Article

Probably Probable Cause: The Diminishing Importance of Justification Standards

Paul Ohm†

The laws that govern police access to private information act like a volume knob set to an officer's level of certainty: the more certain an officer is that a desired investigative step will turn up evidence of a crime, the more weight we give to his or her request to access private information, and the more privacy we allow his or her request to outweigh. These laws rest upon the belief that we can distinguish between meaningfully different levels of police certainty and balance them against meaningfully different levels of privacy. But what if they rely on a false precision? What if the police rarely have any suspicion without having a great amount of suspicion?

This Article challenges the implicit trust and great weight our search and surveillance laws place on so-called justification standards. This is a timely intervention, because the faith in justification standards is growing.[1] The most important standard, probable cause, derives from the Fourth Amendment to the Constitution,[2] but over the past few decades, the courts and Congress have embraced other, lower standards—given names

† Associate Professor of Law, University of Colorado Law School. I want to thank the editors of the *Minnesota Law Review*, Professor Bill McGeveran for the invitation to participate in the Symposium, and Michael Beylkin for his excellent work as a research assistant.

1. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007) (arguing for a "reconceptualization" of the Fourth Amendment's justification standards).

2. U.S. CONST. amend. IV provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

like "reasonable suspicion" and "mere relevance"—demanding less of the police and in return justifying less invasive intrusions.[3] Recently, some scholars have argued for an even broader use of justification standards, applying them where they have not before been applied, and devising new levels of certainty, apparently continuing to believe that we can measure police certainty in small and distinct increments.[4]

This Article pushes back against this trend by arguing that changes in communications and surveillance technologies have collapsed the categories of police justification. In increasingly common situations, whenever the police have any suspicion at all about a piece of evidence, they almost always have probable cause and can meet the highest level of justification. In these situations, police need is a monolith, an all-or-nothing thing, not something we can tune our laws to in small steps.

Understand the limits of this claim: for traditional investigations involving little or no modern technology, the old assumptions about the differences between probable cause and reasonable suspicion continue to hold. For example, the beat cop on the sidewalk will often have reasonable suspicion about unfolding, suspicious activity long before he or she has probable cause.[5]

But when crime moves from the sidewalk to the Internet, something very different unfolds. When investigating an Internet crime scene, the police almost always have probable cause whenever they have any suspicion at all due to the design of modern communications networks and, in particular, because of the crucial role played by online intermediaries like telephone and Internet service providers. This important point has never before been recognized by legal scholars: the Internet is a hunch-free zone.

This matters a great deal because Congress has constructed an elaborate warren of online privacy protections that describe a sliding scale that tries to mirror the Fourth Amendment's: the more suspicion the police have, the more online privacy they are entitled to invade. These statutes, and in particu-

3. *See infra* Part I.A.

4. *See* SLOBOGIN, *supra* note 1, at 30–45 (arguing for a "proportionality principle" that adds justification standards to new situations).

5. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968) (creating the reasonable suspicion standard for sidewalk stop-and-frisk encounters).

lar the Electronic Communications Privacy Act (ECPA),[6] promise a finely crafted privacy but, it turns out, deliver a much more roughly hewn product. And because so much conduct and communication, criminal and otherwise, have moved online, with more moving online each day, laws like ECPA now define a crucial bulwark of privacy in modern life.

This matters as well because in the near future, Congress will likely revisit ECPA, which was written in 1986 when fewer than 10,000 computers connected to the Internet. If past is precedent, the debate about how to amend ECPA will center on justification standards. Privacy groups will urge Congress to increase ECPA's many standards up to probable cause. The Justice Department will forcefully resist, arguing that higher standards will lead to undetected and unsolved crime.

But this coming debate will amount to nothing but sound and fury. Because the police tend to have either probable cause or nothing whenever they investigate a crime online, any hard-fought changes from lower to higher standards will do very little to alter the balance between privacy and security. Congress should instead seek other ways to balance police need with privacy, and this Article provides a menu of such options including increased judicial and legislative oversight, new procedures, and additional consequences for violations.

