Electronic Surveillance Law and the Intra-Agency Separation of Powers

By Paul Ohm*

Introduction

THE QUESTION FOR REFORM of our statutory electronic surveillance laws is no longer "if" but "when." By declaring a significant part of the Electronic Communications Privacy Act ("ECPA") unconstitutional in *United States v. Warshak*,[1] the U.S. Court of Appeals for the Sixth Circuit gave Congress the push it needs to fix an outdated statute. In *Warshak*, the Sixth Circuit held that the FBI may not obtain copies of the content of email messages stored with email providers without a warrant, invalidating an important part of ECPA.[2] Yet, outside of the Sixth Circuit's jurisdiction, the police may continue to request email from providers with less than a warrant. As a result, the constitutional questions faced in *Warshak* will likely bubble up in other courts. I predict most courts of appeals will follow the lead and borrow from the sound reasoning of the Sixth Circuit by declaring the same provisions of ECPA unconstitutional.[3]

Eventually, Congress will act. That a provision of a federal statute authorizes an unconstitutional process is a bit of an embarrassment. That the provision represents a critical part of the principal statutory scheme regulating online search and seizure is much worse. What ECPA allows the police to do without a warrant calls into question core values like free speech and association; freedom to think, read, and communicate; and other values like innovation, economic

* Associate Professor, University of Colorado Law School. Thanks to the editors of the University of San Francisco Law Review and Professor Susan Freiwald for inviting me to take part in this symposium. Many of the anecdotal observations in this piece are based upon my personal observations, developed while I served as a trial attorney in the Justice Department's Computer Crime and Intellectual Property Section, from 2001 to 2005.

1. 631 F.3d 266 (2010).
2. *Id.* at 288.
3. *Id.* (holding that an email subscriber possesses a Fourth Amendment reasonable expectation of privacy in email stored with a provider by analogy to telephone calls and sealed letters and distinguishing records falling within the third party exception).

growth, and the moral standing to shame foreign governments that want to crack down on their citizens' use of the Internet. Congress should embrace ECPA reform, and it should act soon. Two promising beginnings are reforms that have been proposed by a coalition calling itself Digital Due Process ("DDP")[4] and several pieces of draft legislation proposed by Senator Leahy.[5]

Even if Congress enacts these reforms, they alone would not be enough to strike the proper balance between law enforcement need and online privacy. ECPA will still present ambiguities, particularly when it applies to emerging technologies. Many of these ambiguities will be hashed out internally within the Justice Department long before they ever come to the attention of judges, advocates, and academics on the outside. ECPA reform is necessary for protecting privacy online, but it is not nearly sufficient.

This essay undertakes a novel institutional analysis of electronic surveillance. Institutional analyses in criminal procedure scholarship are somewhat rare and often they amount to a macro-level weighing of relative institutional competencies.[6] This essay is premised on the idea that we might find new solutions to vexing old problems—in this case, protecting individual and group privacy from undue invasion by government electronic surveillance—by taking detailed account of the internal structures of the machinery of law enforcement.

Specifically, this essay builds on a proposal by Neal Katyal, who argued for the use of internal—in other words, within one branch of government—separations of power.[7] Katyal recommended separating power between different, co-equal executive branch departments—the State and Defense Departments—on matters of national security.[8] This kind of *inter-agency* approach will not work in the realm of elec-

4. *See generally About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org (last visited Jan. 15, 2013) (calling for amendments to ECPA requiring search warrants for access to stored content or location, stepped up judicial review for pen registers, and limits on non-particularized, dragnet surveillance).

5. *See generally* H.R. 2471, 112th Cong. tit. II (2012) (as reported by S. Comm. on the Judiciary, Nov. 29, 2012) (requiring search warrants for stored contents); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (requiring search warrants for stored contents and location).

6. *See, e.g.*, Patricia Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 332 (2011) (suggesting that "institutional competence tend[s] to oversimplify the surveillance law landscape").

7. Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006).

8. *Id.* at 2325–27.

tronic surveillance given the need for criminal law enforcement to have sole and entire control over their criminal investigations.

Instead, this essay proposes introducing *intra-agency* separations of powers that pit part of the Justice Department against itself, creating competition for interpretations of statutory and constitutional surveillance law. Specifically, the Criminal Division of the Justice Department already allocates responsibility for electronic surveillance in two distinct sections: the Office of Enforcement Operations ("OEO") and the Computer Crime and Intellectual Property Section ("CCIPS"). Yet, it seems the two sections tend to divide responsibility for different questions of electronic surveillance and rarely embrace overlapping authority. By encouraging additional joint deliberation between these two sections, this essay proposes a novel way to improve the richness of the debate over electronic surveillance; notice and participation of higher-ranking Justice Department officials; and the possibility for helpful second opinions. The hope is that these changes will more often lead to better results.

This essay proceeds in two parts. Part I argues that current proposals for the reform of electronic surveillance law focus solely on inter-branch solutions, which cannot by themselves assure privacy in the face of technological change. Part II performs a micro-scale institutional description of the Criminal Division of the Justice Department—revealing that OEO and CCIPS have been given similar, but non-overlapping, authority over electronic surveillance law—and argues for reform to bring these two sections into more frequent debate and discussion.

