nevertheless, when I began this research, I expected to find some statutes that directly addressed law enforcement interests and some in which those interests were incidental. I thought I might be able to classify statutes according to the material protected—for instance, those explicitly regulating police investigative activity (like Title III, ECPA, or the DNA Identification Act), those directly aimed at general consumer privacy (like HIPAA, CCPA, RFPA, GINA, or the VPPA), and those aimed at regulating information acquired by the government (like the Privacy Act, DPPA, FERPA, or the IRS Code). But although that was to some degree true (such as with statutes like FISA or COPPA), I learned that most statutes were both motivated by and enacted in response to a range of public and private concerns. For example, passing the Wiretap Act was as much about preventing corporate espionage as it was about circumscribing police power, and HIPAA drafters worried as much about personal data being abused by the government as they did about misuse by researchers or the insurance industry.

Categorizing statutes according to the degree to which privacy is their primary focus likewise failed to provide meaningful insights. Rarely was only one purpose identifiable, and it was hard to classify, much less rank, concerns as diverse as job discrimination, overzealous researchers, free-

41. The major exception to this rule, however, is the Privacy Act, which is a form of an omnibus protection.

42. See generally Fred H. Cate, Privacy in the Information Age 80 (1997) (describing American law as “[a] patchwork of uneven, inconsistent, and often irrational” federal and state rules); Bamberger & Mulligan, supra note 40, at 249, 258 & n.32 (citing sources and noting that “[t]he dominant critique denounces the existing patchwork of privacy statutes as weak, incomplete, and fractured”).

43. The drafters defined the problem of technological developments as centered on fears that “[c]ommercial and employer-labor espionage is becoming widespread. It is becoming increasingly difficult to conduct business meetings in private. Trade secrets are betrayed. Labor and management plans are revealed.” S. Rep. No. 90-1097, at 67 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2154. The list did go on to worry that “each man’s personal, marital, religious, political, or commercial concerns can be intercepted” but it reads like an afterthought. Id. ECPA echoed these concerns: “Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.” S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556–57.

44. See, for example, FERPA, HIPAA, and GINA.

45. See, for example, HIPAA and the DNA Identification Act.
dom of speech,46 government abuse,47 corporate powers and marketing,48 and crime prevention.

The same problems arose in an attempt to classify statutes according to the entity holding the information. First, although in some instances a government entity exclusively controls the information (e.g., DPPA, the IRS Code, Privacy Act), a unitary label of “government” seemed indefensible given that some federal statutes target the federal government, while others regulate states and localities (e.g., the IRS Code and Privacy Act versus the DPPA and FERPA). Moreover, many statutes implicate both public and private interests—healthcare and education providers can be either public or private entities, and heavily regulated utilities like phone or cable have quasi-public status. Even banking, a quintessentially private industry, has a strong public component in that many institutions are federally insured.

Nor did the comprehensiveness of a statutory scheme prove a useful sorting device. There certainly are statutes that regulate privacy more broadly than others—the Privacy Act, HIPAA, and FERPA each cover a wide range of entities and materials whereas statutes like VPPA and COPPA target niche interests. And some statutes target privacy directly (like the Privacy Act, CCPA, RFPA, and VPPA) whereas others regulate it indirectly, as just one component in a larger regulatory regime (like HIPAA, FERPA, and FCRA). But all such distinctions, while certainly reasonable, offered little payoff for my purposes. For instance, it does not seem to have much effect on the terms of a statute that it is specifically targeted to privacy versus some other special interest. Nor does scope seem to have a meaningful impact on the remedies available, the scope of the law enforcement exemption, or other characteristics particularly relevant to criminal justice.

Finally, given my focus on law enforcement exemptions, I thought it worthwhile to consider the relationship between statutory coverage and the corresponding degree of protection under the Constitution. Here, I met with moderate success: by and large, these exemptions do appear to chiefly regulate law enforcement activity in areas of indeterminate constitutional protection. That is, imagine three scenarios in which Congress intervenes to regulate privacy statutorily: (1) when the Constitution would otherwise prohibit the law enforcement action; (2) when it is unclear whether the Constitution would permit or forbid it; and (3) when the Constitution permits an activity that Congress wishes to curtail. Title III, the PPA, and arguably the DNA Act are the only statutes targeted at conduct explicitly governed by the Fourth Amendment; the PPA adds to the protection accorded by the Constitution, whereas the other two essentially match it.49 Conversely, only the RFPA, FCRA, and the Pen Register Act occupy a space

46. See, for example, CCPA, VPPA, and the PPA.
47. See, for example, ECPA, FERPA, and HIPAA.
48. See, for example, FCRA, COPPA, ECPA, and DPPA.
49. It was not clear at the time the DNA Act was enacted that this was the case, although precedent strongly suggested that collection of DNA from individuals—even convicted felons—would implicate Fourth Amendment interests.
explicitly left vacant by cases declaring the absence of a cognizable constitutional interest. The remaining statutes falls into a void of uncertain protection—where the Court has neither expressly declared nor denied a legitimate expectation of privacy.

That is not to say that a rough appraisal of a particular statute’s constitutionality is impossible: many statutes address situations likely governed by the so-called “third-party doctrine,” which holds that information knowingly exposed to a third party ceases to be private and thus receives no Fourth Amendment protection. But such guesswork is just that—there are contrary indications that some information held by third parties, like health records or email records, might in fact garner constitutional protection.

Nevertheless, as I explore in greater depth in Section I.C, ambiguous constitutional status hardly appears determinative: there are ample areas that Congress has chosen not to regulate, despite the clear absence of constitutional protection. In sum, my survey suggests that the federal code lacks not just an omnibus provision protecting privacy but also any principled basis for defending the piecemeal protections it does contain.

Indeed, if anything seems clear from an examination of the legislative history of privacy statutes, it is that Congress does less leading and much more following when it comes to regulating privacy. The most common prompt for legislation is some catalyzing event, whether a Supreme Court case, a newspaper story, or a tragic incident. Close examination of statutory privacy protections simply affirms what the critics utter in complaint:

51. See, e.g., Miller, 425 U.S. at 435.
52. For example, the Supreme Court in Ferguson v. City of Charleston, 532 U.S. 67 (2001), invalidated a joint program between hospital workers and police to identify cocaine-addicted pregnant women. Although the ultimate holding rested on an opaque set of theories, the Court found that the women retained a privacy interest in their collected urine samples and the resulting tests. Id. at 1288. Because the hospital workers were county officials, however, the Court did not have to address whether the entanglement with law enforcement would itself have been enough to violate the Constitution. Id. at 1287. With regard to email, the Sixth Circuit in United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), recently held that the defendant had an expectation of privacy in his emails, and that his privacy was violated when agents compelled his internet service provider to hand his emails over without a warrant or probable cause. The court, however, found that the exclusionary rule did not apply. Id. at 288. More recently, Justice Sotomayor in her concurrence in United States v. Jones, 132 S. Ct. 945, 957 (2012), suggested that the third-party doctrine might need revisiting.
54. For example, an article about Robert Bork inspired the VPPA, as recounted infra in the text accompanying note 65. Likewise, an article in Parade magazine about student records inspired Senator Buckley, who entered the article into the Congressional Record, to push for the passage of FERPA. See 120 CONG. REC. 13,953 (1974).
55. For example, the DPPA was passed after it came to light that actress Rebecca Schaeffer had been murdered by a stalker who had easily obtained her address from the Department of Motor Vehicles. See 140 CONG. REC. 7924–25 (1994) (statement of Rep. Moran).
that regulations are atomistic, inconsistent, atheoretical, and idiosyncratic. But despite an inability to slot federal privacy statutes into one coherent model, I believe that some conclusions may still be drawn, especially regarding criminal justice.

C. Statutes Tend to Address Technology-Based Concerns

Given the broad range of motivations explored above, we might expect that no single thread ties general privacy statutes together. But, in fact, nearly all statutes seem to share one galvanizing interest: technology. Just as the “[r]ecent inventions” of “[i]nstantaneous photographs ... and numerous mechanical devices”56 prompted the birth of privacy at the start of the twentieth century, so too have more recent technologies propelled the enactment of privacy statutes in that same century’s final quarter.

Of course, many privacy statutes broadcast this connection via titles that reference electronic communications, online activities, cable, and DNA. But concerns about electronic recordkeeping emerge in other less overtly technology-based statutes as well. Starting with the grandfather of federal privacy, the Privacy Act of 1974, the theme emerges clearly. The progenitor of the Privacy Act was a series of hearings and reports centered on modern government data-gathering and recordkeeping methods. One passage of the Senate Report concluded as follows:

When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make [sic] it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.57

HIPAA was likewise motivated by concerns that federal efforts to enhance administrative efficiency would, in light of new technologies, render sensitive medical information more vulnerable to improper disclosure.58 The RFPA was in large part a response to federal laws mandating collection and retention of financial transaction data, which spawned concerns over

potential abuse of "modern information technologies." Variations on the same theme are visible even in the DPPA and FERPA, although less pronouncedly so. At times, the articulated fear was that the government could abuse the electronic stores of information that it had either generated or collected, as was the concern with RFPA, HIPAA, FERPA, DPPA, Real ID, DNA, the IRS Code, and the Privacy Act. At other times, Congress seemed to be responding instead to the rising concern that private parties would exploit technology for private benefit—as was the concern with FCRA, COPPA, and the VVPA. In every case, the fear was that technology had changed, and therefore imperiled, the recording, storage, retrieval, and sharing of information.

To illustrate just how pervasive the technological commonality is, consider a final example: the VPPA. At the most superficial level, the statute obviously responds to new technology—specifically, home video rentals. But the tale of the statute's inspiration confounds this technological connection, since the law was precipitated by a Washington City Paper story about then-Supreme Court nominee Robert Bork, which revealed a list of 146


60. Passage of the DPPA was prompted by a series of high-profile cases in which stalkers or other criminal offenders obtained access to personal information of potential victims through routine inquiries at state departments of motor vehicles; this concern was heightened by the perception that a lucrative financial market existed for states to sell such information to private entities. See, e.g., Protecting Drive [sic] Privacy: Hearing on H.R. 3365 Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary, 103d Cong. (1994) (statement of Janlori Goldman, Director, Privacy and Technology Project, American Civil Liberties Union), available at 1994 WL 212813.

61. FERPA "was perceived as a parental rights bill designed to halt government intrusion," and its primary sponsor, Senator Buckley, "noted that the Watergate revelations had emphasized the dangers of government data gathering and the abuse of personal files." Ellen M. Bush, The Buckley Amendment and Campus Police Reports (Aug. 8, 1992) (unpublished student conference paper), microformed on ERIC No. ED 351 677 (U.S. Dep't of Educ.).


videos he had rented from his local store.65 To the extent that the technological advance of VHS was an issue, it had to do with the fact that renting movies to enjoy at home offered an opportunity to pierce the anonymity of a person's entertainment choices.

Yet the same threat to privacy could be posed by a journalist seeking information about choices that have nothing to do with VHS movies. The legislative history affirms as much. Sprinkled throughout the record are concerns along these lines:

> [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. . . . I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.66

And so the story is one of technology used to record, and potentially reveal, material information like dietary or consumer choices. Technology poses the threat of data assemblage and exploitation—even though the underlying data might be as primitive as local library records.

Tellingly, though, Congress passed a statute about video rentals, not grocery store receipts or library books. And it did this despite the fact that the bill went through most of the legislative process titled the Video and Library Privacy Protection Act. Most of the hearings centered on library book privacy, and many of the statements focused on books, not videocassettes. Yet the library provisions did not survive. In the final Senate Report accompanying the enacted VPPA, there is only one short reference to library records:

> Although the original impetus for the legislation was the disclosure of Judge Bork's video rental list, the bill's sponsors, Senators Leahy, Grassley, Simpson and Simon, included a similar protection for library borrower records, recognizing that there is a close tie between what one views and what one reads.

The subcommittee reported a restriction on the disclosure of library borrower records similar to the one on video records. However, the committee


66. S. Rep. No. 100-599, at 5–6 (1988) (alterations in original) (statement of Sen. Leahy). The rest of the Senate Report includes numerous additional references to concerns about technologically enhanced recordkeeping. E.g., id. at 6 (statement of Sen. Simon) ("There is no denying that the computer age has revolutionized our world."); id. at 7 (statement of Janlori Goldman, Counsel, American Civil Liberties Union) ("These precious rights have grown increasingly vulnerable with the growth of advanced information technology.").
was unable to resolve questions regarding the application of such a provision for law enforcement.\textsuperscript{67}

In other words, despite the similarities between books and videos, and even despite the common concern of technological aggregation, law enforcement interests were sufficient to overcome the privacy interests in the former, but not the latter.\textsuperscript{68} And, of course, it is not just library records that have eluded congressional action. The Supreme Court has rejected privacy claims in a variety of brick-and-mortar interests—like in discarded trash\textsuperscript{69} or the open fields of private land\textsuperscript{70}—and those rulings all met with congressional silence.

In sum, across the breadth of federally enacted statutes dedicated primarily to the protection of privacy, the theme of technological advancement emerges as a common thread. To be sure, there are obviously areas in which technology threatens privacy and yet the federal legislature has not

\textsuperscript{67} Id. at 8.

\textsuperscript{68} Reader privacy is a contentious area. For instance, the Supreme Court has indirectly suggested that there might be some constitutional protection for reader privacy. United States v. Rumely, 345 U.S. 41, 48 (1953) (Douglas, J., concurring) (oft-cited concurrence suggesting privacy in context of review of conviction of bookseller who refused to disclose customer lists to House committee), but it has also repeatedly held that there is no heightened Fourth Amendment scrutiny for law enforcement actions that implicate First Amendment interests; see, e.g., New York v. P.J. Video, Inc., 475 U.S. 868, 875 (1986) (rejecting argument that higher standard of probable cause was required to support warrant to seize material protected by First Amendment); Maryland v. Macon, 472 U.S. 463, 466, 469 (1985) (rejecting heightened scrutiny for police officer's purchase of magazine from bookstore); Zurcher v. Stanford Daily, 436 U.S. 547, 565-66 (1978) (rejecting argument for higher standard to seize material from newspaper office). \textit{But cf.} In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (finding First Amendment interests superseded government interest in gaining access to patron's records); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Colo. 2002) (holding that "the Colorado Constitution requires that the innocent bookseller be afforded an opportunity for an adversarial hearing prior to execution of a search warrant seeking customer purchase records" and finding search warrant at issue not enforceable). There is no general federal statutory protection for reader privacy, although the Privacy Act might be deemed to provide limited protection in the context of federal libraries. The primary protection derives from state privacy laws (some of which have law enforcement exemptions, see, e.g., Tex. Gov't Code Ann. § 552.124(a)(3) (West 2011)), as well as ethical norms promulgated by the American Library Association, see generally

\textsuperscript{69} California v. Greenwood, 486 U.S. 35 (1988) (holding that there is no expectation of privacy in trash). The Bork episode provides a perfect example of this, as the journalist likened his search to the well-established journalistic practice of rifling through the trash for clues—a statutorily (and constitutionally) unregulated activity. Dolan, \textit{supra} note 65 (likening quest for video rental records to A.J. Weberman's scrutiny of Bob Dylan's trash and general pursuit of "garbageology").