Finally, the collapse of justification standards will challenge traditional approaches to surveillance law beyond ECPA, particularly in the interpretation of the Fourth Amendment. As the intermediated architecture of the Internet spreads to new parts of society, the categories of police certainty will collapse in new types of investigations. Carefully calibrated justification standards will mean less with each technological innovation, which will force us to find new approaches to ensuring the Fourth Amendment's protections keep pace.

This Article proceeds in four parts. Part I describes the constitutional roots of justification standards and the important role they play in online privacy law. Part II offers the proof of the Article's central argument: at every stage of an online investigation, the police tend to have probable cause or nothing at all. Part II also offers three important exceptions, none of which swallow the rule. Part III describes what we should change about ECPA once we stop fighting about whether we

6. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

should change its justification standards. Part IV extends the argument from ECPA to the Fourth Amendment and beyond.

I. JUSTIFICATION STANDARDS

Courts weighing the legality, under the Constitution or a statute, of police stops, seizures, searches, and arrests, often rely on justification standards. According to these standards, as the police begin to narrow their investigations to fewer people and places, the law allows them to engage in more invasive deprivations of privacy.[7] These standards are stated as probabilities, measuring how likely it is that the police action will lead to evidence of crime.[8] The most important three standards are probable cause, reasonable suspicion, and mere relevance, and they each find root in the Fourth Amendment.

A. CONSTITUTIONAL ROOTS

The Fourth Amendment expressly recites only one justification standard—probable cause, the standard for obtaining a search warrant.[9] Courts have introduced other standards into Fourth Amendment doctrine that the police must meet before they can search or seize people or property, sometimes saying that these standards satisfy the text's requirement of probable cause, but more often endorsing these standards under a general rule of reasonableness for state surveillance which they identify in the Amendment's prohibition against "unreasonable searches and seizures."[10]

7. *See Terry*, 392 U.S. at 21 ("[T]here is 'no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails.'" (quoting Camara v. Mun. Court, 387 U.S. 523, 536–37 (1967))); SLOBOGIN, *supra* note 1, at 21 ("[A] search or seizure is reasonable if the strength of its justification is roughly proportionate to the level of intrusion associated with the police action.").

8. *See* New Jersey v. T.L.O., 469 U.S. 325, 346 (1985) ("[T]he requirement of reasonable suspicion is not a requirement of absolute certainty: 'sufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment . . . .'" (quoting Hill v. California, 401 U.S. 797, 804 (1971))).

9. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

10. *Id.* ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

Most importantly, the Supreme Court in 1968 embraced the "reasonable suspicion" standard in *Terry v. Ohio*.[11] In *Terry*, the Court upheld both short, investigatory sidewalk stops and ensuing frisks for weapons even when police lack probable cause.[12] The touchstone of the standard is reasonableness, and in such situations a police officer is allowed to rely not on "inchoate and unparticularlized suspicion or 'hunch[es]'" but rather on "specific reasonable inferences which he is entitled to draw from the facts in light of his experience."[13]

Reasonable suspicion remains the standard for investigatory stop and frisk, but this standard has been spotted in only a few other places in constitutional criminal procedure. Most importantly, *Terry* is often cited in the "special needs" cases, which dispense with the warrant and probable cause requirements when they might interfere with specialized, non-law enforcement government purposes, such as school discipline and safety,[14] government workplace searches,[15] probationer monitoring,[16] and drug testing of some state employees.[17]

11. 392 U.S. at 30 (approving "carefully limited search[es]" for weapons "where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous").

12. *See id.* at 27 ("[T]here must be a narrowly drawn authority to permit a reasonable search for weapons for the protection of the police officer, where he has reason to believe that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual . . . .").

13. *Id.*

14. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) ("[T]he accommodation of the privacy interests of schoolchildren with the substantial need of teachers and administrators for freedom to maintain order in the schools does not require strict adherence to the requirement that searches be based on probable cause . . . .").

15. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 724 (1987) ("In our view . . . a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers.").