I. The Need to Supplement the Inter-Branch Review of Electronic Surveillance

The inter-branch check—by way of requiring a judge's permission before conducting electronic surveillance—is not enough by itself to protect privacy from overreaching or abusive police practices. Today's rules impose significant limits on the amount of information judges receive and the amount of discretion judges wield. Even if we were to reform electronic surveillance law to significantly increase the power of judges, we would still face intrinsic limits that should encourage us to seek extra-judicial forms of protection.

A. The Limits of Today's Judicial Review

Today's electronic surveillance laws, both constitutional and statutory, do not give judges enough power to access the facts underlying police requests for permission to conduct surveillance nor enough discretion to refuse those requests. Under some statutes, the judicial role is merely ceremonial. Even worse, these limits on judicial review are not distributed uniformly across contexts. Judges seem to have the least amount of power in the types of cases we worry about the most: those involving invasive new forms of technology.

Today's laws leave many forms of electronic surveillance unregulated, assigning no role whatsoever to the judicial branch. Courts have interpreted the word "search" in the Fourth Amendment to set forth a binary distinction: some acts of electronic surveillance are regulated by the Fourth Amendment, and others are not.[9] Unless a statute indicates otherwise, the police are free to conduct surveillance in the latter category without ever consulting a judge. Thus, the Court in *Smith v. Maryland*[10] held that pen registers, which record the numbers dialed on a particular telephone line, are not searches within the meaning of the Fourth Amendment, thereby permitting the police to conduct a pen register without a warrant.[11] Citing *Smith*, lower courts have found other acts of electronic surveillance not to be searches within the meaning of the Fourth Amendment, such as non-content monitoring of Internet traffic[12] and access to basic subscriber information stored by an Internet service provider.[13]

When Congress enacted ECPA, it diverged from the simple binary model of the Constitution by creating intermediate levels of inter-branch protection and requiring the police to seek court orders in particular situations that otherwise would not have required the inter-branch check.[14] Despite these attempts to increase judicial involvement above the Fourth Amendment floor, ECPA still allows a fair amount of electronic surveillance by the police without an inter-branch check. Using only a subpoena, for example, the police can obtain some forms of content stored with providers, as well as basic subscriber information, such as name, address, and billing informa-

9. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967) (holding that government's electronic surveillance and recording of petitioner's words while using a telephone booth constituted a search within the meaning of the Fourth Amendment).

10. 442 U.S. 735 (1979).

11. *Id.* at 739–46.

12. United States v. Forrester, 512 F.3d 500, 509, 513 (9th Cir. 2008).

13. United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999).

14. 18 U.S.C. § 2703(b) (2006).

tion.[15] Even more significantly, ECPA protects the privacy of the content of stored records for only two categories of providers, "electronic communications services" and "remote computing services."[16] Neither category likely covers many types of online providers, such as e-commerce sites and web publishers, giving the police the freedom to obtain sensitive records with no judicial check.[17]

Even when electronic surveillance law grants judges a role in approving electronic surveillance, it too often fails to give them the tools they need to administer meaningful oversight. The best example is the Pen Register and Trap and Trace Devices Act.[18] This law—which governs real-time surveillance of non-content information, such as telephone numbers dialed, websites visited, and email to/from information—grants judges an exceedingly limited role. Judges "shall" grant the government an order to conduct the surveillance "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[19] This language does not appear to require the police to divulge any facts about its investigation, and at least one court has called the judge's role merely "ministerial."[20] Although this is the most glaring example of how judicial review alone is an insufficient safeguard for privacy, there are other, less egregious examples.[21]

These limits of judicial supervision in today's electronic surveillance law are not evenly distributed. Instead, judges probably participate least in some of the most worrisome cases: those involving cutting-edge technology. Think of the practice and law of electronic surveillance as falling into three rough categories. The first category can be characterized as "Settled." This category includes practices that are long-established, well-known, and fully litigated. The police (and the public) know precisely where such practices fit within the constitu-

15. *Id.* § 2703(c)(2).

16. *Id.* §§ 2510, 2711.

17. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1230–31 (2004) (arguing that eBay is not covered by the Stored Communications Act ("SCA")).

18. *See generally* 18 U.S.C. §§ 3121–27 (2006).

19. *Id.* § 3123(a).

20. *See* United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

21. Consider, for example, ECPA's "d-order" standard, which gives access to various kinds of content and non-content information stored with a provider. 18 U.S.C § 2703(d) (2006). Some have criticized the standard as providing too low a hurdle for access to such private information. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 175–76 (2007).

tional and statutory laws of electronic surveillance, and fights over these techniques are now rare. Some examples include: pen registers and trap-and-trace devices for telephone numbers or email headers, which fall within the Pen Register and Trap and Trace Devices Act ("Pen Register Act");[22] requests to providers for basic subscriber information associated with an account username or other identifier;[23] and surveillance using silent video.[24]

To be clear, some continue to be dissatisfied with the rules governing the Settled category. Many grumble about the low standards allowed under the Pen Register Act, for example.[25] But they complain in these cases about the quality of the privacy protection, not about the meaning of the Act, and they direct these complaints toward the legislature, not the courts.