Nonetheless, it is remarkable that the overwhelming majority of federal privacy statutes address one particularly threatening thing.

**D. Law Enforcement Interests Dominate**

If technology issues propel the expansion of federal privacy protections, then another interest—law enforcement—can be said to curtail it. The story of the library-records provision, recounted above, is just one example of the powerful influence of law enforcement. Study of the scope of these statutes reveals three truths: first, virtually no privacy statutes erect absolute bars to access; second, law enforcement is the sole interest consistently exempted from general provisions; and third, law enforcement regularly offers its perspective on, and plays a critical role in shaping, not just those exemptions but the terms of the statutes themselves.

Significantly, no current statute erects an absolute bar to accessing its regulated material. This need not, of course, be the case. For example, in 1967, President Johnson publicly denounced wiretapping in his State of the Union address, saying that “[w]e should outlaw all wiretapping—public and private—wherever and whenever it occurs, except when the security of this Nation itself is at stake—and only then with the strictest governmental safeguards. And we should exercise the full reach of our constitutional powers to outlaw electronic ‘bugging’ and ‘snooping.’”

A somewhat more recent statutory model even exists: when a law protecting the privacy of substance abuse treatment records was first enacted in 1970, it proclaimed a total ban on disclosure absent patient consent. Legislators even decried as “undesirable” a provision in the original bill that allowed limited access. In successfully securing the deletion of even that narrow provision, they argued that if “information of nonconsenting persons may be disclosed under court order . . . [it] could result in a widespread notion among individuals with
alcohol problems . . . that the prohibition against disclosure of their personal records is subject to a powerful exception."74 Indeed, although subsequent amendments have loosened these strictures, the statute still forbids the use of records to "initiate or substantiate any criminal charges against a patient."75

But every other federal statute has, from its inception, provided controlled access for an assortment of entities, including researchers, public health officials, emergency responders, educators, therapists, medical professionals, and agency regulators—just to name a few.76 Yet while these identities change, the law enforcement exemption stays the same. Criminal conduct statutes make such exceptionalism sharply visible, since the exemptions often stand alone. The VVPA, for instance, prohibits surreptitious photographing of private body parts, but exempts "lawful law enforcement, correctional, or intelligence activity."77 Similarly, the Telephone Records and Privacy Protection Act of 2006 makes "pretexting" a crime, but exempts "law enforcement agencies."78 The CFAA regulates "hacking" and applies to all but "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency."79

This heedfulness to the needs of law enforcement does not occur spontaneously. Instead, unsurprisingly, law enforcement representatives regularly and routinely weigh in to address the impact that statutory protections will have on their interests, and to help shape or guide the scope of the inevitable law enforcement exemption. Of course, for a statute that is largely defined by its law enforcement provisions, like the Wiretap Act, this might be expected. But history shows that law enforcement typically offers comments on a wide range of proposed legislation, and resistance by law enforcement may hinder or even prevent the passage of a generally applicable statute. Law enforcement resistance to financial privacy protections caused many standstills before the RFPA was successfully enacted.80 Similarly, HIPAA drafters explicitly noted that the regulations were not intended to affect law

---


75. 42 U.S.C. § 290dd–2(c) (2006). These amendments introduced exceptions that parallel those found in HIPAA, including for use in medical emergencies and anonymous research. Id. § 290dd–2(b)(2).


77. 18 U.S.C. § 1801(c).

78. Id. § 1039(g) (Supp. V 2011).


80. Numerous financial privacy bills had been introduced from as early as 1973; in fact, over five congressional hearings had been held on the topic. But in each case, law enforcement interests vigorously opposed, and ultimately killed, any legislation restricting law enforcement access to financial records. See Kirschner, supra note 59, at 28.
enforcement access in any way but were intended only to heighten penalties in the event of misuse.\textsuperscript{81}

In contrast, it is less common that a privacy-protective entity with a specific focus on criminal justice issues weighs in. The repeat players advocating for privacy before legislators are all-purpose organizations like the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, and the Electronic Frontier Foundation. As such, their agenda tends to focus largely on mainstream socioeconomic concerns. Less commonly seen are representatives of privacy interests specific to domestic criminal justice and the populations most affected by domestic policing, whether defined as groups like the National Association of Criminal Defense Lawyers or the National Legal Aid and Defender Association, the Innocence Project, or even the Legal Defense Fund or the Urban League.\textsuperscript{82} There is no single NGO or interest group dedicated exclusively to protecting the privacy of the policed poor. There are instead general criminal justice NGOs with a long list of other matters to attend to (e.g., the death penalty, the right to counsel, et cetera), minority- or poverty-focused groups that likewise fill their dockets with topics like anti-discrimination and welfare reform, and generalized privacy entities that tend to focus their attention on mainstream concerns like general consumer privacy. For this reason, in perusing the legislative history of many of these enactments, it is not uncommon to find comments or testimony from representatives of the Department of Justice ("DOJ"), the FBI, and other state and local law enforcement and prosecutorial entities (mainly through professional associations) focused exclusively on the question of law enforcement access, while the contrary views are mainly addressed to the general

\textsuperscript{81} See Dep't of Health \& Human Servs., Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996, at II.E.9 (1997), available at http://epic.org/privacy/medical/hhs_recommendations_1997.html ("We are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies.").

\textsuperscript{82} The reason for this is perhaps clear. A quick review of those organizations' websites, some of which list congressional testimony, reveal a busy docket focused on issues exclusively related to criminal justice. See, e.g., Nat'l Ass'n Crim. Def. Law., Federal Action, http://www.nacdl.org/federalaction/ (last visited Oct. 12, 2012) (listing legislative priorities as crime labs and forensics reform, discovery reform, grand jury reform, indigent defense, national security, sentencing reform, sex offenses, street gangs, and white-collar crime); History of NLADA, Nat'l Legal Aid \& Defender Ass'n, http://www.nlada.org/About/About_HistoryNLADA (last visited Aug. 29, 2012) (detailing focus on right to and quality of counsel issues, along with civil matters); Reports and Publications, Innocence Project, http://www.innocenceproject.org/news/reports.php (last visited Aug. 29, 2012) (annual reports detailing testimony on topics such as post-conviction review, improvements in forensic science, state laws on DNA access, wrongful convictions, and eyewitness identification); Signature Programs, Nat'l Urban League, http://www.nul.org/what-we-do/our-signature-programs (last visited Aug. 29, 2012) (describing focus on legislative issues such as work and housing opportunities).
provisions of the law, rather than with specific attention to its law enforcement exemptions.

Accordingly, although generalizations are more subjective and hence riskier here, it might be argued that more than any other factor, the greatest determinant of the scope of a law enforcement exemption is the degree to which law enforcement deems the covered material important. For example, the statutes for the most part allow law enforcement ready access to drivers' records, electronic records (like emails), health records, and basic credit identification information. The DPPA, ECPA, HIPAA, and FCRA all address information commonly accessed in criminal investigations, and each contains provisions that allow disclosure on the basis of a simple administrative request of law enforcement. At the other end of the spectrum, less seemingly probative material such as video rental records and cable records (for instance, pay-per-view history) are exceptionally difficult to obtain, requiring heightened evidentiary showings and formal process.\textsuperscript{83} The passage of the VPPA provides one plausible example of the power of law enforcement: the VPPA is unusual in that it provides a statutory exclusionary rule, which arguably is the result of the atypical silence of law enforcement interests during the short period surrounding its passage.\textsuperscript{84}

Of course, this rule is not without exception. Most pertinently, areas protected specifically by the Fourth Amendment—such as wiretapping of phone lines—require heightened protection (warrant and probable cause) and yet cover very useful investigative material. Similarly, the PPA restricts search warrants of journalists' offices beyond the constitutional standard and yet it is easy to imagine that this information is also frequently helpful. Conversely, there are statutes such as FERPA that have restrictive-access provisions and yet regulate information likely to be of limited utility for most law enforcement investigations.

Nevertheless, the degree of protection from law enforcement seems far more likely to turn on whether the information is useful in investigations than it does on widely shared intuitive notions of what is more or less deserving of privacy,\textsuperscript{85} suggesting the strength of law enforcement's ability to influence the scope of exemptions. Perhaps for this reason, the law enforcement exceptions take highly individualized shapes. They are neither blanket provisions permitting unfettered access nor cookie-cutter templates

\textsuperscript{83} See infra notes 161–164 and accompanying text.

\textsuperscript{84} The VPPA was enacted quickly in the wake of the Bork incident, and the bulk of the hearings were consumed either by the initial provisions of the bill that also would have protected library records or by the concerns of direct marketers. See Video and Library Privacy Protection Act of 1988: Joint Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary and the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary, 100th Cong. 123–25 (1989). For reasons unclear from the record, the FBI declined to testify with regard to the bill and instead promised to submit written comments, which never arrived. Id. at 146. The DOJ submitted written comments but they focused on various access provisions rather than the remedy for violation. See id. at 150.

\textsuperscript{85} See SLOBOGIN, supra note 14, at 184 (reporting results of empirical study on expectations of privacy).
replicated across every statute. But before turning to that variation, the next Section considers two situations in which law enforcement interests tend to trump all other interests, resulting in not just diminished privacy protections but also the imposition of affirmative disclosure obligations.

E. Protection Focuses on Individuals, Not Entities, and Especially Members of the Economic Mainstream

Just as technology to some degree drives the expansion of federal privacy law, and law enforcement to some degree slows it down, there are two other characteristics of federal privacy protection that might be noted. First, federal statutory privacy law tends to be protective of individual, not entity, interests. And second, federal statutory privacy law tends to be protective of mainstream, not marginal, socioeconomic interests.

1. Individuals, Not Entities

Privacy statutes appear quite deliberately to protect the interests of individuals, as opposed to corporations or other collective entities. This was perhaps made starkly clear in the recent Supreme Court case *FCC v. AT&T Inc.*, in which the Court held in a brief, unanimous opinion that federal protections for “personal privacy”—in that case, an exemption in the Freedom of Information Act—applied only to individuals and not to corporations. Other statutes reflect a similar orientation: The RFPA covers financial records only of a “person,” defined as “an individual or a partnership of five or fewer individuals.” Likewise, the FCRA defines “consumer” as “an individual” and focuses on “consumer report[s].”

Of course, there are exceptions: Title III and the SCA cover communications by corporate agents as well as private individuals, and the IRS Code extends to entity and not just individual returns. But the bulk of dedicated

86. See RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 299 (1981) (noting that “the general trend of legislative activity was to increase the privacy of individuals . . . and decrease that of business firms and other organizations” while acknowledging that “(t)he pattern is actually more complicated”). There are many distinctions that have been made between individual and entity privacy. For instance, a public corporation is typically heavily regulated, and must by law disclose a wide swath of information. Even a privately held company might have a broad array of legal obligations to disclose or publish certain information, or to make such information available to regulators. Moreover, privacy is typically justified by reference to the needs of personal autonomy, freedom from embarrassment or humiliation, or basic principles of liberty—none of which is as readily translated to the inanimate corporate context.


91. Privacy does, however, vary according to the nature of the return filed. See 26 U.S.C. § 6103 (2006 & Supp. V 2011). For instance, joint returns are limited to disclosure to one of the filing parties, whereas a C corporation return can be disclosed to board of directors’ designees, officers, and employees as approved by the principal and certain shareholders. Id.
federal privacy statutes appear concerned primarily with individual privacy: DPPA regulates individual driver's licenses, while most business licenses are public.\textsuperscript{92} And numerous statutes, including some primarily aimed at personal privacy, require active disclosure of the same information as regards business entities.\textsuperscript{93}

2. The Poor

It is not just collective entities that are often excluded from privacy's protective reach. Historically, federal statutory privacy laws have also left unprotected—or even deliberately exposed—the private matters of those in the lower socioeconomic classes.\textsuperscript{94}

Consider, for instance, federal legislation conditioning public assistance grants. With regard to public housing, federal law states that any contracting agency "shall furnish any Federal, State, or local law enforcement officer, upon the request of the officer, with the current address, Social Security number, and photograph (if applicable) of any recipient of assistance."\textsuperscript{95} To make such a request, an officer need not have any formal legal process or be investigating a housing-related claim. Instead, she need only provide a name and an assurance that the person "has information that is necessary for the officer to conduct the officer's official duties," is a fugitive felon, or is in violation of probation or parole.\textsuperscript{96} In other words, an investigator seeking a peripheral witness can obtain from the housing authority that witness's address, Social Security number, and photograph without any showing of suspicion or process of any kind. Moreover, this provision applies "[n]otwithstanding any other provision of law"; thus, even if a state were to attempt to provide greater privacy for its denizens, it would not succeed.\textsuperscript{97} And the penalty for violating the provision by obtaining information under

\begin{footnotesize}
\begin{enumerate}
  \item \textsuperscript{92} 18 U.S.C. §§ 2721-2725 (2006).
  \item \textsuperscript{93} There are also some independent protections for corporate information like trade secrets, see, e.g., Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839 (2006 & Supp. V 2011), as well as for copyright, trademark, and other legal doctrines that serve the goals of entity privacy or control over information dissemination, see, e.g., Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (2006) (liability for bad faith in registering domain names), and restrictions on the sharing of business data with various governmental entities, e.g., 15 U.S.C. § 176a (bureau of commerce); 13 U.S.C. § 402 (economic analysis and labor statistics).
  \item \textsuperscript{94} Of course, this thesis is not absolute. The government has long sold information collected during the census, which obviously applies across socioeconomic boundaries, without any interference from Congress. See, e.g., Solove, supra note 35, at 1149–50. Conversely, a federal statute has long protected the privacy of records related to substance abuse treatment (which might be deemed a less mainstream interest). See supra notes 73–75 and accompanying text.
  \item \textsuperscript{95} 42 U.S.C. § 1437z (2006) (emphasis added).
  \item \textit{Id}.
  \item \textit{Id}.
\end{enumerate}
\end{footnotesize}
“false pretenses” or disclosing it improperly is a fine-only misdemeanor conviction or possible civil liability.98

Similarly, although the original welfare legislation contained some privacy safeguards,99 the passage of the 1996 Personal Responsibility and Work Opportunity Reconciliation Act (“PRWORA”)100 significantly eroded the protection afforded to welfare recipients. The federal welfare provisions, or Temporary Assistance to Needy Families (“TANF”) as it is now known, not only fail to impose any procedural barriers to collection of private information but in fact require disclosures to law enforcement in circumstances identical to that for public housing.101

Even more intrusively, the law requires beneficiary recipients to provide detailed paternity information or, if paternity is unknown, to list all possible fathers.102 One scholar succinctly explains as follows:

[PRWORA] specifically allows the states to vest their child support collection agencies with the administrative power to impose the following without judicial review: orders on employers to divulge extensive information about their employees; orders on employers, financial institutions and governmental agencies to withhold a payer’s income or to seize his/her assets; orders on the putative biological parents and their alleged children to submit to genetic tests; and orders on single mothers to provide the name, address, Social Security number, driver’s license number, employer, and any other necessary identification information for the alleged father.103

The state is, admittedly, required to take steps to safeguard information generally, but the statute does not set any specific floor.104 And, as in the

---

98. Id. § 1437d(q)(6), (7).
103. Id. at 147. Smith elaborates further on how child support cooperation rules affect single mothers:

The PRWORA specifically orders each state to compel single mothers who receive welfare benefits to cooperate with state agencies in establishing the paternity of their children and in obtaining child support payments. Although similar legislation had been in effect since the mid-1970s, the PRWORA directs the states to sanction clients who do not cooperate, expands administrative powers, and decreases the level of judicial review. It also weakens an important exemption: whereas previous federal law and regulations had required states to exempt women subjected to domestic violence from child support cooperation rules, the PRWORA has given the states the freedom to define the exemption themselves.