16. *See, e.g.*, Griffin v. Wisconsin, 483 U.S. 868, 875–76 (1987) ("We think it clear that the special needs of Wisconsin's probation system . . . justify replacement of the standard of probable cause by 'reasonable grounds' . . . .").

17. *See, e.g.*, Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 666 (1989) ("[The Government's] substantial interests [in drug testing Customs agents] . . . present a special need that may justify departure from the ordinary warrant and probable-cause requirements."); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 620 (1989) ("The Government's interest in regulating the conduct of railroad employees to ensure safety . . . 'likewise presents special needs beyond normal law enforcement that may justify depar-

Other less-than-probable-cause standards sometimes appear in Fourth Amendment cases, but these are less well defined. For instance, the police can compel papers or testimony from people with a grand jury subpoena upon a showing of mere relevance without violating the Constitution.[18] Moreover, when something is found not to be a search or a seizure, no justification at all is needed. The police can look through "open fields,"[19] fly over private property,[20] pull garbage from the curb,[21] and track phone numbers dialed[22] with no justification.

B. STATUTORY STANDARDS FOR ONLINE PRIVACY

The Fourth Amendment's protections weaken online because the Supreme Court has refused to apply the Fourth Amendment to cases involving certain records held by third-party intermediaries like banks[23] and telephone companies.[24]

---

tures from the usual warrant and probable-cause requirements.'" (quoting *Griffin*, 483 U.S. at 873–74)).

18. *See* United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) ("[W]here . . . a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines 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.").

19. Oliver v. United States, 466 U.S. 170, 183–84 (1984) ("[I]n the case of open fields, the general rights of property protected by the common law of trespass have little or no relevance to the applicability of the Fourth Amendment.").

20. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450 (1989) ("[The police] were . . . free to inspect the yard from the vantage point of an aircraft flying in the navigable airspace as this plane was."); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) ("We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment.").

21. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40 (1988) ("[W]e conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.").

22. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745 (1979) ("We . . . conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"). Phone number tracking is now regulated by statute. *See* Pen Register and Trap and Trace Act, 18 U.S.C. §§ 3121–3127 (2006).

23. United States v. Miller, 425 U.S. 435, 445–46 (1976) (holding that documents produced pursuant to subpoenas *duces tecum* directed against banks were not in violation of the Fourth Amendment).

24. *See, e.g.*, *Smith*, 442 U.S. at 736 n.1, 745 (concluding that the installa-

Whether or not these cases will control in the case of e-mail or web surfing records remains to be decided, but Congress has tried to patch a potential gap in privacy protection by enacting several important privacy statutes which, like the Fourth Amendment, demarcate the line between permissible and impermissible surveillance with justification standards.[25]

When Congress deems something a particularly invasive type of surveillance, it typically requires probable cause to conduct it. For example, the police need probable cause to monitor a person's electronic communications in real time under the Wiretap Act,[26] and intelligence agents need probable cause to conduct electronic surveillance under the Foreign Intelligence Surveillance Act.[27]

In contrast, two important statutes—the Stored Communications Act (SCA)[28] and the Pen Register and Trap and Trace Act (Pen Register Act),[29] both originally enacted in the ECPA—permit the police to access some online communications and records with less than probable cause. The SCA governs police access to information stored with an online intermediary.[30] It governs access to both content,[31] for example, e-mail messages stored with an e-mail provider like Gmail, and noncontent,[32] for example, a log file revealing the Internet protocol (IP) addresses of those who have visited a given webpage.

The SCA requires the police to demonstrate probable cause before they may access some content stored with some providers, for example some e-mail messages.[33] In other cases, the

tion of a pen register—"a mechanical device that records the numbers dialed on a telephone"—does not constitute a "search" within the meaning of the Fourth Amendment).

25. *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). (governing government access to information transiting or stored on computer networks).

26. 18 U.S.C. § 2518(3) (2006). The Wiretap Act requires the police to meet a series of other obligations before conducting a court-ordered wiretap. *See id.* § 2518(1).

27. 50 U.S.C. § 1805(a)(3) (2006).