The second category we might call the "Leading Edge." This includes practices that have been in use for some time yet continue to sit under clouds created by ambiguities in the laws and have yet to be resolved in litigation. Two of the highest profile battles in recent years have involved Leading Edge fights over cell-site location[26] and the use of court orders to obtain the content of email messages.[27] These courtroom battles exemplify where the inter-branch function operates best. Calls to reform electronic surveillance law focus mostly on Leading Edge fights, and indeed, current reform calls focus much of their attention on location and email.[28]

Finally, the "Bleeding Edge" category refers to relatively new practices, often involving emerging technologies. Not only have Bleeding Edge practices failed to receive a careful vetting in court, but they are also often completely unknown outside law enforcement. The police experiment with new technologies long before they ever deploy them widely, and they can use them without revealing that fact to the public for years. In fact, even once the public discovers the police's use of a possible new technique, it will not be until the police actually use it to

22. *See* 18 U.S.C. §§ 3121–27 (2006).

23. *See id.* § 2703(c)(2).

24. *See* United States v. Torres, 751 F.2d 875, 882–83 (7th Cir. 1984).

25. *See, e.g.*, *Our Principles*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Jan. 15, 2013) [hereinafter *Our Principles*] (principle number three urges at least a "d order" standard for pen register and trap and trace orders).

26. *See, e.g.*, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

27. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

28. *See, e.g.*, *Our Principles*, *supra* note 26.

gather evidence and bring charges against a criminal defendant that the courts will have an opportunity to conduct judicial review.

We have seen this pattern play out repeatedly. There were rumors that the FBI had been using home-grown spyware techniques to search pseudonymous email accounts for years before one case was confirmed.[29] A similar pattern of rumor without official confirmation (much less opportunity for judicial review) has accompanied the police uses of key logging techniques,[30] drones,[31] cell-site simulators (such as "stingray"),[32] honeypots,[33] the repurposing of cell phones,[34] and in-car navigation devices[35] as hidden microphones. In fact, none of these relatively vintage technologies has been brought before judicial review any more than a handful of times, and some have never been reviewed.

The problem may in fact be becoming much worse with the rise of new technologies that attack "public facts."[36] For example, the police may be collecting DNA from public places[37]—lifting a target's discarded coffee cup, for example—and using facial recognition technologies to identify people on surveillance video.[38] Last term, the Supreme Court began to struggle with these issues in *United States v. Jones*,[39] the "GPS Beeper" case. Although the Court found the use of the GPS tracking device in that case to be a Fourth Amendment search, the majority reasoned on relatively narrow grounds,[40] and only in the concurrences did the Justices advance theories that might ex-

29. *See* Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 18, 2007), http://www.wired.com/politics/law/news/2007/07/fbi_spyware.

30. *See* United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

31. Peter Finn, *Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate*, WASH. POST (Jan. 23, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

32. *See* Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html.

33. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415, 471–72 (2012).

34. Declan McCullagh & Anne Broache, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET NEWS (Dec. 1, 2006), http://news.cnet.com/2100-1029_3-6140191.html.

35. *See In re* Order Authorizing Roving Interception of Oral Commc'ns, 349 F.3d 1132 (9th Cir. 2003).

36. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

37. *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 862–74 (2006).

38. Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. (forthcoming 2013).

39. 132 S. Ct. 945 (2012).

40. *Id.* at 949–53.

tend beyond relatively narrow contexts.[41] It may be years or longer before the courts provide definitive guidance. Judicial review of techniques that act on public facts is even less likely to occur sooner than other Bleeding Edge techniques, such as spyware or key loggers. This is because no statute purports to regulate these facts, and the police (and the prosecutors who advise them) are probably not yet altering their behavior significantly in anticipation of a possible sea change in Fourth Amendment law. It is thus very likely that the police will embrace public facts surveillance long before the judiciary subjects them to any scrutiny.

We tell hopeful stories about the power of the judiciary to check police surveillance abuses. These stories neglect the deeply embedded structural tendencies that shield so many worrisome Bleeding Edge techniques from review.

B. Why Legal Reform Offers No Panacea

If today's laws fall short of giving judges meaningful oversight over electronic surveillance, isn't the answer to expand the judicial role? Reforming ECPA to give judges more power over electronic surveillance is imperative. ECPA is riddled with too many holes in coverage that leave unregulated access to some of the most sensitive online services. The Pen Register Act provides no effective judicial review. Courts should reassess the way they construe the Fourth Amendment to take better account for the way new technology invades privacy. Although legal reform is *one* answer, it is not *the only* answer. There are several limits to relying on legal reform to increase the power of judges in this space.

The first limit is temporal: any reform of ECPA or the Fourth Amendment will take time. Even though the DDP movement has brought new energy to calls to amend ECPA, and even though the first bill embracing some of the DDP principles has been voted out of committee, full passage seems unlikely any time soon.[42] It may take years before we see meaningful and comprehensive ECPA reform. In the meantime, we need to supplement the weak forms of inter-branch review under the current law.

Second, any form of ECPA reform will be necessarily incomplete, leaving significant forms of electronic surveillance outside any judicial

41. *Id.* at 954–57 (Sotomayor, J., concurring); *id.* at 962–63 (Alito, J., concurring).