Id. at 123–24 (footnotes omitted).
104. 42 U.S.C. § 602(a)(1)(A)(iv). State implementation of privacy protections vary markedly, in that some limit disclosure to purposes directly connected to the administration of benefits whereas others are more permissive. See generally Gustafson, supra note 99, at 667–81 (detailing sharing of welfare records with law enforcement for investigative purposes, state
case of public housing, the law enforcement access provisions override any contradictory state protections. They further allow the sharing of basic information (such as name, address, and case number) with "private industry councils," namely local groups of business leaders.

These provisions have been actively, not just passively, exploited by law enforcement. For example, in the wake of these provisions’ passage, federal officials set up “Operation Talon,” a program designed to mine welfare and housing rolls to apprehend persons with outstanding warrants. Moreover, states commonly condition receipt of welfare benefits on the provision of sensitive personal data—data that, as the foregoing attests, is then fully open to public officials’ inspection. Eight states now require the collection of biometric information, and some impose random drug testing. Lastly, the law is unsettled as to the constitutionality of unannounced, random searches of welfare recipients’ homes, and so federal privacy legislation, if anything, encourages rather than forbids such searches.

Persons with criminal records, an estimated 80 to 90 percent of whom are indigent, also have virtually nonexistent federal privacy protections:

---


107. Gustafson, supra note 99, at 670–71 (adding that such measures are costly and have not been shown to significantly reduce fraud). Between 1997 and 2006, the program has led to the arrest of over 10,000 individuals. Id. at 671. It should be noted that it is not the case that the capture of fugitives necessarily results in a cost savings to public programs—even if one person was improperly enrolled in benefits, it is still the case that family members may be eligible to continue receiving assistance. Id. This program may remind some readers of Project Match, a 1977 program to compare welfare and employee records in order to detect fraud, and that represented one of the first forays into data mining by the federal government. See James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 WASH. L. REV. 1, 43 (2003).

108. Gustafson, supra note 99, at 675. There were significant debates in the 1970s over the requirement that the Social Security number be used as a basis for obtaining benefits. See id. at 668 n.114.

109. See id. at 679–80. It should be noted that there has been some recent resistance to mandatory drug testing for welfare recipients. See Lebron v. Wilkins, 820 F. Supp. 2d 1273 (M.D. Fla. 2011) (issuing preliminary injunction enjoining suspicionless drug testing of federal welfare recipients under Florida law).

110. Compare Samson v. California, 547 U.S. 843 (2006) (upholding warrantless, suspicionless searches of homes of conditional releases), and Wyman v. James, 400 U.S. 309 (1971) (holding that the Fourth Amendment was not violated by an announced cursory visit to the welfare recipient’s home by social workers), with Parrish v. Civil Serv. Comm’n, 425 P.2d 233 (Cal. 1967) (finding by California Supreme Court that random midnight raids violated the Fourth Amendment).

"In the United States, criminal records are effectively public, either by law or in practice."112 Indeed, federal law has arguably made criminal records more accessible. First, federal statutory law has indisputably moved toward greater centralization of criminal histories, rather than sheltering such history from public consumption.113 As a result, whereas historically "an individual’s criminal records were not easily retrievable because a searcher would not know which court held the relevant records[, r]ecent statewide centralization and automation of court records systems has vastly increased record identification and accessibility."114 Second, new federal laws mandate that background checks be conducted for a wide range of reasons, including for certain employment positions, which creates incentives for others to begin looking for, compiling, and even selling such records.115 And in the absence of federal laws mandating confidentiality protections for criminal records, there has emerged a “thriving private sector industry” aimed at providing such information to interested parties.116 At most, entities providing this information are covered by the Fair Credit Reporting Act, which one expert describes as “offer[ing] very little protection for persons who have a criminal record.”117 Thus, not only do federal statutes create and then provide essentially free and unfettered access to criminal records for law enforcement personnel,118 but they also fail to


112. James B. Jacobs & Dimitra Blitsa, Sharing Criminal Records: The United States, the European Union, and Interpol Compared, 30 Loy. L.A. Int’l & Comp. L. Rev. 125, 142 (2008) (“They can be obtained through three channels: (1) courts and court systems; (2) state criminal record repositories; and (3) private companies that sell information. While the state-level repositories and the FBI’s National Criminal Information Center (NCIC) restrict access to their criminal records, court records are open to the public as a matter of historical practice and constitutional common law. Private information companies mostly obtain criminal record information from courts and sell it to private customers.”) (footnotes omitted)).


114. Id. at 183.

115. Id. at 178–79. In fact, criminal convictions are now considered relevant to a wide range of determinations, including government benefits, voting rights, student loans, public housing, educational programs, public licenses, and so on. See, e.g., Chris Jay Hoofnagle, Big Brother’s Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. INT’L L. & COM. REG. 595 (2004); James B. Jacobs, Mass Incarceration and the Proliferation of Criminal Records, 3 U. ST. THOMAS L.J. 387, 389–90 (2006).


117. Id. at 186 n.57.

meaningfully circumscribe access to those records by other private persons.119

In sum, not only has federal statutory law failed to provide safeguards protecting the privacy of low-income persons, but it has actually affirmatively compromised their privacy by mandating disclosure on the thinnest showing of law enforcement need.120 To the extent that technology has played a role with respect to the privacy of the poor, it has been to capitalize on opportunities to share information, rather than to view digitalization as a threat.

Before closing, I want to briefly anticipate some likely reservations about these claims. First, some might expect that the government simply protects privacy less vigorously when acting in its spending or appropriations capacity, but that turns out not to be the case. Rather, many of the federal privacy statutes currently in effect use expenditures as the hook through which to impose baseline protections. Whether through federal highway funding, FDIC status, or Medicare appropriations, Congress has repeatedly chosen to enhance, not lessen, privacy coverage. Indeed, consider one direct comparison—federal Social Security. Social Security beneficiaries, who reflect a far more diverse socioeconomic profile, receive privacy protection commensurate with other mainstream socioeconomic classes, including checks on accuracy and notice prior to disclosure.121 Even recipi-

information, first for criminal justice purposes and second for both criminal and noncriminal justice purposes). Although the compact was described as “privacy neutral,” in fact it makes criminal record information available for noncriminal justice purposes (like private employment background checks) regardless of state law. See id. at 135–36. By comparison, criminal history information is much more difficult to obtain in Europe, as a matter of both practical coordination and deliberate policy choice. Id. at 137–44 (“In the United States, criminal records are effectively public, either by law or in practice. . . . While most EU countries make conviction records available to judicial authorities and in some cases to police and other public authorities, they almost never provide private individuals and entities (e.g., employers) with another individual’s criminal history record.” (footnote omitted)).

119. To be sure, state laws may regulate access to or use of criminal records—for instance, by sealing arrest histories or barring use of criminal records in employment decisions—but no federal mandate requires such provisions.

120. 42 C.F.R. § 431.306 (2012) (describing federal standards for release of information, which includes a policy to safeguard the information); Khiara M. Bridges, Privacy Right and Public Families, 34 HARV. J.L. & GENDER 113 (2011) (describing highly intrusive information gathering performed as a condition of public assistance for state prenatal care). To be clear, the Constitution does not fare much better. Christopher Slobogin, The Poverty Exception to the Fourth Amendment, 55 FLA. L. REV. 391, 401–05 (2003).

121. They are specifically covered by the Privacy Act, including the Computer Matching and Privacy Protection Act Amendments of 1988, which otherwise does not apply to the states. See George B. Trubow, Protecting Informational Privacy in the Information Society, 10 N. ILL. U. L. REV. 521, 526 (1990); see also infra Section I.F (describing typical access provisions of federal privacy statutes). Section 7 of the Privacy Act of 1974 states that it “shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.” Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909, reprinted in 5 U.S.C. § 552a note at 712 (2006).
ents of unemployment compensation and student loans receive a bit more protection.

Second, some might expect that the government always exploits the information that it has in its possession, so that the disproportionate exposure of the poor is due simply to their entanglement with various federal programs. But federal income tax records are among the most protected pieces of personal information; laws strictly circumscribe law enforcement access to tax records. And even though the Privacy Act is significantly broader, with many avenues for law enforcement to obtain information from federal agencies, it still does not go so far as to mandate divulgence of information, much less in such detail. Nor does Congress restrict its reach in deference to federalist principles: privacy statutes address such classic state tasks as driver’s licensing and even highly localized activities like education or cable-services provision.

Moreover, these provisions cannot be explained as the simple result of congressional efforts to stamp out fraud or crime. To the extent that the government has a strong financial stake in social benefit programs, the majority

122. 20 C.F.R. § 603.5(e) (2012) (allowing “[d]isclosure of confidential UC information to a public official for use in the performance of his or her official duties”); id. § 603.7(b)(2) (allowing such disclosure “without the actual issuance of a subpoena”). This protection is slightly greater in that it also includes provisions for safeguarding further disclosures. Id. § 603.9 (imposing requirement that states require “recipient to safeguard the information disclosed against unauthorized access or redisclosure” through storage, processing, and other precautionary guarantees).

123. See 34 C.F.R. § 5b.9(b)(7) (2012) (allowing such disclosure to a government agency without consent if “the activity is authorized by law, and if the . . . agency . . . has submitted a written request . . . specifying the record desired and the law enforcement activity for which the record is sought”).


125. Critics note that the “routine use” exception is a “gigantic loophole.” Solove, supra note 35, at 1167. And the Act has “been eroded by about a dozen exceptions. For example, agencies can disclose information without the consent of individuals to the Census Bureau, law enforcement entities, Congress, and consumer reporting agencies. . . . Nor does the Privacy Act apply to court records.” Id. at 1167 (footnote omitted). Along these lines, it should be noted that the FBI recently announced that it intended to create a “data warehouse” that consolidated a number of diverse record sources (for example from the Departments of Defense, Energy, Homeland Security, State, and Treasury, as well as from public sources), Privacy Act of 1974, System of Records, 77 Fed. Reg. 40,630 (July 10, 2012) http://www.gpo.gov/fdsys/pkg/FR-2012-07-10/pdf/2012-16823.pdf. It then announced that this database would be exempt from Privacy Act protection pursuant to the law enforcement exemption. Privacy Act of 1974: Implementation, 77 Fed. Reg. 61,275 (Oct. 9, 2012) (to be codified at 28 C.F.R. Part 16); http://www.gpo.gov/fdsys/pkg/FR-2012-10-09/pdf/2012-24753.pdf.
of its investment goes to Social Security and Medicare, not means-tested public assistance. And, of course, the government’s absolute stake in spending is small; in 2011, roughly 13% of the federal budget was allocated to safety net programs, whereas medical benefits consumed 21% and Social Security 20%. To the extent that these provisions might be excused as helping to police crime generally, it is notable that even driver’s license information receives more protection in that disclosures to law enforcement are mandated only in connection with motor vehicle offenses and states are affirmatively limited in their ability to sell information without the driver’s consent. Indeed, to the extent that stopping crime generally is a concern, it is worth noting that Congress has affirmatively blocked the creation of—one potentially powerful tool: a weapons database.

Nor is it the case that Congress has responded with federal legislation only in areas in which the government itself has some special role in generating, or seeking, the information that might be exposed. Government has no direct role in video rentals and cable provision, an indirect role in healthcare and financial services, and a direct role in education and licensing, and yet all of these areas have received targeted privacy protections. Similarly, although some material would likely appeal more to the private or public sector, the statutes reveal no particular tendency to shelter information from the prying eyes of one or the other. In short, it is not as though only one kind of privacy threat can lay claim to congressional interest—the statutes cover everything from private information for private gain to private information for public disclosure for public gain and public disclosure for private gain.

126. Such programs include the following:

[The refundable portion of the earned-income and child tax credits, which assist low- and moderate-income working families through the tax code; programs that provide cash payments to eligible individuals or households, including Supplemental Security Income for the elderly or disabled poor and unemployment insurance; various forms of in-kind assistance for low-income families and individuals, including food stamps, school meals, low-income housing assistance, child-care assistance, and assistance in meeting home energy bills; and various other programs such as those that aid abused and neglected children.


127. Id.


129. Id. § 926(a). To the extent that this might be explained as a function of the Second Amendment or federalist concerns, it is important to remember that housing and welfare both implicate constitutional values—such as intimate association or family welfare—and also are traditionally state interests.
F. Law Enforcement Access Provisions Preference Subpoenas over Warrants, and Regulate Not Just Acquisition but Also Use

Even recognizing that federal statutes do not just fail to safeguard but actually affirmatively undermine the privacy of the poor with regard to law enforcement, the amount of protection they accord to mainstream interests should not be overstated. Law enforcement exemptions in privacy statutes exhibit a wide range of variation. Some impose intricate requirements, while others provide more vaguely defined standards for access. Interestingly, the variation does not seem to follow any intuitive scaling of protections.\(^{130}\) That is, it is not the case that the areas in which most individuals likely expect the greatest privacy correspond to the strictest statutory standards for access.\(^{131}\) For example, it has been observed that there are greater protections for cable records than there are for health records.\(^{132}\)

Despite wide variation, some general tendencies about law enforcement access can be gleaned. Specifically, with regard to domestic law enforcement access, federal privacy statutes (1) typically allow access pursuant to a standard less than the constitutional default, which is a warrant and probable cause; (2) demonstrate a strong preference for the use of subpoenas, although they often impose additional requirements on the use, transfer, and disposal of information that exceed those mandated by the Constitution; and (3) show a strong preference for advance notice to the individual, when relevant, although they also often contain provisions to delay or circumvent that notice requirement.