28. 18 U.S.C. §§ 2701–2711.

29. *Id.* §§ 3121–3127.

30. *See id.* § 2703 (describing the procedures a governmental entity must abide by to require the disclosure of a wire or electronic communication).

31. *See id.* § 2703(a).

32. *See id.* § 2703(b).

33. *See id.* § 2703(a). The text is arguably ambiguous about which e-mail messages receive this protected treatment, and the question is under debate in the courts. *See infra* Part II.B.2.

SCA requires one of two lesser standards, the mere-relevance standard for a grand jury or administrative subpoena,[34] or the standard specified in 18 U.S.C. § 2703(d) for obtaining a court order, colloquially called a "d-order."[35] To obtain a d-order, the police must offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[36] Like the Supreme Court did in *Terry*, the d-order requires "specific and articulable facts,"[37] which has led some scholars to refer to a d-order as a *Terry*-stop requirement for e-mail.[38] At any rate, the d-order standard is probably much more stringent than the mere-relevance subpoena standard.[39]

The Pen Register Act governs police surveillance of non-content attributes of electronic communications in real time.[40] The police must comply with it to track, for example, the phone numbers dialed from a particular phone or the IP addresses of the websites visited by a particular user.[41] The justification standard is low, requiring "relevan[ce] to an ongoing criminal investigation."[42] Moreover, the police are not required to divulge the facts that establish relevance; instead, they need merely "certif[y] . . . that the information likely to be obtained" is relevant.[43] Courts have interpreted this to mean that they

34. *See* 18 U.S.C. § 2703(b)(1)(B); *see also In re* Gimbel, 77 F.3d 593, 598 (2d Cir. 1996) (extending the Supreme Court's holding in United States v. Morton Salt Co., 338 U.S. 632, 652 (1950), that administrative subpoenas for corporate records need only be "reasonably relevant" to individual financial records).

35. *See, e.g.*, 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, 1219 (2004) (discussing the "d-order" under § 2703(d)).

36. 18 U.S.C. § 2703(d).

37. Terry v. Ohio, 392 U.S. 1, 21 (1968).

38. ORIN S. KERR, COMPUTER CRIME LAW 515–16 (2006).

39. *See* Kerr, *supra* note 35, at 1233–35 (arguing the subpoena requirements should be dropped as "surprisingly low" in favor of a d-order requirement). *But see* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 161–62 (2005) (arguing that the d-order requires only relevance and materiality, both low standards under evidence law).

40. 18 U.S.C. §§ 3121–3127; *see also id.* § 3127 (defining "pen register" and "trap and trace device").

41. *See id.* § 3127(3).

42. *Id.* § 3123(a)(1).

43. *Id.* § 3122(b)(2).

lack the discretion to deny pen register applications that are properly formed.[44]

Congress probably implemented these sub-probable cause standards in the SCA and Pen Register Act for two reasons. First, Congress might have wanted to strike a compromise, giving the government access to information that did not seem terribly private and thus not worthy of the protection of probable cause, while at the same time setting the standard at a high enough level to prevent police fishing expeditions. According to legislative history, the d-order standard was designed specifically to prevent fishing expeditions. The House Report explained that Congress crafted the d-order standard to be "higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against 'fishing expeditions' by law enforcement."[45]

Second, Congress might have set sub-probable cause standards because it wanted to provide privacy-by-tuning-knob online. It might have imagined that it could allow moderate incursions into online privacy when the police have moderate levels of suspicion.

My hunch-free Internet theory contradicts the second rationale more than the first. Fishing expeditions sometimes happen online, although as I will argue, they seem to happen much less often than some people believe.[46] Our laws should require justification standards to prevent fishing expeditions, and this Article does not argue otherwise, but I will demonstrate why privacy-by-tuning-knob just does not work.

C. CALLS FOR REFORM

Scholars who have considered the question unanimously agree that Congress should amend the SCA and Pen Register Act to strengthen privacy protection, and many have focused on elevating justification standards.[47] Many recommend a "probable cause for everything" standard, advocating a warrant requirement in place of every subpoena and d-order requirement.