42. David Kravets, *Senate Committee Approves Bill Requiring Warrants for E-Mail*, WIRED THREAT LEVEL (Nov. 29, 2012), http://www.wired.com/threatlevel/2012/11/ecpa-reform-approved/.

check. Advocates of the DDP reform movement, for example, have proposed four reforms to ECPA: a warrant requirement for police access to content stored with any Internet provider; a warrant requirement for access to mobile phone location information; more searching judicial review of requests for pen register orders; and the end of dragnet surveillance of records with a mere subpoena.[43] To be sure, these proposals would significantly increase the judicial role over electronic surveillance, especially the first proposal. Yet even if these reforms were fully enacted, they would still allow significant freedom of police surveillance without judicial involvement. DDP has not called, for example, for reform of the rules for government access to "basic subscriber information," which can be obtained with a subpoena.[44] Nor has DDP advocated extending ECPA to cover additional types of providers, even though the statute arguably does not cover e-commerce sites, news sites, web advertisers, and other potential sources for leads in investigations.[45] ECPA reform is unlikely to embrace all four of DDP's requests. It is far more likely that legislators will seek a compromise—one that responds to the concerns that law enforcement officials have expressed.[46]

More fundamentally, ECPA currently allows a vast amount of surveillance without judicial review through the many exceptions that the law provides. Providers can voluntarily provide customer records to the police, for example, if they reasonably believe there is an emergency situation.[47] They can also hand over customer records with the

43. *Our Principles*, *supra* note 26.

44. 18 U.S.C. § 2703(c)(2) (2006).

45. *See* Kerr, *supra* note 17, at 1230–31. Kerr's reasoning would possibly extend to other providers that neither "provide[ ] users . . . the ability to send or receive" communications under 18 U.S.C. § 2510(15), nor provide "computer storage or processing services" under § 2711(2). 18 U.S.C. § 2510(15) (2006) (defining "electronic communications service"); *id.* § 2711(2) (defining "remote computing service"); *see also* Kerr, *supra* note 17, at 1230 ("The legislative history indicates that 'processing services' refer to outsourcing functions.").

46. For example, in September 2012, Senator Leahy introduced a bill that would implement only the first of the four DDP principles, search warrants for content. *See* Declan McCullagh, *Senators Prepare to Vote on Netflix and E-mail Privacy*, CNET NEWS (Sept. 20, 2012), http://news.cnet.com/8301-13578_3-57516501-38/senators-prepare-to-vote-on-netflix-and-e-mail-privacy/. In another sign that ECPA reform cannot happen without political compromise, the proposal attaches the fix to a separate measure that weakens privacy protection in the Video Privacy Protection Act. *See* Mark M. Jaycox & Lee Tien, *ECPA Reform May Require Warrants for Email, But Hurts Video Privacy*, ELECTRONIC FRONTIER FOUND. DEEPLINKS BLOG (Sept. 19, 2012), https://www.eff.org/deeplinks/2012/09/ecpa-reform-may-require-warrants-email-hurt-video-privacy.

47. 18 U.S.C. § 2702(b)(8), (c)(4) (2006).

consent of their customers,[48] and many terms of service are so sweeping as to arguably constitute that consent.[49]

Similarly, those who have argued for an expanded judicial role over electronic surveillance under the Fourth Amendment nevertheless preserve freedom for some extra-judicial police action. Dan Solove, for example, has argued that the courts should abandon the "reasonable expectation of privacy" test for determining when a search has occurred within the meaning of the Fourth Amendment.[50] In its place, Professor Solove would apply constitutionally mandated procedures any time police "information gathering . . . causes problems of reasonable significance."[51] However, this test already appears to exclude some forms of information gathering, although Professor Solove intends for it to pose a very low hurdle.[52] Moreover, activities covered by Professor Solove's test need not always require judicial review and a warrant, as Professor Solove is open to other, lower forms of procedural processes.[53] To similar effect, Chris Slobogin has long championed a "proportionality principle" for the Fourth Amendment, according to which the justification required for a search or seizure will vary proportionately with the invasiveness of the action.[54] But Professor Slobogin's examples demonstrate that proportionality also allows some police action without a judicial check.[55]

Third, although we should increase the role of the judiciary over electronic surveillance, there should be limits to how much we require the courts to be involved, lest we interfere too much with the efficiency of the police. Electronic surveillance law must balance the need to detect and prevent crime against the privacy of the people.[56] Striking this balance right should mean letting a nimble police force respond quickly to imminent threats and crimes without having to clear unnecessary hurdles. Specifically, police work happens iteratively. A

48. *Id.* § 2702(b)(3), (c)(2).

49. *Cf.* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no Fourth Amendment reasonable expectation of privacy in work computer because of agreement to privacy policy allowing monitoring of Internet use).

50. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1528 (2010).

51. *Id.*

52. *See id.* at 1529 ("Under this approach, the Fourth Amendment would likely apply to a very broad range of government information gathering activities.").

53. *Id.* at 1529–30 (showing a willingness to consider the practical consequences of a particular enforcement mechanism for Fourth Amendment violations rather than imposing a "one-size-fits-all rule requiring a warrant supported by probable cause").

54. SLOBOGIN, *supra* note 22, at 21–47.

55. *Id.*

56. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 481–82 (2011).

police investigation—either in the real world or online—often begins with speculative leads and great uncertainty.[57] Police officers rely on training, intuition, and even an occasional hunch to develop more certainty. There is no categorical reason to deny the police access to all electronic information during the earliest stages of their investigations. Some forms of electronic police work seem to pose so slight a threat to privacy that they should be allowed without a judicial check. The only question is where we draw the line.

For example, a sound balance in ECPA should permit the police the freedom to use public domain resources such as web search engines, publicly available databases, and websites without the need for judicial approval.[58] The police need not ask a judge for permission to use Google, the WHOIS database, or Wikipedia. Also, ECPA reform should further the ability of the police to issue a grand jury subpoena directly to the target of the investigation requesting copies of content, for example, requests to obtain copies of email from the account owner not the provider.[59]

But if we agree to leave some police behavior outside the inter-branch check of judicial review, we should find other ways to monitor this behavior for abuses. The next section explores a novel possibility: expanded use of intra-agency review. But it is important to reiterate that any new extra-judicial checks we identify can work in conjunction with judicial review. This is not an either-or choice.