Only two privacy statutes condition access for law enforcement using the traditional requirement of a warrant and probable cause, and both of them are constitutionally required to do so. Specifically, Title III imposes a probable cause and highly particularized warrant standard,\(^{133}\) and the PPA restricts (beyond constitutional levels) what information law enforcement can seize from the press and when.\(^{134}\) But these statutes are atypical. Every

\(^{130}\) See infra notes 124–125 and accompanying text. But see supra Part I.D (suggesting that law enforcement’s interest in the regulated material may influence the scope of protection).

\(^{131}\) SLOBOGIN, supra note 14, at 184 (reporting survey results on perceived intrusiveness of various investigative behaviors); SOLOVE & SCHWARTZ, supra note 28, at 442 (“Other federal privacy statutes generally provide stronger protection for third-party records than does the HIPAA rule.”). Similarly, education records get more protection than bank records.

\(^{132}\) SOLOVE & SCHWARTZ, supra note 28, at 442.

\(^{133}\) Arguably, the CCPA provides greater restrictions as well, in that it sets out a requirement of “clear and convincing evidence” as opposed to mere probable cause. 47 U.S.C. § 551(h)(1) (2006). However, the CCPA was amended by the USA PATRIOT Act to ease access for communications provided through a cable company, Pub. L. No. 107-56, § 211, 115 Stat. 272, 283–84 (2001), even though other information remains difficult to access.

\(^{134}\) Each responded to the Court, but in different ways: Title III was enacted in response to the Supreme Court’s findings in Katz v. United States, 389 U.S. 347 (1967), that there was a legitimate expectation of privacy in a phone conversation, and in Berger v. United States, 295 U.S. 78 (1935), that the particularity requirement demanded more than a blanket warrant to authorize a wiretap. The PPA was enacted in response to the Court’s opinion in Zurcher v.
other federal privacy statute, in contrast, allows disclosures based on a warrant and probable cause, but also permits access upon lesser showings, most commonly a court order or a judicial, grand jury, or administrative subpoena.135

In fact, the statutes demonstrate a near-universal preference for the judicial subpoena as the baseline for access. It might be argued that a number of statutes depart significantly from this general rule, in that they allow access pursuant to an administrative subpoena or request.136 For instance, the RFPA allows access based only on written request, assuming no more formal process is available.137 HIPAA likewise provides for an administrative request

Stanford Daily, 436 U.S. 547 (1978), which refused to heighten protection for the press. See generally Bellia, supra note 14, at 300, 309 n.73.

135. There are arguably two exceptions to this rule. First, the Stored Communications Act requires a warrant for a subset of covered material—namely, to compel disclosure of unopened emails in storage for fewer than 180 days. 18 U.S.C. § 2703(a) (2006 & Supp. V 2011). Second, there are a handful of statutes that contain language stating simply that they do not prohibit any “lawful law enforcement . . . activity,” without specifying what that might include. See, e.g., 18 U.S.C. § 1801(c) (2006).

136. Administrative subpoenas are regularly issued by federal agencies seeking to compel the production of testimony or documents in order to execute either an adjudicative or investigatory administrative function. The authority to issue such subpoenas derives from statutory grants of power that typically also prescribe its precise scope. CHARLES DOYLE, CONG. RESEARCH SERV., RS22407, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A SKETCH, at CRS-2 (2006). In the past thirty or so years, the power to issue administrative process in connection with criminal investigations has steadily broadened. Id. at CRS-3. The earliest statute allowed the Attorney General to issue subpoenas in connection with her duties to police controlled substances, Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, § 506(a)-(c), 84 Stat. 1236, 1272-73 (codified as amended at 21 U.S.C. § 876 (2006)); then the Inspector General Act of 1978 bestowed similar power on an authorized Inspector General, Pub. L. No. 95-452, § 6(a)(4), 92 Stat. 1101, 1104 (codified as amended at 5 U.S.C. app. § 6(a)(4) (2006 & Supp. V 2011)). The power now covers criminal investigations as diverse as health care fraud, child abuse, and threats against the president. 18 U.S.C. § 3486 (2006 & Supp. V 2011). This provision of HIPAA was the first to clearly be intended for use in criminal investigations, and unlike its predecessors, it is more protective in its terms. See Doyle, supra, at CRS-3 to CRS-4 (citing 18 U.S.C. § 3486, the administrative subpoena provision added by HIPAA). The War on Terror has revived interest in administrative subpoenas, Risa Berkower, Note, Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations, 73 FORDHAM L. REV. 2251, 2252, 2270-71 (2005), and Congress has taken up the issue several times recently, see, e.g., S. 2555, 108th Cong. (2004); H.R. 3037, 108th Cong. (2003). See generally Berkower, supra.

137. 12 U.S.C. § 3408 (2006). Pursuant to the statute, written requests may be made only where (1) “no administrative summons or subpoena [sic] authority reasonably appears to be available to that Government authority”; (2) agency regulations authorize it; (3) the sought material is “relevant to a legitimate law enforcement authority”; and (4) the notice-and-challenge provisions are followed. Id. Thus, it simply allows law enforcement to “request” the information—it does not compel the institution to turn it over. Compare id. (“Government authority may request . . .”), with id. §§ 3405-3407 (“Government authority may obtain . . .”). Again, I underscore here that my focus is on domestic criminal law enforcement; pursuant to the USA PATRIOT Act, national security letters—initially a fairly circumscribed tool found in the RFPA and ECPA—are now available in a much broader array of situations. Pub. L. No. 107-56, § 505, 115 Stat. 272, 365-66 (2001). Thus, although facially this provision
option, with a lesser standard than that required for subpoenas, orders, or warrants.\textsuperscript{138} The DPPA allows disclosure of highly restricted personal information for use by "any court or law enforcement agency[,] in carrying out its functions," without specifying whether any legal process is required.\textsuperscript{139} FCRA allows access to identifying information (such as name, former and current addresses, and employment history) upon request.\textsuperscript{140} COPPA allows collection, use, and disclosure of information of child internet users without parental consent in cases where "to the extent permitted under other provisions of law," doing so "provide[s] information to law enforcement agencies or for an investigation on a matter related to public safety."\textsuperscript{141} The Privacy Act permits disclosure for "criminal law enforcement activity if the activity is authorized by law, and if the head . . . has made a written request to the agency . . . ."\textsuperscript{142}

But in all of these instances, the disclosure is optional: the entity may disclose the requested information but disclosure is not compelled by law.\textsuperscript{143} In order to compel the disclosure of information to law enforcement, the majority of statutes require at minimum a subpoena or court order.\textsuperscript{144} Of course, may appear to expand authority dramatically, in reality it may be the case that it is invoked only in unusual or exceptional circumstances. See, e.g., Jones v. Dept. of Air Force, 947 F. Supp. 1507, 1512-14 (D. Colo. 1996) (finding that Air Force investigators’ use of written request exception was proper, because, inter alia, although inspector general had administrative subpoena authority, at the time of investigation it was limited by policy to dollar amounts seemingly in excess of those at issue in fraud case). See generally Richard Cordero, Annotation, Construction and Application of Right to Financial Privacy Act of 1978, 112 A.L.R. Fed. 295 (1993) (referring to section 3408 in only one small entry).

\textsuperscript{138} See 45 C.F.R. § 164.512(f)(ii)(C) (2012). There are also provisions for specific law enforcement needs, like locating fugitives or missing persons, reporting victim’s conditions in emergencies, reporting possible homicides, reporting crimes on the premises, or other emergencies. See id.

\textsuperscript{139} 18 U.S.C. §§ 2721(b)(1), 2725(4) (2006) (describing highly restricted personal information to include photographs, Social Security number, and medical or disability information). Personal information (identifying information, including Social Security number and photographs) shall be disclosed in relation to motor vehicle safety and theft functions. Id. § 2721(b).


\textsuperscript{143} The optional nature of compliance allows proponents of administrative subpoena authority to view it as simply allowing the government to bypass cumbersome procedures to obtain information that already is routinely accessed using grand jury subpoenas. However, opponents view it as an end run around the probable cause, particularity, and neutrality standards embodied by the Fourth Amendment, and warn against expanding the categories beyond narrow fields in which limited records would prove relevant (for instance “health fraud” versus “any fraud”). See, e.g., Jameel Jaffer, Panel Report: Secret Evidence in the Investigative Stage: FISA, Administrative Subpoenas, and Privacy, 5 CARDozo PUB. L. POL’Y & ETHICS J. 7 (2006).

normally one would consider a subpoena a lesser threshold of security than a warrant. Judicial subpoenas are typically issued in connection with an investigation or proceeding, pursuant to statutory or other investigative authority, and are limited only by jurisdictional reach and a requirement that they not be "unreasonable or oppressive."\(^\text{145}\) In the federal context, they are commonly issued by grand juries investigating criminal matters; although if a case is pending before a court, the parties may have power to issue subpoenas under the federal rules or, in the case of the criminal defendant, the Sixth Amendment Compulsory Process Clause.\(^\text{146}\) Regardless of the issuer, they are typically issued unilaterally, on a showing of mere relevance, and require neither notice to the opposing party nor permission of a court.\(^\text{147}\) In general, subpoenas are thus considered fairly permissive and powerful access tools.\(^\text{148}\) Similarly, court orders necessitate judicial permission and a pending matter, but are normally available upon only a relevance showing.

But the reliance on devices other than a warrant requirement may offer greater protection for privacy than appears at first glance. Federal statutes often impose additional procedural protections—such as heightened proof thresholds, advance notice, and use restrictions—that exceed the basic probable cause standard applicable to an ordinary warrant. For example, the CCPA requires that the court order be based upon "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be

---

\(^{145}\) FED. R. CRIM. P. 17(c). Significantly, the Supreme Court adapts these standards according to context. It has thus limited trial subpoenas by three requirements: "(1) relevancy; (2) admissibility; and (3) specificity." United States v. Nixon, 418 U.S. 683, 699-700 (1974). In contrast, grand jury subpoenas will be quashed only upon a challenger's showing that there is "no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991).

\(^{146}\) See U.S. CONST. amend. VI; FED. R. CRIM. P. 17; see also United States v. Morton Salt Co., 338 U.S. 632, 642 (1950) ("The judicial subpoena power not only is subject to specific constitutional limitations, which also apply to administrative orders, such as those against self-incrimination, unreasonable search and seizure, and due process of law, but also is subject to those limitations inherent in the body that issues them because of the provisions of the Judiciary Article of the Constitution."); Nixon v. Sirica (In re Grand Jury Proceedings), 487 F.2d 700, 737 (D.C. Cir. 1973) ("Judicial subpoenas seek information in aid of the power to adjudicate controversies between individual litigants in a single civil or criminal case.").

\(^{147}\) FED. R. CRIM. P. 17; R. Enters., Inc., 498 U.S. at 296–300 (referencing subpoena process and relevancy standard for trial and grand jury subpoenas). Many statutes also authorize law enforcement access via a court order, but a court order is by its nature almost always a higher threshold than a subpoena because it requires the express approval of a judicial official. However, because an investigator can petition a court for an order even in the absence of an ongoing formal proceeding or grand jury investigation, it might in some cases be a preferable vehicle for obtaining information.

\(^{148}\) At the same time, we might expect that a judicial subpoena is narrower than either a grand jury or administrative subpoena in that it is issued in connection with a pending matter (rather than an investigation) and is overseen by a judicial officer.
material in the case." Like a warrant, a court order must be granted by a neutral magistrate, but the clear and convincing standard exceeds the warrant's probable cause standard, just as the requirement of materiality arguably does. The VPPA requires that court orders be based on probable cause, which would appear to mirror the warrant requirement. The IRS Code requires that, for non-tax-related investigations, the court order mandate disclosure only to federal law enforcement if there is "reasonable cause to believe, based on information believed to be reliable, that a specific criminal act has been committed" as well as "reasonable cause to believe that the return . . . may be relevant to a matter relating to the commission of such act," and the return "is sought exclusively for use in a Federal criminal investigation or proceeding concerning such act, and the information . . . cannot reasonably be obtained . . . from another source." This "last resort" element represents another departure from constitutional practice, which imposes no requirement that law enforcement attempt to obtain information in a less intrusive fashion before seeking a warrant. In short, although "subpoena" or "court order" seems to be the threshold, the proof requirements often track or even exceed those necessary to secure a Fourth Amendment warrant.

Moreover, with regard to subpoenas, the most common additional requirement is that prior notice be given to the affected individual that the information is sought. Thus, for example, the RFPA, CPPA, VPPA, 

149. 47 U.S.C. § 551(h)(1) (2006). For cable companies that provide phone or internet access, information is available, not including subscriber programming selections, pursuant to Title III, SCA, and the Pen Register Act. See id. § 551(c)(2)(D).

150. Whether it is in fact a higher standard likely turns on whether the statutory terms, which require a showing that "the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case," id. § 551(h)(1), comport with or exceed the particularity requirement of the Fourth Amendment.

151. See 18 U.S.C. § 2710(b)(3) (2006). Again, it is hard to know how to square a court-order provision, requiring probable cause, with a warrant requirement. The VPPA allows access pursuant to a warrant as well as a court order, see id. § 2710(b)(2)(C), implying some distinction between the two. It may be that the only difference is that court orders are available for civil and not just criminal matters.

152. I.R.C. § 6103(i)(1)(B) (2006); see also Treas. Reg. § 301.6103(i)–1 (2012). Disclosure is permitted to state law enforcement agents only for tax offense purposes, I.R.C. § 6103(d), and other limited reasons, see, e.g., id. § 6103(l)(6) (child support enforcement); id. § 6103(l)(7) (benefits programs), while disclosures to federal officials for tax-related offenses do not require judicial process at all, id. § 6103(h).

153. 12 U.S.C. §§ 3405(2), 3406(b), 3407(2), 3408(4)(A) (2006). The statute was amended repeatedly to restrict the notice requirement or allow for delays, such that, for instance, notice to grand jury targets is now forbidden. Id. § 3420(b)(1).

154. 47 U.S.C. § 551(h)(2) (requiring that an individual be given "the opportunity to appear and contest such entity's claim"). It also more generally requires prior written consent for disclosure, subject to a handful of exceptions. Id. § 551(c)(1).

155. 18 U.S.C. § 2710(b)(2)(C), (3) (requiring that all court orders issue "only with prior notice to the consumer," although presumably warrants and grand jury subpoenas could avoid the notice requirement).
FERPA, and PPA all require notice of some kind. Of course, notice is particularly significant with regard to these statutes because nearly all of them cover information held by third parties, and thus disclosure could otherwise occur without the knowledge of the affected person. Nevertheless, the notice requirement is not universal. HIPAA, the Privacy Act, and the DPPA lift an otherwise general notice requirement for its authorized law enforcement disclosures, and many of the statutes supply the government with an avenue for requesting a delay of notice or withholding notice altogether.

The final way in which federal privacy statutes regularly exceed constitutional standards is that they constrain not just the acquisition of material but also its use. For instance, the RFPA strictly regulates the transfer of lawfully obtained financial records, circumscribing their permissible use even in the grand jury and requiring notice to the customer upon transfer. The RFPA’s barriers around use and transfer were replicated in subsequent enactments. By way of additional examples, the VPPA provides for destruction of records and encourages “appropriate safeguards against unauthorized disclosure” for any material accessed through compelled disclosure. The DPPA limits resale or redisclosure of lawfully obtained information, mainly for those uses already permitted by statute. FERPA requires written certification from juvenile justice authorities before disclosure, and further allows the institution to deny access to third parties found to be too lax in redisclosing. The CCPA even requires destruction of information if it is

156. 20 U.S.C. § 1232g(b)(2) (2006). FERPA also segregates “law enforcement records,” which are those created separate from education records and maintained for law enforcement purposes only, and allows them to be accessed only by law enforcement officials of the same jurisdiction. Id. § 1232g(a)(4)(B)(ii). It also has a special provision for state juvenile justice actors, id. § 1232g(b)(1)(E), and designees of the Attorney General monitoring such programs, id. § 1232g(b)(1)(C).


158. 45 C.F.R. § 164.512(f) (2012).


Privacy in the Criminal Justice System

“no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access.”

In sum, although privacy statutes at first blush appear to lower the standard for law enforcement access to covered materials by infrequently imposing a warrant or probable cause requirement, in significant respects they offer greater protection from intrusion in that they may raise proof thresholds, require advance notice of disclosure, restrict subsequent transfer or use, and mandate destruction of records.

In fact, statutory provisions for grand jury, administrative, or judicial subpoenas also afford more protection than does a standard subpoena under the Fourth Amendment because subpoenas in general have been accorded only the barest protection, even when a Fourth Amendment interest is implicated.

Moreover, the Supreme Court has defined the “reasonableness” standards for subpoenas broadly, rarely invalidating a law enforcement request. Accordingly, although the RFPA subpoena provisions clearly fall well below the warrant and probable cause requirement, they are more or less consonant with the lesser “reasonableness” and “relevance”


169. The constitutional law governing the acquisition of evidence through a subpoena duces tecum stands somewhat in opposition to the law governing the acquisition of evidence through physical search and seizure. Whereas a search is governed by Fourth Amendment law, with minimal to nonexistent Fifth Amendment protection, a subpoena is largely regulated through the Fifth Amendment and left only lightly regulated by the Fourth Amendment. See Andresen v. Maryland, 427 U.S. 463 (1976) (holding that the Fifth Amendment was not implicated, and the Fourth Amendment not violated, by search warrant resulting in seizure of business documents); Hale v. Henkel, 201 U.S. 43, 74–76 (1906) (holding that Fourth Amendment did not automatically prohibit subpoena duces tecum issued to corporate officer, but invalidating issued subpoena as unreasonably broad). The Court has not wholly disclaimed application of the Fourth Amendment to subpoena processes; those cases suggest that only the barest regulation applies. However, one source of uncertainty lies in the fact that most cases involve the subpoena or seizure of business, and not personal, documents:

Without attempting to summarize or accurately distinguish all of the cases, the fair distillation, in so far as they apply merely to the production of corporate records and papers in response to a subpoena or order authorized by law and safeguarded by judicial sanction, seems to be that the Fifth Amendment affords no protection by virtue of the self-incrimination provision, whether for the corporation or for its officers; and the Fourth, if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be “particularly described,” if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant.

The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.


170. 2 WAYNE LAFAVE, SEARCH AND SEIZURE § 4.13(a) (4th ed. 2004) (“Although the Supreme Court has stated in dicta that the Fourth Amendment continues to limit the subpoena power of the government, the Court has rejected Fourth Amendment objections to subpoenas in every case it has decided in modern times.”). The Fifth Amendment only comes into play for personal papers sought from the suspect herself, which while not themselves protected, may be protected from compelled production. United States v. Doe, 465 U.S. 605 (1984) (subpoena); Andresen, 427 U.S. 463 (search warrant); see also United States v. Hubbell, 530 U.S. 27 (2000).
requirements generally governing subpoenas for constitutionally protected information. More importantly, the RFPA provides additional procedural protections beyond the Fourth Amendment standard because in most cases the statute imposes notice, use, and transfer restrictions of lawfully obtained records.

G. Available Remedies in the Event of Violation Differ from the Constitutional Standard of Evidentiary Exclusion

Another significant distinction between statutory and constitutional regulation of privacy can be found in the remedies available upon violation, which depart from the customary exclusionary rule. Only two statutes provide for exclusion of evidence as a remedy for violations: Title III and the VPPA. Of course, the exclusionary rule was effectively mandated as regards Title III, because Katz v. United States and Berger v. New York had already made it clear that improper wiretapping violated the Constitution. As for the VPPA, the legislative record does not clearly reveal why it includes an exclusionary remedy. One possibility is that much of the testimony before the committee included examples of law enforcement

171. See, e.g., See v. City of Seattle, 387 U.S. 541, 545 (1967); United States v. Powell, 379 U.S. 48, 57 (1964) (administrative subpoena by IRS did not require probable cause standard); Walting, 327 U.S. at 208-09 (setting out general standard of reasonableness for administrative subpoena and specifically rejecting requirements that particular crime be charged, probable cause exist, or there be narrowest precision in scope of request); see also United States v. R. Enters., Inc., 498 U.S. 292, 298 (1991); United States v. Morton Salt Co., 338 U.S. 632, 641-42 (1950) (distinguishing judicial subpoena power, which “extends only to adjudication of cases and controversies and... [whose] investigative powers should be jealously confined to these ends,” from administrative subpoena, which has more inquisitorial power). The Federal Rules of Criminal Procedure also require that grand jury subpoenas not be “unreasonable or oppressive.” FED. R. CRIM. P. 17(c)(2).

172. Cf. SEC v. Jerry T. O’Brien, Inc., 467 U.S. 735, 741-42 (1984) (holding that the Securities and Exchange Commission target was not entitled to notice of issuance of third-party administrative subpoenas and affirming that Powell governs judicial enforceability of administrative subpoenas and requires that the administrative entity had a “legitimate purpose in issuing the subpoenas, that the requested information was relevant and was not already in the Commission’s possession, and that the issuance of the subpoenas comport with pertinent procedural requirements”). However, it should be observed that subsequent amendments have focused largely on modifying various notification provisions, both to prohibit the financial institution from notifying customers whose records are sought, and to permit the government to delay fulfilling its statutory notice obligations. See Berta Esperanza Hernández, RIP to IRP—Money Laundering and Drug Trafficking Controls Score a Knockout Victory over Bank Secrecy, 18 N.C. J. INT’L L. & COM. REG. 235, 246 n. 78 (1993).

173. 18 U.S.C. §§ 2515, 2710(d) (2006). Of course, the Title III exclusionary rule applies only to oral and wire communications; electronic communications are exempted. Notably, the exclusionary provision is actually broader than the constitutional remedy in that it applies to interceptions by private, not just government, actors. See Orin S. Kerr, Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 HASTINGS L.J. 805, 837 n.154 (2003).

making what were considered abusive demands for information. A more cynical explanation may be that the hearings represented the rare instance in which law enforcement’s interests were underrepresented: the FBI failed to submit comments on the proposed legislation and the DOJ’s comments did not speak to remedies.175

The remaining statutes at best give exclusion of evidence secondary consideration. A couple of statutes arguably permit exclusion by allowing, in the language of the CPPA, “any other lawful remedy available”176 without mentioning suppression expressly, but that seems contingent upon a finding of a constitutional violation. Other statutes imply disallowance of exclusion of evidence as a remedy, such as through a provision that describes a variety of “exclusive” remedies that do not include suppression. Language of that variety can be found in the RFPA,177 SCA,178 and PPA.179 Several statutes expressly prohibit the exclusion of improperly obtained evidence.180

Finally, many statutes are altogether silent on the question of additional remedies, including HIPAA, FERPA, COPPA, DNA, DPPA, FCRA, and the IRS Code. Naturally, litigants have argued that this silence allows for application of the exclusionary rule. For example, defendants have cited HIPAA regulations’ explicit reference to the Fourth Amendment, along with the intimate nature of the covered material, as support for exclusion of evidence as a remedy for privacy violations by law enforcement.181 However, most courts have rejected that contention.182 The same kinds of arguments have

175. See, e.g., supra note 84.
177. 12 U.S.C. § 3417(d) (2006) (“The remedies and sanctions described in this chapter shall be the only authorized judicial remedies and sanctions for violations of this chapter.”); see, e.g., United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986).
178. 18 U.S.C. § 2708 (2006) (“The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.”). The Pen Register Act has also been interpreted to reject exclusion, see, e.g., United States v. Thompson, 936 F.2d 1249 (11th Cir. 1991).
180. In addition, the language prescribing a statutory exclusionary remedy is of particular importance because violations of state constitutional law do not necessarily require suppression of evidence in federal court, whereas a federal statute can effectively bar introduction of evidence in any court. See Kenneth J. Melilli, Exclusion of Evidence in Federal Prosecutions on the Basis of State Law, 22 GA. L. REV. 667, 713 (1988) (noting that although “silver platter doctrine” and Mapp forbid introduction of evidence seized unlawfully under the Fourth Amendment, regardless of court or seizing officer, most circuits have interpreted Elkins as allowing introduction of evidence in federal court seized only in violation of state law).
also been raised and rejected with regard to claims made under FERPA, the DNA Act, FCRA, the Privacy Act, and the IRS Code.

Instead, federal privacy statutes seem to show a strong preference for civil remedies. There exists such diversity among these liability provisions that they defy generalization. It is likewise difficult to judge how well they work, either as a deterrent to violations or as restitution to those harmed. Instead, I will say only that effective civil enforcement requires a party to surmount a variety of hurdles. First, many statutes limit liability to willful or deliberate violations of their terms, and therefore fail to provide a remedy for the likely more common occurrence of negligent or reckless disclosure to law enforcement. Second, damages awards under the statutes may be negligible, given that punitive damages—if authorized—tend to apply only to willful violations, and disclosures of sensitive personal information can be difficult to value monetarily (especially if the consequence of such disclosure is apprehension of a criminal). Third, many statutes provide a good-faith defense for actors behaving in perceived compliance with the statute’s terms, including broad provisions that essentially allow full reliance on law enforcement’s interpretation of the statute. Fourth, recovery can be hampered by various doctrines of immunity, coupled with statutory

185. See, e.g., United States v. Edgar, 82 F.3d 499 (1st Cir. 1996).
187. See, e.g., United States v. Orlando, 281 F.3d 586, 596 (6th Cir. 2002) (“The exclusionary rule is therefore inapplicable to the present case, because any purported violation of § 6103 did not infringe upon Daniels’s constitutional rights.”); Nowicki v. Comm’r, 262 F.3d 1162, 1164 (11th Cir. 2001); United States v. Michaelian, 803 F.2d 1042, 1046–48 (9th Cir. 1986); Marvin v. United States, 732 F.2d 669, 672–73 (8th Cir. 1984).
189. See, e.g., Doc v. Chao, 540 U.S. 614 (2004) (holding that the Privacy Act allows recovery for only actual damages, and therefore denying $1,000 award to claimant who successfully showed that Department of Labor improperly disclosed Social Security number). But see, e.g., Duncan v. Belcher, 813 F.2d 1335 (4th Cir. 1987) (authorizing recovery of damages without proof of actual damages under RFPA).
190. E.g., Title III, 18 U.S.C. § 2529(d); RFPA, 12 U.S.C. § 3417(c); PPA, 42 U.S.C. § 2000aa-6(h). Courts may also interpret law enforcement reliance on statutory provisions later ruled unconstitutional to constitute “good faith,” and thus preclude recovery. See, e.g., United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (holding that even if police acquisition of cell-site data were unconstitutional, police acted in good-faith reliance on SCA).
191. A range of immunity doctrines can impede recovery. Suits against the government require either a federal cause of action (like section 1983 or Bivens) or a state analogue. A state may have sovereign immunity, and a locality’s immunity can be limited by requirements that plaintiffs show a policy, custom, or failure to train with deliberate indifference. Suits against persons in their official capacity raise the specter of qualified immunity if their actions did not, at the time, violate clearly established law. However, it should be noted that federal
limitations (although they appear less often than one might expect), on the ability to sue law enforcement actors, rather than just the entity making the disclosure. At least one statute allows for a private action against the agency, but limits the liability of willfully offending government employees to disciplinary action within the civil service system. Fifth, some statutes—like FERPA, HIPAA, and COPPA—do not provide for a private right of action, but rather depend entirely on public enforcement, and advocates have complained that authorities have been lax. Finally, it is worth noting that a handful of statutes provide for criminal penalties for violations, but an almost equal number do not.

H. Accountability and Transparency Mechanisms
May Be More Readily Available

To the extent that the Fourth Amendment holds law enforcement accountable or renders its abuses transparent, it is largely through the privacy statutes may at times serve as the basis for a claim raised under state law, even where federal law might be unavailing.

192. *E.g.*, Daniel v. Cantrell, 375 F.3d 377, 383–84 (6th Cir. 2004) (dismissing VPPA-based claims against law enforcement officers who obtained video rental records, noting that statute allowed recovery against only the video rental providers). Of course, such a provision particularly matters in the absence of an exclusionary rule, since a defendant whose information is improperly disclosed by a third party relying on law enforcement representations may have neither a route for civil redress (due to the third party’s good-faith defense, and the lack of a cause of action against the officer) nor one for criminal redress (because the exclusionary rule does not apply).


195. *See, e.g.*, SOLOVE & SCHWARTZ, supra note 28, at 439–40 (describing lack of any enforcement actions in first three years of HIPAA); Solove, supra note 35, at 1168–69 (“Although the Privacy Act requires an individual’s permission before his or her records can be disclosed, redress for violations of the Act is virtually impossible to obtain.”). The Department of Health and Human Services now maintains a website that highlights its enforcement efforts, which have significantly increased. See U.S. DEP’T OF HEALTH & HUMAN SERVS., Health Information Privacy, http://www.hhs.gov/ocr/privacy (last visited Oct. 12, 2012).


exclusionary rule. So given that legislators seem to disfavor the exclusionary rule, are there other means through which they secure compliance? Examination of privacy laws reveals strengths, such as the imposition of heightened transparency and recordkeeping requirements, as well as weaknesses, in the form of lack of accountability.

First, of course, statutes may impose civil, criminal, and administrative penalties for violations. But as the previous Section explains, such remedies do not always serve an accountability or deterrent function, due to the improbability of successful judgment or recovery. Second, although the notice requirements contained in the majority of federal statutes might suggest that a record is generated whenever a party lodges a request (whether a written letter, subpoena of some kind, or court order), which then might be amplified by any resulting proceedings, in reality it can be difficult to aggregate such information in the absence of a specific directive to do so. Thus, while there might in the abstract be a paper trail of administrative subpoenas issued pursuant to the VPPA, and a concomitant record of any related judicial challenges or hearings, such information is virtually impossible to assess comprehensively.