II. The Department of Justice and the Internal Separation of Powers

A. Substituting a Judicial Check with an Internal Separation of Powers

If practical or prudential reasons prevent us from imposing judicial scrutiny in some cases, we should ask, what is it about a judge's scrutiny that disciplines police behavior? Once we enumerate these qualities, we might find them in other places. First, a judge must have enough information to understand the facts of the investigation. Second, a judge's interests must not align perfectly with the interests of

57. Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1527 (2010).

58. 18 U.S.C. § 2511(2)(g)(i) (2006) (allowing exception to ECPA in cases involving communications that are "readily accessible to the general public").

59. Kerr, *supra* note 17, at 1211–12. The recipient of the subpoena is of course able to ask a judge to quash the subpoena. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005) (discussing motions to quash subpoenas).

the investigators. Finally, a reviewing judge must be granted the discretion to either refuse the request or at least slow things down in order to obtain more information. Although judges may be well positioned to satisfy these requirements, they do not alone possess a monopoly on these qualities. Indeed, we can find parties possessing the same three qualities we find in judges—access to information, nonaligned interests, and discretion—within the executive branch. In fact, we can find it within the Justice Department itself.

This argument builds on the work of Neal Katyal, law professor and former Acting Solicitor General.[60] Professor Katyal, writing about national security law after 9/11, spotlighted the little noticed checking function that occurs within the executive branch.[61] In an uncommon twist, he celebrated bureaucracy.[62]

Professor Katyal focuses specifically on inter-agency checking, advocating for rules that assign more than one agency oversight over national security decisions and the power and incentive to check one another.[63] For example, he celebrates the fact that the State Department and the Defense Department often find themselves needing to convince the White House of the relative virtues of proposals having to do with terrorism.[64] Rather than a redundant inefficiency deserving to be driven out, Katyal recommends ways to bolster the bureaucratic overlap.[65]

But national security law and policy during the war on terror differ significantly from the day-to-day grind of discrete criminal investigations in which most electronic surveillance questions arise. The kind of national security decisions on which Katyal focuses include large, complex, and inherently international geopolitical puzzles. It makes sense that the State Department and Defense Department—not to mention the Justice Department and intelligence community—all play a part in the deliberations around such questions. In contrast, any given criminal investigation tends to be the province of one agency—usually the Justice Department but sometimes the Department of Homeland Security. International cooperation is still too rare to involve the State Department very often, and the USA PATRIOT

60. Katyal, *supra* note 8.

61. *Id.* at 2316.

62. *Id.* at 2317.

63. *Id.* at 2319–20.

64. *Id.* at 2327.

65. *Id.*

Act notwithstanding, there remain walls between most criminal cases and national security investigations.

If we want to harness the benefits of bureaucratic overlap, we need to do it within the organization chart of a single agency. As we will see in one case study, modern executive branch agencies like the Justice Department are so large and multifarious that we can replicate Katyal's benefits of bureaucracy within a single agency.

B. Electronic Surveillance and the Criminal Division[66]

In order to craft opportunities for bureaucratic overlap and checking within the Justice Department itself, we need to engage in a rather unglamorous excavation of the internal structure of the agency. This is a very specific inquiry, one that is difficult to generalize to other agencies, and indeed, one that may accurately depict the truth during only a limited snapshot in time. As the Justice Department evolves into new forms, we may need to revise the following description.

The Criminal Division of the Justice Department consists of fourteen non-administrative offices and sections.[67] Almost every section is assigned a single (sometimes broad) substantive or procedural focus. Substantively focused sections bear responsibility for the investigation and prosecution of a particular type of criminal or crime. Examples include the Organized Crime and Gang Section, the Fraud Section, and the Narcotic and Dangerous Drug Section. Procedurally focused sections help the substantively focused sections and the U.S. Attorney offices in the field navigate a particular phase of a criminal case or type of procedural hurdle. Examples include the Appellate Section, Office of International Affairs, and Office of Policy and Legislation.

One section that departs significantly from this model, as a master of both substance and procedure, is the Computer Crime and Intellectual Property Section ("CCIPS").[68] Much of CCIPS's focus is

66. Some of the facts described in this subpart are known to me from the experience I gleaned while a staff attorney for the Justice Department but are difficult to find independently documented. I have tried to find documentary support for the most important facts underpinning my argument. Errors involving uncited facts are my responsibility alone.

67. *Criminal Division: Organizations*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/about/orgchart.html (last visited Dec. 10, 2012).

68. CCIPS is not the only section with a dual mission. Another notable example is the Asset Forfeiture and Money Laundering Section, which focuses on both procedures for seizing assets in any case (criminal or civil) as well as the substantive federal criminal law of money laundering. *See Asset Forfeiture and Money Laundering Section*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/afmls/ (last visited Nov. 4, 2012).

substantive: it oversees the nation's computer hacking and criminal intellectual property laws.[69] But a pocket of CCIPS attorneys focuses on the procedural question of access to information stored on computers and computer networks. This unit was unofficially, and affectionately, called the "ECPA Team" when I was a member. It serves as a national clearinghouse for field agents and prosecutors for advice on the constitutional and statutory laws governing law enforcement access to the content of email accounts, web traffic logs, standalone computers, cell phones, and more.[70]

That CCIPS has taken on such an important role can probably be attributed to the influence and stature of its founder and the fact that most lawyers know little about technology. The single, most important force behind the creation of CCIPS was Scott Charney, now Microsoft's Vice President for Trustworthy Computing. Mr. Charney created CCIPS in 1996.[71] It was likely his influence and vision at the time that led the Justice Department's front office to entrust CCIPS with a broad mandate to advise the field on matters of both procedure and substance. Charney's successors and the scores of line attorneys who have been through CCIPS have proved to be good stewards of this responsibility.