Third, federal privacy statutes show no consistent commitment to ensuring structural reform or systemic change, which can be difficult to achieve through individualized remedies. As Paul Schwartz noted, for example, "The Privacy Act does not give federal courts the power to order agencies to change their data processing practices." To be sure, there are some exceptions: the DPPA authorizes imposition of a daily fine of $5,000 on a DMV office shown to have a policy or practice of noncompliance, and HIPAA, FERPA, and the DNA Act all (at least in theory) condition benefits on evidence of structural compliance. Significantly, all of those actions are dependent on a public official bringing suit.

Although forcing compliance may be difficult, many federal privacy statutes—especially those that apply to government release of information—nonetheless enhance accountability by imposing documentation and public-reporting rules. Most classically, Title III imposes a raft of re-

198. Of course, there is much academic debate regarding the actual effectiveness of exclusion, but in principle the doctrine provides both an incentive for law enforcement to conform its behavior to the constitutional standard as well as a mechanism for law creation, norm setting, and public transparency.

199. In other words, although a statute may provide an individual remedy for violations—in the form of damages or an injunction, say—a party cannot necessarily seek the kind of structural reform necessary to ensure broad future compliance. Solove, supra note 35, at 1168–69. Many statutes do allow for equitable remedies, but that does not necessarily mean that a court will use its power to order a fundamental reconfiguration of an institution's practices.


201. 18 U.S.C. § 2723(b).

porting requirements that generate detailed records of all wiretaps sought and granted under its provisions. FERPA likewise requires that entities record all requests for access, "indicat[ing] specifically the legitimate interest that each . . . has in obtaining the information," and mandates the creation of an office and review board within the Department of Education for the purposes of investigating violations. The IRS Code requires "compliance with a comprehensive system of administrative safeguards and record keeping requirements" that has "been strengthened over the years." The CMPPA compels regular congressional reports and creates a "Data Integrity Board." In contrast, recordkeeping requirements are less commonly found in statutes that regulate disclosures made by private entities, such as the VPPA (video rental agencies), FCRA (credit agencies), or COPPA (online service providers).

Notably, such requirements seem particularly susceptible to erosion: several statutes initially contained strong reporting standards that were subsequently reduced or eliminated. For instance, the Privacy Act initially required biennial reports to Congress, but that requirement was effectively repealed. Similarly, the RFPA initially ordered an annual report to Congress documenting all applications for delay of notice filed by the government and all customer challenges, as well as a report on government requests for financial records, but that rule was repealed in 1992.

In sum, whereas the imposition of accountability mechanisms like reporting requirements or oversight boards arguably achieves more protection for privacy rights than imposition of an exclusionary rule, there remains troubling inconsistency across statutes both with respect to imposing and monitoring those standards. Even still, given the choice between relying on the application of the exclusionary rule—which is notoriously unsatisfying

---

203. 18 U.S.C. § 2519. However, a wide array of experts have agreed that "Congress . . . bungled even a relatively easy task—the creation and maintenance of a system for systematic collection of telecommunications surveillance statistics." Schwartz, supra note 68, at 919.

204. 20 U.S.C. § 1232g(b)(4).

205. Id. § 1232g(g).


207. 5 U.S.C. §§ 552a(u), 552a(s) (2006).


in that it rewards the criminal for the "constable's blunder"—and requiring entities to generate data that would record and publicize the whole breadth of police investigative activity, many privacy advocates would undoubtedly choose the latter.

1. Federal Privacy Statutes Tend to Set Floors, Rather than Ceilings

A common criticism of Fourth Amendment law is that it nationalized the work of policing and prosecution, a historically state and even local affair. Congressional action, particularly in this political environment, likewise raises questions about the proper extent of federal power. States have always been and continue to be active regulators of personal privacy. As Paul Schwartz observed, "[S]tates have often been the first to identify areas of regulatory significance and to take action." Accordingly, this Section considers the federalism question from three perspectives: (1) the degree to which federal statutory privacy laws focus on traditionally federal concerns, as opposed to areas of traditional state concern; (2) whether and under what general conditions federal statutory privacy laws preempt their state counterparts; and (3) whether and under what conditions federal laws appear to influence or exert pressure on states to enact their own privacy provisions or vice versa.

Assessing federalism interests is never a simple affair, but it is particularly complicated with regard to criminal justice. There are multiple variables that may be involved, including the nature of the requesting official (federal or state), the nature of the authority under which a request is made (for instance, the Pen Register Act allows state officials to use the federal law), the forum in which the request is litigated (federal or state courts), and the scope of any exclusionary or evidentiary rules that might apply in that forum. Suffice it to say that it is beyond the purview of this Article to explore every permutation of these variables with regard to each statute, so my goal in this Section is instead to draw broadly applicable conclusions that might illuminate the federal question, albeit from afar.

First, federal privacy statutes extend beyond the conventional federal domain. At one end of the continuum is a statute like the Privacy Act, which applies only to federal agencies. Next along might be something like the RFPA, which applies broadly to financial institutions, a typical federal concern, and only restricts disclosures made to federal agencies and officials. Then might sit statutes such as ECPA, FCRA, and arguably even HIPAA.
which have strong state and local dimensions but speak so centrally to interstate commerce that even a parsimonious interpretation of federal power would justify intervention.

But a handful of statutes cover issues typically entrusted entirely to states or localities. FERPA addresses education; CCPA addresses the provision of cable services; the DPPA addresses driver's licenses; and VPPA addresses video rentals. In the increasingly globalized village, each of these areas obviously has the capacity to significantly impact interstate and even international concerns. Nevertheless, they are also historically sites of strictly local- or state-level control.\footnote{A parallel argument might be made of statutes federally criminalizing privacy-intrusive behavior, such as the Video Voyeurism Act.\footnote{Of course, it bears admitting that Congress has also enacted privacy laws that indirectly protect states' rights: in order to prevent the creation of centralized firearm registries, Congress passed a law prohibiting any rule or regulation that requires federally mandated firearms licenses be maintained such that “any system of registration of firearms, firearms owners, or firearms transactions or dispositions be established.”\footnote{In fact, litigants have raised, and courts have largely rejected, federalism complaints about privacy statutes. In Reno v. Condon, the Supreme Court heard a challenge to the DPPA based on a claim that it exceeded the commerce power and violated the Tenth Amendment.\footnote{In its brief unanimous opinion upholding the Act, the Court summarily rejected the State's argument, noting that the “DPPA regulates the States as the owners of data bases,” rather than commandeering employees or mandating passage of particular laws.\footnote{If the DPPA offers any guidance, it seems that a significant measure of federal privacy regulation of traditional state tasks can withstand constitutional federalism challenges.\footnote{To the extent that Congress possesses and has used relatively broad power to regulate privacy, it then remains to inquire into the relationship between the substantive content of that regulation and the residual power left to the states. Have federal privacy statutes on balance set floors for privacy upon which states are able to heap additional protections, or have they established ceilings beyond which no additional safeguards may ascend? A statute such as the RFPA provides a good illustration of the inherent}}}}}}}}  

complexity of answering that question: the RFPA is limited to requests by federal officials and allows states to impose more restrictive privacy practices in some cases, but it also contains provisions that preempt state laws with regard to certain kinds of requests for information.

Nevertheless, some rough conclusions may be drawn. Federal privacy enactments appear to have set baselines for protection that states can, and have, enhanced with their own enactments. A wide range of statutes explicitly contain provisions preempting state laws that lessen protection but expressly permitting state laws exceeding federal standards. Such statutes include the VPPA, HIPAA, the Wiretap Act, FERPA, CCPA, and GLB. The SCA goes a step further, showing deference to state law by requiring that court orders "not issue if prohibited by the law of such State." In contrast, only two federal privacy statutes expressly preempt not just directly conflicting state legislation but also any state legislation that would exceed their scope. Specifically, the Fair and Accurate Credit Trans-


actions Act amendments to the FCRA prohibit states from enacting laws that would impose higher standards on consumer reporting agencies, and COPPA likewise requires that "[n]o State or local government may impose any liability . . . inconsistent with . . . this section." Perhaps tellingly, those two statutes deal directly with national commercial interests—precisely the situation in which uniform privacy standards have been proposed as most desirable.

Naturally, the complete picture of preemption is far more complicated. Although federal privacy statutes generally do not preempt more privacy-protective state enactments, in reality they cast shadows—both formal and informal—that are longer than may first appear. The partial-preemption provisions of HIPAA have been criticized as "'vague and confusing,' 'abstruse and unworkable,' and burdensome, with the potential to 'create a compliance nightmare for which no obvious answers exist.'" A handful of cases—including the high profile attempt by the Department of Justice to obtain the medical records of women who received late-term abortions—have squarely confronted the conflict between HIPAA's rather broad law enforcement exemption and state confidentiality provisions, with mixed results. FERPA has similarly received criticism for ostensibly setting a floor for privacy but in effect opening a door for federal legislators to meddle in classic state concerns. Similar ambiguities arise with respect to Title III and the SCA. For example, Title III clearly sets a federal floor for wiretaps,

230. Id. § 6502(d).


233. Compare Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004) (quashing subpoena on ground of undue burden on hospital when weighed against patient privacy and limited probative value, but otherwise finding Illinois patient privilege inapplicable in federal question suits like the one at issue), with Nat'l Abortion Fed'n v. Ashcroft, No. 03 Civ. 8695(RCC), 2004 WL 555701, at *6 (S.D.N.Y. Mar. 19, 2004) (finding that HIPAA did not incorporate state privacy statute that was more stringent than federal standard and thus disclosure of medical records was permitted under federal evidence rules, which do not require compliance with state privacy law).

and thus preempts any conflicting inferior state law, but an argument can be made that ECPA's provisions regarding stored communications (as opposed to intercepted communications in transit) are not likewise preemptive. Nonetheless, the ultimate conclusion of this Section—that federal statutory privacy tends to lay floors rather than raise ceilings—seems sound.

As a final piece in the federalism picture, I want to say a word about the influence that federal statutory privacy plays in prompting state regulation, and vice versa. It is certainly true that states have often been the first movers in enacting privacy protections, and that this movement has in turn prompted federal legislation. From the breadth of provisions detailed above, it also seems fair to conclude that Congress’s broad Commerce Clause and Spending Clause powers have allowed it to reach a wide range of interests, and that to the extent that coverage exhibits gaps or holes, it is unlikely that we can attribute most of them to a lack of perceived or actual power on the part of federal regulators.

At the same time, it is also true that in many cases, “states simply mimic or expand upon existing federal regulation, and state regulation is largely attributable to the momentum of federal regulation.” Of particular interest to criminal justice, one researcher observes that states seem particularly responsive with regard to “quasi-constitutional provisions regulating official conduct,” whether in response to federal decisions that set floors (like Katz) or that expose important gaps in constitutional protection (like United States v. Miller, Smith v. Maryland, or Zurcher v. Stanford Daily).

As it is difficult to assess whether state or federal legislators are more inclined to act first and under what circumstances, it seems that for now the best we can say is that the evidence is inconclusive. In other words, “[t]he existence of substantial state regulation of information privacy does not con-

235. See Leonard Deutchman & Sean Morgan, The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors, AM. PROSECUTORS RES. INST., 6 (Jul. 2005), http://www.ndaa.org/pdf/ecpfa_isps_obtaining_email_05.pdf (“Because there is a difference between the Fourth Amendment rights protected under Title III and the statutorily-created rights found in the SCA provisions of the ECPA, and because the preemption language of Section 2516 so clearly applies solely to Title III, it can be argued that federal law regarding stored electronic communication (e-mail) does not preempt and control state law as does federal wiretap law.”).


237. Consider the RFPA, for instance. Although it only applies to requests by federal officials, it does not seem to make that choice out of legal necessity given the broader reach of companion statutes. See supra note 220 and accompanying text.

238. Bellia, supra note 236, at 889.

239. Id.; see also Smith v. Maryland, 442 U.S. 735 (1979) (holding that there was no protectable interest in the numbers keyed into a telephone); Zurcher v. Stanford Daily, 436 U.S. 547 (1978) (holding that the First Amendment press right did not block execution of a warrant); United States v. Miller, 425 U.S. 435 (1976) (holding that financial records handed over to a third-party financial institution receive no Fourth Amendment protection).
firm that competitive federalism is thriving—nor does the fact that states are often followers of federal action suggest that it is not.240

J. Relative Flexibility of Statutory Enactments

The last observation about federal privacy law relates to its capacity to adapt to changing circumstances. Examination of federal privacy law suggests that while Congress does, in fact, undertake substantial revisions on occasion, it has also shown reluctance, or inability, to keep up with the times. Specifically, this Section shows that Congress has not always proven adept at maintaining the currency of legal standards. As a result, the existence of individual privacy has occasionally hinged on arbitrary distinctions. For example, important statutory distinctions in the ECPA have notoriously been rendered obsolete with the passage of time, and other provisions may turn on arbitrary considerations, such as whether a website is accessed through an iPad or a desktop computer, whether a video recording has audio, or whether a caller uses a cordless phone.241

To the extent that statutes do maintain flexibility, such flexibility results as often from careful (or fortuitous) drafting that allows for expansive judicial interpretations as from subsequent amendment. For instance, because the VPPA covers not just “prerecorded video cassette tapes” but also “similar audio visual materials,” courts could readily interpret the statute to include DVDs and other materials.242 In this respect, any flexibility in a statutory enactment derives from common law principles of statutory interpretation.

Nevertheless, Congress has shown an ability to adapt to changing circumstances. Amendments to FERPA addressed concerns about victim access to law enforcement records held by educational institutions. The CMPPA updated the Privacy Act to address the advent of technologies capable of mining data for information. The CCPA was amended when it became clear that cable technology would be used not only to transmit passive images but also to provide internet and voice services. And financial and health regulations have been amended to address the rise in electronic data transfer and e-commerce.

In sum, although Congress has demonstrated some willingness to amend and enact laws that reflect contemporaneous concerns, it has also demonstrated a stubborn resistance or woeful incapacity to rectify obviously flawed and outdated provisions. In addition, many of its most successful statutes have endured largely because of vague terms that can be adapted by

240. Bellia, supra note 236, at 890.
242. “[I]n construing the scope of the Act, this Court must strive to protect this aspect of an individual’s right to privacy in the face of technological innovations that threaten this fundamental right.” Dirkes v. Borough of Runnemed, 936 F. Supp. 235, 239 (D.N.J. 1996).
judicial officials to apply to changed circumstances, suggesting that courts have their own adeptness in keeping up with the times.

***

In closing, a survey of federal privacy statutes reveals a range of insights: they emerged in the late twentieth century; they are sectoral rather than comprehensive in scope; they are largely motivated by technological developments; they primarily protect the privacy of individuals, most especially those in the socioeconomic mainstream; they universally provide for law enforcement access to covered material; law enforcement access typically departs from the warrant and probable cause default of the Fourth Amendment, but often imposes additional standards such as the regulation of use and not just acquisition or the requirement of prior notice; the statutes strongly disfavor the exclusionary rule remedy and are more inclined to impose private civil or public enforcement remedies along with criminal penalties; many of those penalties, by law or in practice, are meaningful only in the event of willful or deliberate breaches; the statutes occasionally, but not uniformly, impose mechanisms for structural accountability or transparency; they reflect no clear commitment to or against federalist principles; and they are not immune to ossification. The next and final Part attempts to use these observations as a means of shedding some light on the debate between constitutional and legislative regulation of privacy in the criminal justice system.

II. Lessons

What do the foregoing observations tell us about privacy in the criminal justice system? In particular, how might they inform our understandings about the respective roles played by Congress and the courts in regulating privacy? How might these revelations answer larger questions about the role that each branch might play in regulating privacy? Two conclusions present themselves. As Section II.A shows, these observations dispute a number of popularly held ideas about the roles of each institution, even while confirming some intuitions as true. As Section II.B argues, the task of regulating privacy in the twenty-first century may simply be so complex that neither institution should claim exclusive control or even be preferred to take the lead. Rather, an approach of collaborative constitutionality is necessary to achieve optimal levels for protecting privacy.

A. Myths Dispelled

As Part I demonstrates, close review of privacy statutes both affirms and disputes several long-standing intuitions about the relative role played by each branch in regulating privacy in the criminal justice context. By way of affirmation, three things are clear: First, Congress has in fact shown a special affinity for addressing technology-based threats to privacy, while
generally ignoring non-technology-based ones. Second, Congress has proven more adept than the courts at implementing mechanisms for systemic oversight of privacy practices, as well as for reform of noncompliant institutions. And third, only courts have shown a strong preference for the exclusionary rule as a remedy for law enforcement violations of privacy rules; legislatures instead rely on a constellation of other tools for such constraints.2

At the same time, my survey reveals several important insights at odds with conventional beliefs. First, in many respects, statutes turn out to protect privacy rights more than the constitutional warrant and probable cause requirement. For example, statutes might require advance notice, allowing the individual the opportunity to seek counsel and initiate adversary proceedings to determine disclosure. They can further amplify the proof standard from general probable cause by requiring clear and convincing evidence, tailored showings of relevance, or exhaustion of other methods. And statutes can impose a wide array of restrictions on the use of lawfully obtained information, such as restricting its subsequent transfer or mandating its destruction. In contrast, the Constitution, when applicable, tends at most to regulate acquisition of information by imposing an ex parte warrant requirement, based only on probable cause and with broad latitude for what constitutes “particularity.” Moreover, constitutional standards rarely reach beyond the moment of acquisition; once law enforcement lawfully obtains information, it is free to use that information however it should wish.

Second, it is not clear that the political processes do a better job than courts of airing and weighing the concerns of all relevant constituencies. Although in theory they might, in practice that rarely seems to be the case. This may call into question two critical assumptions favoring legislative supremacy made by Professor Kerr and others: that legislatures are better poised to gather facts about new technologies, and that “privacy rules present relatively few opportunities for rent-seeking” behavior by special interest groups.244 Part I suggests that law enforcement has a clear and constant voice in the political process, whereas the interests of privacy tend to be represented by groups interested less in privacy vis-à-vis policing (and the poor that make up the vast majority of criminal defendants) than privacy as experienced by the middle and upper classes.

In contrast, in a Fourth Amendment hearing, the government has a strong voice and advocate in the form of the prosecution, but a specific defendant must represent the privacy of the policed classes (often poorly, in the sense of either the lawyer’s capabilities or the ubiquity of that client’s interests). This is not to say that one institution has always done a better job

---

243. Of course, an empirical determination of which remedy is more effective is beyond the scope of this Article.

than the other. Rather, it simply suggests that neither the Court nor Congress at present seem particularly inclined toward protecting the privacy of socio-economically vulnerable groups, and neither the Court nor Congress has proven more or less willing to consider the needs of law enforcement.

As an added complication to this picture, it is important to note an emerging corporate interest in the continual expansion of police investigative technologies. Most technological surveillance devices are developed, marketed, and maintained by private sector industries, not nonprofit or government entities. Private, profit-motivated industries have strong financial interests in expanding the use of GPS tracking devices, biometrics, and other investigative tools for law enforcement purposes. Thus, contrary to the notion that there are few rent-seeking actors in criminal justice, in fact there are strongly motivated and highly organized interest groups to lobby for rules that promote the purchase and use of their products. Of course, in some cases, entities that operate technologies used by the mainstream population may have an interest in protecting the rights of their consumers—thus internet service providers may balk at disclosing information that their customers would find invasive, or wireless providers may fight against intrusive requests. Nevertheless, as Part I shows, legislators can easily minimize such problems by providing legal safe harbors for compliance with requests, and even by mandating nondisclosure ("gag orders") to ward off public relations nightmares.

Third, despite claims to the contrary, constitutional standards are not clearly more intricate, opaque, or inflexible than statutory standards. Statutes have an equal if not greater capacity to be unclear, vague, and convoluted. In other words, it may be just as hard for the officer on the beat to know the intricacies of a statutory rule as those of a constitutional one. Moreover, it is not the case that Congress regularly amends privacy statutes as they become obsolete; provisions like ECPA or the VPPA are hardly current, and have stayed relevant at best due to creative interpretation on the part of judges. Similarly, the flexibility of common law adjudication means that courts can in fact adapt constitutional rules over time rather easily as circumstances change, and that courts do in fact adapt statutory rules if given proper latitude.

Finally, there are clearly some areas about which the evidence regarding relative strengths is in equipoise. For instance, in opposition to those who claim that constitutional rulings trammel the interests of states, it is not obvious that statutory enactments are more likely to be respectful of federalist principles. Many statutes actively preempt contradictory state laws, or set up

---

245. As I explain in a manuscript currently in progress, many contemporary tools of criminal justice (such as DNA, drug analysis machines, and even computer software) rely upon the development of materials and instruments by the private sector.

Privacy in the Criminal Justice System

such a confusing web of preemption that it requires judicial intervention to elucidate the permissible bounds.

Nor is it evident that either institution can lay claim to a superior means of enforcing its rules. The exclusionary rule, practiced almost exclusively by the courts, obviously has a long and controversial history. And yet its continued endurance, even in the wake of recent erosion, speaks to the lack of clearly suitable alternatives. To that extent, the statutory provisions that mirror those alternatives—say, by providing for civil remedies or disciplinary sanctions—arguably serve to deter lawless police action no more effectively.

However, it does seem that Congress alone has demonstrated a willingness, even if imperfectly executed, to impose structural checks that do more to deter violations ex ante than might ex post alternatives. Statutes like FERPA or the DPPA that allow for interventions at the institutional level may end up preventing larger numbers of inadvertent improper disclosures than case-by-case adjudication (whether criminal or civil) ever could. And mandating disclosure of police investigative activity may bring to light abuses perpetrated against persons found to be innocent, something that current Fourth Amendment doctrine wholly obscures, with its focus on an exclusionary rule that by its nature brings to light only cases in which evidence is in fact found during the search.

B. Rethinking the Processes of Privacy

What then does all this mean for the optimal allocation of power between these two branches in regulating privacy? The answer, of course, must in large part turn on one’s own preconceptions about the optimal degree of privacy protection. However, it is not my intention to engage that debate here or persuade any reader that my own privacy-protective inclinations represent the ideal. While acknowledging that the two have a relationship to one another, my effort is focused more on enhancing the legal processes by which privacy is defined in our society than on advancing a particular substantive agenda about what that privacy ultimately might be.

I argue in this Section that it is undesirable for either the Court or Congress to assume sole or even primary responsibility for regulating privacy in the twenty-first century. The task is simply too complex to leave to one or the other: Congress has proven too reluctant to take the lead without prompting (whether from the Court or from popular events), and the Court has proven too hesitant to grant certiorari or to confront headlong cases raising technology-based questions. Instead, the ideal would be to draw on the relative strengths of each institution to compensate for the other’s weaknesses: courts can benefit from the democratic accessibility and credibility...
of legislatures, and legislators can benefit from the moral authority and insulation from interest-group politics that judges enjoy. Building on the literature on collaborative constitutionalism and interbranch dialogue,\textsuperscript{249} I propose that the branches should work cooperatively to define and protect privacy as regards criminal justice interests. And though my proposition applies most directly to intrusions enabled by new technologies, since that appears to be the area where Congress has demonstrated the greatest willingness to act, it could in theory apply more broadly to any of the interests enveloped by the Fourth Amendment.

The history of criminal justice privacy already contains several examples of one model of such collaboration. Perhaps most famously, the Berger and Katz opinions, which respectively invalidated a New York wiretap law and held wiretapping to be a constitutionally protected activity, exemplify a process by which the Court declares that an investigative method implicates a Fourth Amendment interest and then sketches the contours of a constitutional statute regulating the activity.\textsuperscript{250} Erik Luna terms this process “constitutional roadmapping,” and uses examples such as Morales\textsuperscript{251} and Dickerson\textsuperscript{252} to explore its strengths and weaknesses.

But that approach, while arguably effective, teeters too closely to paternalistic oversight of Congress by courts. Although it utilizes the strengths of courts—to protect against a core infringement of rights and enforce procedural floors—it dismisses the relative power of legislatures to offer more

\textsuperscript{249} Several models of such cooperative rule elaboration have been proposed over time. \textit{See}, e.g., \textsc{Bruce Ackerman}, \textsc{We the People: Foundations} 5 (1991); \textsc{Alexander M. Bickel}, \textsc{The Least Dangerous Branch} (2d ed. 1986); \textsc{Cass R. Sunstein}, \textsc{One Case at a Time} (1999); Benjamin Cardozo, \textit{A Ministry of Justice}, 35 \textsc{Harv. L. Rev.} 113 (1921). This approach perhaps draws most directly from Guido Calabresi’s idea of the “second look,” \textsc{Guido Calabresi}, \textsc{A Common Law for the Age of Statutes} (1982), and Erik Luna’s notion of constitutional roadmaps, Erik Luna, \textit{Constitutional Road Maps}, 90 J. \textsc{Crim. L. \& Criminology} 1125 (2000). With specific respect to criminal justice, Peter Swire proposed a beefing up of the expectation-of-privacy test, as well as a procedural test for high-tech surveillance. Swire, supra note 16, at 924–30.

\textsuperscript{250} \textsc{Katz v. United States}, 389 U.S. 347, 353–56 (1967); \textsc{Berger v. New York}, 388 U.S. 41, 54–56 (1967). In contrast, opinions like \textsc{Smith and Miller} arguably rest on the other end of the same continuum—they declare certain activity untouched by constitutional rules (pen registers, bank records) and leave it to Congress to decide whether to act. \textsc{Smith v. Maryland}, 442 U.S. 735, 741–42 (1979); \textsc{United States v. Miller}, 425 U.S. 435, 442–43 (1976). The Privacy Protection Act of 1980 perhaps offers an example of the principle at work, although in a counterintuitive fashion, as there the legislature decided to enhance the threshold imposed by the Constitution. 42 U.S.C. §§ 2000aa to 2000aa-12 (2006); \textit{see also} text accompanying note 127.


\textsuperscript{252} \textsc{Dickerson v. United States}, 530 U.S. 428 (2000) (invalidating a statute intended to override the ruling that created the \textsc{Miranda} warnings for suspects).

\textsuperscript{253} \textsc{Luna, supra} note 249, at 1127–28. Ultimately, Luna is “not convinced that constitutional road maps are inevitably superior or inferior to other dialogic strategies, or that they will, in fact, increase interbranch dialogue in particular cases.” \textit{id.} at 1241.
granulated responses to protect cherished rights. By essentially scripting a constitutional rule, courts using this approach may simply dictate the terms of the statute to Congress and strip the legislature of all incentive to look to its own strengths, including its ability to set broad terms of compliance that are more innovative than the customary expectations of courts, such as a warrant, probable cause, or the exclusionary rule.

For this reason, a preferred template for the kind of constitutional collaboration that I am imagining might be found in more obscure cases such as *South Dakota v. Opperman*\(^{254}\) or *Florida v. Wells*.\(^{255}\) In those cases, the court addressed the constitutionality of a search conducted pursuant to the so-called “inventory exception,” and found that the police action was constitutional if it had complied with a preestablished policy, but unconstitutional if conducted ad hoc or with unconstrained discretion.\(^{256}\) The precise terms of the policy were less important than the existence of the policy and the fact of its regularity. The critical fact was ex ante constraints on discretion, suggesting that a degree of variation in search policies is not only permissible but expected. Another provision of the Constitution models just such an approach: the Third Amendment states, “No Soldier shall, in time of peace be quartered in any house... but in a manner to be prescribed by law.”\(^{257}\) Such language emphasizes that it is the principle of legality that controls constitutionality.

Similarly, the Court might address Fourth Amendment questions with a greater emphasis on procedural, rather than substantive, review. In recognizing constitutional interests, the Court would still assume an agenda- and baseline-setting role.\(^{258}\) But rather than find that any police action that implicates the Fourth Amendment automatically requires a warrant and probable cause, the Court could rely on the “reasonableness” clause of the Fourth Amendment and focus instead on the quality of safeguards aimed at protecting the interest. Indeed, the substantive nature and scope of such safeguards might vary dramatically, and yet the police action would remain constitutional. Constitutional review would thus look more like a checklist of components than the current alternatives: the rejection of any constitutional interest resulting in a total lack of constitutional scrutiny; application

---


\(^{255}\) 495 U.S. 1 (1990) (invalidating under inventory-search exception a search in which closed containers were opened because the jurisdiction lacked a policy concerning the opening of containers).

\(^{256}\) *Wells*, 495 U.S. at 4–5; *Opperman*, 428 U.S. at 374–76. This exception permits law enforcement to conduct warrantless searches of impounded property for the purpose of taking inventory. See *id*.

\(^{257}\) U.S. CONST. amend. III (emphasis added). I am grateful to Peter Swire for this observation.

\(^{258}\) Akin to Rick Hills’s suggestion that state laws can prompt business interests to put topics on the federal agenda because those interests seek federal preemption, Roderick M. Hills, Jr., *Against Preemption: How Federalism Can Improve the National Legislative Process*, 82 N.Y.U. L. REV. 1, 19–20 (2007), judicial rulings can similarly prompt law enforcement to put topics on the federal agenda for the same reason.
of one-size-fits-all, one-shot warrant and probable cause requirements; or ad hoc formulations of "reasonableness" rules.

Significantly, Justice Sotomayor's visionary concurrence in United States v. Jones took a step in this very direction. Recognizing the changing nature of police information gathering, she suggested that the executive branch might require "oversight from a coordinate branch," and intimated that the Court should "cease[] to treat secrecy as a prerequisite for privacy." Although she did not elaborate on what she considers to be the proper role, if any, of courts in applying the Fourth Amendment to a new method such as GPS testing, her comments leave room for the possibility that something other than conventional Fourth Amendment analysis might be allowed.