Expansions of authority within an organization as vast as the Criminal Division often set off a zero-sum challenge to the authority of another unit. CCIPS's focus on electronic surveillance overlapped in important ways with the mission of another unit: the OEO. OEO "oversees the use of the most sophisticated investigative tools at the Department's disposal."[72] This crisp mission statement belies the odd mix of authorities within OEO's purview, including entry into the witness protection program, subpoenas directed at attorneys and the press, and even gambling device registration.[73] OEO is perhaps best known in federal criminal law enforcement as an important bureaucratic check placed before those who would administer a lawful wiretap.[74] According to federal law, all applications to the court for orders

69. *Computer Crime and Intellectual Property Section*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/cybercrime/ (last visited Dec. 10, 2012).

70. *Id.*

71. David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 CONN. L. REV. 1, 6 (1998).

72. *Office of Enforcement Operations*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/oeo/ (last visited Jan. 8, 2013).

73. *See id.*

74. Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971, 983–84 (2003).

for a wiretap must first be approved by a specified political appointee of the Justice Department.[75] In most routine cases, Justice Department rules delegate this authority to OEO.[76]

The overlap between OEO and CCIPS operates on two levels. First, the Wiretap Act, a law dating to 1968, was expanded significantly in 1986 to cover wiretapping that occurs on computer networks.[77] Field agents and prosecutors hoping to wiretap a computer network probably need to seek the advice of both units—OEO because of its role in approving wiretap requests and CCIPS for technological assistance. Both units consider it their responsibility to oversee the consistent application of the Wiretap Act. The overlap of responsibility is even more apparent when one considers the relative rarity of computer wiretapping with a court order. According to the annual Wiretap Report, law enforcement officers seek orders to wiretap computer networks fewer than ten times each year.[78] Yet anecdotal experience suggests that wiretap-eligible surveillance happens more often by at least an order of magnitude. The vast majority of computer network surveillance never gets submitted to a judge and thus never falls within the Wiretap Report because it falls within an exception to the order requirement. Wiretapping a computer network without an order is permitted, for example, with the consent of a party,[79] if it is necessary to protect a provider's rights and property,[80] or if it is subject to the so-called computer trespasser exception, which allows wiretap surveillance to track an unauthorized intruder.[81]

75. 18 U.S.C. § 2516 (2006) (assigning authority for this power to "[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division" (citation omitted)).

76. U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-7.110 (1997), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm ("When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit (ESU) of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings . . . .").

77. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, 100 Stat. 1848 (1986).

78. *See, e.g.*, ADMIN. OFFICE OF THE U.S. COURTS, WIRETAP REPORT 2011 tbl. 6 (2011), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf (listing four orders nationwide for wiretaps for calendar year 2011).

79. 18 U.S.C. § 2511(2)(d) (2006).

80. *Id.* § 2511(2)(a)(i).

81. *Id.* § 2511(2)(i).

The second overlap is less formal. Keeping up with electronic surveillance requires a team of lawyers who can understand both law and technology. The clean statutory division between wiretaps and stored communications—and thus the line between OEO and CCIPS—does not make sense from a technological focus. Packets flow and stop and flow again, making the lines between surveillance statutes quite arbitrary, and doing the same to the lines between Justice Department offices.[82]

Though counterintuitive, the conflict between offices may be a feature, not a bug. We should celebrate the fact that two different, independent subunits of the Justice Department are locked in a contest for policymaking authority.

But we should not celebrate what appears to be the Justice Department's way of resolving the possible turf wars that arise from this arrangement. The Justice Department seems to prefer tamping down the conflict, treating each new question as a "jump ball" between the sections. Once the jump ball is controlled—once one section or the other asserts its authority over a particular subject and is deemed the winner by management—it seems to bear precedential force. This might be sound managerial practice, but it may not be the best approach for civil liberties or the nation.

Consider the empirical proof that the Justice Department has been doling out electronic surveillance subjects between the two offices. It is difficult for an outsider to peer inside the black box of Criminal Division work assignments. One of the only external clues we have appears in the signature block of briefs submitted in cases involving electronic surveillance. These signatures are summarized in the appearances block of published court opinions.[83] In Westlaw's ALLFEDS database, OEO appears twelve times, and CCIPS appears seven times. Because Department of Justice attorneys do not always list their home office, I conducted the search using the names of CCIPS and OEO attorneys that I know focus on electronic surveillance issues.[84]

82. *See* United States v. Councilman, 418 F.3d 67, 72–79 (1st Cir. 2005) (discussing whether "electronic communication" within the scope of ECPA is limited to communications traveling through wires or includes communications temporarily stored on a computer).

83. A potential problem with this method is that unpublished opinions and cases, which are briefed but disposed of without any opinion, do not easily reveal the attorneys who authored the brief. There is no reason to suspect that such cases would reflect a break from the identified trend.