To lay out with greater specificity just what such review would look like, Professor Peter Swire and I recently drafted a proposal that envisions four steps. First, the court would determine whether a constitutional interest was at stake—in other words, whether a "Fourth Amendment moment" had occurred. If such a moment were established, then the court would ask whether there were any formal limits on the exercise of law enforcement discretion. Here, we imagine the limits as either legislative- or executive-branch policies, spelled out and formalized in advance, which would govern the activity. If no such limits on discretion existed, then the intrusion would be presumptively unreasonable under the Fourth Amendment. If such standards did exist, however, the third step would be to review the reasonableness of those standards. This scrutiny would be structural and systematic, with a high degree of deference as explained in greater detail below. Finally, if the standards were found to be reasonable, then the last step would be to determine whether the police action had complied with those standards. If so, the activity would be deemed constitutional.

So how would procedural review unfold? The core tasks would be to ensure that there were such entities charged with outlining policies, that the processes for devising them were known to the electorate, and that the ultimate policies were not grossly unjust. Preference should be given to limits elaborated legislatively, rather than through executive discretion, although the latter should be met only with greater skepticism, not presumptive invalidity. Moreover, because the pace of technological change may make it difficult for legislatures to elaborate the substantive standards governing a

259. 132 S. Ct. 945, 954–57 (Sotomayor, J., concurring).
261. Justice Alito's concurrence likewise suggested that legislative action might be desirable; but whereas Justice Sotomayor's opinion broaches tantalizing ideas about new forms of constitutional review, Justice Alito's opinion arguably suggests that in the future the Court would willingly defer—perhaps even wholesale—to legislative enactments. Id. at 964 (Alito, J., concurring in the judgment) (noting the absence of federal legislation regarding the use of GPS trackers, and thus concluding that "[t]he best that we can do in this case is to apply existing Fourth Amendment doctrine").
particular investigative method (for instance, which GPS tracking devices or DNA loci should be used at a given time), such decisionmaking may be delegated to more responsive, but nonetheless accountable, administrative bodies. Such entities would preferably maintain a neutral stance, with a balanced composition of interests. Regardless, courts would be well situated to review the regulatory output of such a body, as they have long played a role in reviewing the procedural fairness and regularity of administrative entities in other contexts.

Although it is impossible in the abstract to provide a list of necessary standards, because they would inevitably change according to the nature of the investigative technique at issue, policies should at minimum share two basic features: they should contain terms that cabin police activity, and they should provide mechanisms for transparency and accountability. Importantly, legislative and executive actors should retain flexibility in choosing how to satisfy these two criteria. Oversight is not intended to place the court in the position of routinely second-guessing the substantive legislative or administrative judgments, nor is it intended to necessarily review the output of those bodies.

Of course, the success of this proposed approach requires that the Supreme Court relax Fourth Amendment conventions beyond its preferences for warrants, probable cause, and the exclusionary rule. Thus, no regulatory constraints should be inherently off the table. For example, courts should remain receptive to, and recognize as constitutionally legitimate, regulatory terms like the one posited by Justice Alito in Jones, which suggested that the substantive nature of the alleged offense might dictate the scope of permissible police activity. More radically, the exclusionary sanction would no longer constitute the sole or even primary permissible constitutional remedy in the event of a violation. In lieu of excluding evidence, for instance, a statute might require strict recordkeeping of surveillance efforts along with regular assessments of the success of those efforts, and it would be the courts’ job simply to ensure that both were actually taking place. Constitutional review would, in the first order, entail an assessment of the comprehensiveness of regulatory efforts to ensure compliance, and then an evaluation of the degree to which they had been faithfully and meaningfully implemented.

Thus, for example, consider a court confronted with law enforcement engaging in location surveillance. Rather than undertake a substantive review that asks what number of days of GPS monitoring are permissible, a court would shift to a primarily procedural inquiry that asks whether a pre-existing policy prescribed limits on the number of days that monitoring may

263. Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy."). Justice Sotomayor also intimated that she would entertain such an exception. Id. at 955 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'") (emphasis added) (quoting id. at 964 (Alito, J., concurring in the judgment))).
take place. It would examine the processes that went into fixing and announcing such a standard, giving greatest credit for public, democratically accountable decisionmaking. Similarly, courts would consider whether a policy contains structural and individual incentives toward compliance, provides corrective mechanisms in the event of violation, and devises sufficient gauges of efficacy and abuse prevention.

No single solution is required; instead a variety of approaches might be constitutional. One statute might provide for periodic audits; another might focus on strict recordkeeping and public disclosure; another might set up post hoc grievance processes. The court’s role would be to ensure the basic effectiveness of the approach, not to impose one version of constitutionality over another. Accordingly, bald assertions of 100-percent success or compliance rates would fail to pass constitutional muster, but demonstration of a functioning system to record, revise, and improve errors would pass constitutional muster. Indeed, it would even allow a regime to be upheld as constitutional notwithstanding failure in a specific case. Naturally, if review of the metrics of a particular method were to indicate that the policy had become abusive, it could on those terms be declared unconstitutional.

However imprecise a procedural approach to cabining police discretion may be, its advantages remain manifold. First, this approach may empower courts to be less parsimonious in their recognition of constitutional interests, because the consequences of such recognition are less severe. At present, acknowledging a Katz reasonable expectation of privacy ("REP") usually translates to imposition of a warrant-and-probable cause standard and possible suppression of evidence. As a result, courts arguably are reluctant to recognize a REP in a wide variety of cases and thereby impose such inflexible procedural standards on law enforcement investigations, particularly as regards the dynamic possibilities for investigation presented by new technologies. If so, the Fourth Amendment may fail to serve its historical role as a bulwark against state oppression simply because it is irrevocably hitched to procedural requirements that end up bulldozing the field.

Freed from conventional constitutional expectations, courts may answer the threshold question of the applicability of the Constitution with less trepidation. A REP could be identified, but rather than automatically triggering an ill-fitting warrant and probable cause requirement for a particular law enforcement activity, the response would be to evaluate existing restrictions on the investigative method or to encourage adoption of new standards.

That brings us to the second benefit of this approach, which is that it creates an incentive for legislative and executive actors to formulate investigative policies in the abstract. Such ex ante consideration is superior to the present custom of post hoc adjudication of discretionary police decisionmaking, often by applying a variable "reasonableness" analysis. It would hopefully foster legislative creativity in addressing the scope of law enforcement power, with the recognition that prospective rules will apply to any potential target. Indeed, by forcing choices upstream from the moment of investigation, rather than with the hindsight of the officer with the criminal in hand, this approach may ultimately enhance rather than diminish
individual privacy rights. Moreover, as the lessons of the preceding Part tell us, legislative solutions can offer not only structural checks that prevent unnecessary intrusion but also incentives to correct institutional flaws that arise. They can do more work in regulating the transfer and use of information, rather than just its simple acquisition. There are even reasons to think that notice-based subpoena requirements might do a better job at safeguarding individual interests—because they allow for adversarial process—than the “neutral magistrates” that issue warrants. And, to the extent that the lack of a uniform federal standard may result in confusion or unappealing jurisdictional variation,\textsuperscript{264} the counterargument may be that permitting such variation as the social, legal, and cultural significance of a new technology is slowly being established will provide the ultimate “laboratories for experimentation” that federal constitutional pronouncements have long been criticized as stifling.

Third, this approach would allow for constraints on police activity better suited to the realities of modern existence. As Justice Alito acknowledged in his concurrence in \textit{Jones}, “In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.”\textsuperscript{265} Resource constraints operated silently in the background of every contested case—simply by engaging in an investigative activity, law enforcement at some level was expressing a belief in its utility and ranking its priority relative to other possible courses of action. But such calculations are absent from the digital field; it is only through explicit articulation of the scope of permissible law enforcement activity that priorities and commitments are likely to be expressed (much less followed).

To be sure, abandoning the tripod of warrants, probable cause, and exclusion that has long served as the foundation for the Fourth Amendment carries with it many risks. There is a legitimate concern that legislative or executive actors would simply craft vague, self-dealing policies. Alternatively, policies may be clear but may also lead to standards far below what has long been considered the barest constitutional threshold—say, by allowing ex parte, unilateral “domestic security letters” compelling the disclosure of sensitive information. Some may also argue that a deferential procedural approach is likely to leave certain populations underprotected, particularly since the population at large has shown little solicitude for criminal justice targets in the past decades (consider punitive enactments such as three-strikes laws, mandatory minimums, and so on).

These concerns are valid, but I would respond that, as the previous Part lamentably acknowledges, such underprotection is arguably already a hallmark of criminal procedure jurisprudence. In this respect, simply

\textsuperscript{264} Precisely the complaint, it should be noted, that Justice Alito’s concurrence made of Justice Scalia’s plurality determination to use state-based common law to define the scope of constitutional protection in \textit{Jones}. 132 S. Ct. at 961–62 (Alito, J., concurring in the judgment).

\textsuperscript{265} \textit{Id.} at 963; \textit{accord id.} at 956 (Sotomayor, J., concurring) (noting that the cheapness and surreptitiousness of GPS monitoring allows it to “evade[] the ordinary checks that constrain abusive law enforcement practices: ‘limited police resources and community hostility.’” (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004))).
demanding, as a constitutional matter, a public legislative and administrative framework for intrusive policing methods of this kind may nonetheless mark an advance over the current approach. Moreover, while such scenarios are a risk, two realities offset my concerns. First, although imperfect, the democratic processes that have propelled enactment of statutory protections across the range of areas that are currently unregulated by the Constitution suggest that, for whatever reason, some momentum in favor of privacy exists among the polity. Thus, wholesale elimination of all safeguards seems unlikely. Privacy from technological intrusions may also resonate more broadly across the electorate, who may worry about their cell phones or internet searches, as opposed to privacy pertaining to topics applicable primarily to specific socioeconomic groups (like privacy in welfare benefits).

Second, in advocating for an approach to constitutional adjudication that is heavily procedural, I do not mean to suggest that the courts would forfeit all power to invalidate any particular police action. In addition to holding unconstitutional wholly uncabined discretion, courts could still exercise substantive review power in extreme cases. Giving courts the authority to invalidate an act runs the risk of frustrating congressional attempts to define the scope of protection, turning judicial review into a game of “guess what I’m thinking.” Thus, I intend for invalidation to occur only in the extreme cases, but it will still be available as a last resort.

Admittedly, articulating the precise scope of this “last resort” core of constitutional protection is inherently difficult, but it is not impossible. For instance, invalidation would be appropriate if the regulatory protections were so threadbare as to render the right essentially meaningless. Thus, a “domestic security letter” standard, with no other procedural safeguards (such as notice or use restrictions) and minimal incentives for structural compliance or corrective reforms, might simply be deemed to offend the baseline “reasonableness” standard to obtain highly sensitive material, such as mental health records. At the same time, that low procedural threshold might be supported if other strong safeguards were in place to prevent and compensate for abuse, or if the information were deemed less intimate (say, car rental history). Conversely, a right may be so inviolable that even elaborate safeguards could not overcome it. In other words, the courts might still hold it unconstitutional to order an individual to undergo a “mind-reading” MRI, no matter how many procedural hoops law enforcement officers were required to jump through.

In sum, allowing courts to invoke the Fourth Amendment as a way of forcing the legislative agenda—thereby compensating for political process flaws that might otherwise permit Congress to leave such areas unattended—while not tying legislative hands with constitutional thread might in the long run offer a better balance between absolute-rights protectiveness and unnecessarily rigid constitutionalism. This process-oriented approach would use judicial review to sharpen legislative processes and improve policing outcomes, while also maintaining the essential rights-defining and values-protecting role of the courts.
CONCLUSION

Whatever one's view of this proposal, one thing is clear. The nature of privacy is changing in our society, as are the legal frameworks that govern it. Criminal justice investigations are no longer largely governed by the Fourth Amendment; instead, an array of generally applicable privacy statutes control access to many of the most important kinds of information available about an individual. The time has come to pay greater attention to these statutes—and in particular to their law enforcement exemptions—and to consider the ways in which privacy will and ought to be regulated in the future.
## APPENDIX

### MAJOR PRIVACY STATUTES

<table>
<thead>
<tr>
<th>Act</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSA</td>
<td>Bank Secrecy Act, 12 U.S.C. § 1951</td>
</tr>
<tr>
<td>CALEA</td>
<td>Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001</td>
</tr>
<tr>
<td>CCPA</td>
<td>Cable Communications Policy Act, 47 U.S.C. § 551</td>
</tr>
<tr>
<td>CDA</td>
<td>Communications Decency Act, 47 U.S.C. § 230</td>
</tr>
<tr>
<td>CFAA</td>
<td>Computer Fraud and Abuse Act, 18 U.S.C. § 1030</td>
</tr>
<tr>
<td>CMPPA</td>
<td>Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a(o)</td>
</tr>
<tr>
<td>COPPA</td>
<td>Children’s Online Privacy Protection Act, 15 U.S.C. § 6502</td>
</tr>
<tr>
<td>DNA</td>
<td>DNA Identification Act, 42 U.S.C. § 14131</td>
</tr>
<tr>
<td>DPPA</td>
<td>Driver’s Privacy Protection Act, 18 U.S.C. § 2721</td>
</tr>
<tr>
<td>E-Gov</td>
<td>E-Government Act, 44 U.S.C. § 3541</td>
</tr>
<tr>
<td>ECPA/Title III or Wiretap Act/ Pen Register Act</td>
<td>Electronic Communications Privacy Act, 18 U.S.C. § 2510</td>
</tr>
<tr>
<td>FCRA</td>
<td>Fair Credit Reporting Act, 15 U.S.C. § 1681</td>
</tr>
<tr>
<td>GINA</td>
<td>Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act, 29 U.S.C. § 1181</td>
</tr>
<tr>
<td>NCPPA</td>
<td>National Crime Prevention and Privacy Act, 42 U.S.C. § 14616</td>
</tr>
<tr>
<td>Privacy Act</td>
<td>Privacy Act, 5 U.S.C. § 552a</td>
</tr>
<tr>
<td>RFPA</td>
<td>Right to Financial Privacy Act, 12 U.S.C. § 3408</td>
</tr>
<tr>
<td>SCA</td>
<td>Stored Communications Act, 18 U.S.C. § 2703</td>
</tr>
<tr>
<td>TBA</td>
<td>Taxpayer Browsing Act, § 26 U.S.C. 7213A</td>
</tr>
<tr>
<td>TRPPA</td>
<td>Telephone Records and Privacy Protection Act, 18 U.S.C. § 1039</td>
</tr>
<tr>
<td>VPPA</td>
<td>Video Privacy Protection Act, 18 U.S.C. § 2710</td>
</tr>
<tr>
<td>VVPA</td>
<td>Video Voyeurism Prevention Act, 18 U.S.C. § 1801</td>
</tr>
<tr>
<td>WCPSA</td>
<td>Wireless Communications and Public Safety Act, 47 U.S.C. § 615</td>
</tr>
</tbody>
</table>