84. The list I used was: "nathan /2 judish"; "richard /2 downing"; "josh /2 goldfoot"; "jenny /2 ellickson"; and "mark /2 eckenwiler."

Let me offer a few observations from this admittedly thin empirical base. First, in my research, OEO and CCIPS attorneys never appear together on a brief. Second, when a topic has arisen that might have reasonably fallen within either section, it has typically been assigned to only one section. From these observations, we can infer that OEO likely has authority over cell-site tracking cases,[85] while CCIPS governs email search warrant cases.[86]

Assuming this inference is correct, these choices might be defensible. The Justice Department's cell-site approach has included some relatively exotic investigative tools such as All Writs Act orders with which OEO probably has dealt more than CCIPS. Likewise, search warrants for email rely heavily on an understanding of computer network design, perhaps falling more within CCIPS's core competency. But rather than merely being the product of rational assignment based on competence, the division of labor probably represents the strong influence of path dependence. One office, for whatever reason, probably embraced a topic first or invested a lot of time and resources into it earlier, and the choice stuck. One can imagine a file stored on the shared network drive of the staff of the Assistant Attorney General for the Criminal Division that lays out the elaborate decision tree dictating who has jurisdiction over what topic.

Put to one side the happy accident that resulted in two sections with overlapping authority. I am not claiming that this was the product of superior institutional design. Rather, I am arguing that insofar as the Justice Department has attempted to eliminate the overlap, it is making a mistake. It is far better that two offices be allowed to debate, disagree, and even negotiate the terms of the federal government's approach to new forms of electronic surveillance.

C. The Benefits of Intra-Branch Debate

The many benefits of intra-branch debate outweigh its potential downsides. First, two voices are better than one. When two sections independently assess a particular issue, both agreement and disagreement can be telling—the former for lending strength in numbers to the assessment and the latter for introducing competing approaches.

85. *See, e.g.*, *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) (briefed and argued by OEO).

86. *See, e.g.*, Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (briefed by CCIPS).

Second, through accident, path dependence, or intentional design, different subcomponents of the Justice Department tend to take on varying approaches and personalities. Consider the political structure of the Department. For example, CCIPS and OEO are led by section chiefs who report to separate Deputy Assistant Attorney Generals ("DAAG"s)—a title given to both political appointees and career civil servants. The DAAGs who oversee CCIPS and OEO each oversee other sections.[87] The CCIPS DAAG also oversees the Human Rights and Special Prosecutions Section and the Organized Crime and Gang Section.[88] Because organized crime tends to be the focus of many incoming Attorney Generals (and the Presidents who appoint them), it seems likely that this DAAG will often know more about gangs than electronic surveillance. Moreover, those who are qualified to lead the Justice Department's organized crime agenda are likely former organized crime prosecutors themselves, possibly even something approaching the caricature of the hard-nosed, aggressive prosecutor type commonly depicted in movies and television. In contrast, the OEO DAAG oversees the Public Integrity Section ("PIN").[89] PIN, a highly specialized section, oversees investigations of elected and appointed public officials suspected of criminal corruption.[90] Traditionally, the OEO DAAG has been a career civil servant, a job that stays with one person for a long time, rather than shifts with every new Attorney General.[91] Thus, one can imagine that the person longing to stand above OEO and PIN must be a careful public servant who is content with chasing corrupt politicians and judges rather than gang leaders.

This seems like a significant distinction. The DAAGs overseeing CCIPS and OEO differ in almost every relevant way. The CCIPS DAAG is politically appointed, whereas the OEO DAAG is a career appointee, presumably unbeholden to the politics of a particular party. CCIPS DAAGs tend to turn over frequently and routinely when a new Attorney General takes office, whereas OEO DAAGs are known

87. *Criminal Division Organizations*, U.S. DEP'T OF JUSTICE (Oct. 4, 2010), http://www.justice.gov/criminal/about/orgchart.html.

88. *Id.*

89. *Id.*

90. *Public Integrity Section*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/pin/ (last visited Oct. 26, 2012).

91. During my time at the Justice Department, the DAAG overseeing OEO was Jack Keeney, who had held the post for many years and, indeed, served for an incredibly long time in the Justice Department. *See* Jerry Markon, *Leaving Justice After 59 Years*, WASH. POST, Sept. 28, 2010, at B03.

for their long tenures in office. While CCIPS DAAGs focus on organized crime and gangs, OEO DAAGs instead focus on rooting out public corruption. At the risk of reading too much into this distinction, one can imagine how these two different areas of focus inculcate different ideas about values and public service. Professor Katyal makes a similar point about the differences between the State and Defense Departments on national security matters, quoting the old saying that "[w]here you stand is a function of where you sit."[92]

The differences between CCIPS and OEO go beyond management. They also have different relationships with the field. Because OEO plays a gatekeeping role for attorneys and agents seeking wiretapping orders, OEO can be a bureaucratic hurdle. In contrast, CCIPS attorneys tend to possess seemingly magical powers—they act as the guardians of highly technical knowledge that people in the field tend not to possess.[93]

D. What Intra-Branch Separation of Powers Would Look Like

Because of these differences in focus, makeup, management, and relationships with the field of the two sections, CCIPS and OEO should be consulted simultaneously to weigh in on difficult and novel questions regarding electronic surveillance. This can take many forms. Prosecutors in the field may be instructed more often to call both offices for informal advice or formal briefing. Political appointees who run the Department of Justice may do the same. Rules may be drafted instructing OEO and CCIPS attorneys to act as consultants on new matters and to comment upon, if not co-author, court briefs.

As with any call for a new bureaucratic process, this will add inefficiency and take more time, but it will be worth the costs. Nevertheless, this proposal should be restricted to cases of new technology and unresolved case law, the Bleeding Edge cases mentioned earlier. When an issue involves an old technology or well-settled questions of law, the Settled and Leading Edge categories, one section should be able to address the question on its own.

Sometimes exigencies will not permit sufficient time to consult both agencies. The FBI may want to conduct a particular form of surveillance to prevent a prospective crime or to avoid flight. In those

92. Katyal, *supra* note 8, at 2324–27 (internal quotations omitted).

93. This quick summary, like so much of the anecdotal information in this essay, helps prove the point but belies the true complexity of the situation. In reality, some OEO attorneys are likely trusted in the field for their knowledge and good counsel, while some CCIPS attorneys are probably seen as officious bureaucrats.

cases, review by the other section can come ex post, assuming each section is obligated to disclose to the other section the decision made and share the underlying evidence.[94]

The point of the exercise is not to encourage constant disagreement and bickering. In some cases, the two sections will probably agree when both are guided by the same legal concepts and understandings of technology. But disagreements will probably happen too, stemming from differences in the sections' institutional roles, personalities, predictions about future trends, or even worldviews. Each disagreement will require a tiebreaking ruling by a neutral arbiter, and because these two sections are managed by different DAAGs, this tiebreaking will likely be performed by the Assistant Attorney General in charge of the Criminal Division.

This is an appropriate use of the Justice Department's resources. Technology moves rapidly, and basic civil liberties are in play with each advance. The higher echelons of Justice Department management *should* be involved when new, highly invasive techniques are proposed. Today, police officers and prosecutors around the country weigh constitutional and statutory law in deciding what type of process is needed, if any, for surveillance of cell phone networks, GPS beepers, and cloud computing services. In making these determinations, which impact the personal privacy of millions of citizens, it would be wise to involve politically appointed managers—people who are accountable directly to the voting population. If those outside law enforcement cannot take a seat at the table during these deliberations, at the very least, their interests should be represented by those who are most politically sensitive.

When the sections agree—deciding that a new surveillance technique requires high or low levels of process—the public should have greater confidence in the result because it was reached independently and from different vantage points. When the sections disagree—with one section recommending higher levels of process and the other recommending lower levels of process—upper-level management will need to break the tie. Whether this will result in a net gain or loss for civil liberties is difficult to predict. If the section that would have had authority absent this check opted for lower levels of process, then adding a new voice would increase the odds of a favorable result for civil liberties. If the reverse was true, it would result in less favorable results

94. *See* Katyal, *supra* note 8, at 2326 (recommending ex post review of national security decisions "when responding to disaster or sudden invasion").

for civil liberties. It is impossible to say categorically which is more likely to occur.

E. Spurring Intra-Branch Debate About Electronic Surveillance

If we can protect privacy from unwarranted, invasive new forms of electronic surveillance by pitting parts of the Justice Department against one another, how can we spur this change? We may apply pressure from outside the executive branch. Congress, for example, may try to utilize its oversight power to pressure the administration to refer electronic surveillance matters to more than one subpart of the Department. The executive branch is likely to resist too much pressure. Congress can also act indirectly, for example, by requesting regular reporting about the number of components or attorneys in the Justice Department who are consulted regarding new forms of electronic surveillance. Congress can also rely on softer, less formal mechanisms—hearings, letters, or political pressure—to encourage this result.

The judiciary may also put pressure on the Justice Department to gather advice from beyond a narrow sphere of advisors. For example, a judge faced with a particularly narrow brief may ask for supplemental briefing. Judges can also take note of the subcomponents represented on the signature page of a brief and place pressure on attorneys to expand the range of advisors.

The Justice Department itself can and should assign responsibility for electronic surveillance to different sections within the Criminal Division. Once again, CCIPS and OEO are the most logical choices for such a division of labor. Other components may also play a relevant role, such as the Fraud, Narcotics and Dangerous Drug, and Child Exploitation and Obscenity Sections, since each of these sections investigate crimes using electronic surveillance. Finally, the Justice Department should consider the split authority for electronic surveillance as it allocates hiring authority to the sections, ensuring that talented and technically knowledgeable attorneys continue to be staffed in both OEO and CCIPS.

Conclusion

As reformers urge Congress to overhaul ECPA and appeal to the Supreme Court to reinvent the Fourth Amendment, they must take care not to ignore the full set of tools at their disposal. Thus far, efforts to reform surveillance law have focused almost entirely on inter-branch proposals that give the judiciary greater oversight over requests to conduct surveillance. Reformers should supplement these

efforts with appeals directed at the Justice Department itself to find ways to increase the frequency, depth, and importance of intra-agency oversight over electronic surveillance. This is not a supplement for other forms of reform; we need greater judicial oversight in addition to this proposal.

Meanwhile, the type of institutional analysis advocated should extend beyond this relatively narrow concept. It is likely that every state attorney general's office, U.S. Attorney's office, and county district attorney's office has a divide like the one between OEO and CCIPS. Reformers with local knowledge should encourage government officials to engage in the intra-agency debate and deliberation described above. One voice is good, but two are better.