44. *See, e.g.*, United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) ("The judicial role in approving use of trap and trace devices is ministerial in nature.").

45. H.R. REP. NO. 103-827, at 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511.

46. *See infra* Part II.C.1.

47. *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299 (2004).

Daniel Solove, for example, argues that "for most uses of electronic surveillance, warrants supported by probable cause should be required."[48] Similarly, Patricia Bellia recommends that "Congress should apply a uniform search warrant standard to all stored communications."[49] Deirdre Mulligan concurs, arguing that "the government should not be allowed to examine [the content of stored e-mail messages] without a warrant based on probable cause."[50]

Even Orin Kerr, someone who can fairly be called the legal academy's biggest fan of the SCA,[51] calls the protection of contents in the Act "surprisingly weak" and "surprisingly low."[52] Professor Kerr does not urge a shift to a probable cause warrant requirement, however, choosing instead a "cautious middle ground," that eliminates access to contents based on mere subpoenas and requires at least the d-order standard.[53]

Not only do scholars unanimously argue for changes to statutory justification standards, they imply that this is asking for a lot. Solove calls his recommendation for probable cause for electronic surveillance a "radical solution,"[54] and a "sweeping" suggestion.[55] He seems to gird himself for a fight, raising and refuting the counterarguments he expects from critics.[56] These scholars think they are asking for a lot because they seem to assume that the change to a probable cause standard from something lower is disruptive, even radical. On the contrary, these scholars may be in fact asking for very little.

Not only have scholars argued for probable cause requirements, but privacy groups have also long lobbied Congress and executive branch agencies to impose new probable cause requirements into the SCA. After the 2008 presidential election, a group called the Constitution Project issued a report signed by twenty-one "Allies" including leading online civil liberties groups the Center for Democracy & Technology and the Elec-

48. Solove, *supra* note 47.

49. Bellia, *supra* note 47.

50. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1592 (2004).

51. *See* Kerr, *supra* note 35, at 1242 ("I would give the current SCA a 'B.'").

52. *Id.* at 1233.

53. *Id.* at 1234–35.

54. Solove, *supra* note 47, at 1266.

55. *Id.* at 1299.

56. *See id.*

tronic Frontier Foundation, urging reforms to the SCA.[57] Specifically, the groups asked Congress to require "[c]omprehensive Fourth Amendment standards, including probable cause . . . for law enforcement access to" all stored e-mail under the SCA.[58]

The Justice Department would likely oppose such a change strenuously. We know this because it has done so before: during the harried legislative process to draft the USA PATRIOT Act, Senator Leahy tried to increase judicial standards in the Pen Register Act, reusing language originally introduced a few years earlier by once-Senator and then-Attorney General John Ashcroft.[59] According to Beryl Howell, who served as General Counsel to the Judiciary Committee at the time, the DOJ "flatly rejected this change,"[60] arguing that it would "create[] needless administrative burdens."[61] Senator Leahy dropped the proposal.[62]

We seem set up for an epic battle, one that lines up critical interests on both sides. If Congress takes up ECPA reform, we should expect significant lobbying by both the privacy groups and the Justice Department surrounding justification standards. At the end of the campaign, one side will win and one side will lose, and the justification standards in the SCA and Pen Register Act will or will not be raised. But no matter the result, the fight alone will force both sides to expend political capital. This is capital that could be spent instead on trying to effect other much more meaningful change, rather than a paper victory that will mean little.

II. WHY THE POLICE USUALLY HAVE PROBABLE CAUSE ONLINE

The central claim of this Article is that at almost every stage of almost every criminal investigation on the Internet,

57. *See* THE CONSTITUTION PROJECT, LIBERTY AND SECURITY: RECOMMENDATIONS FOR THE NEXT ADMINISTRATION AND CONGRESS 184–90 (2008), *available at* http://www.constitutionproject.org/pdf/Liberty%20and%20Security%20Transition%20Report.pdf.

58. *See id.* at 184.

59. *See* United and Strengthening America Act of 2001, S. 1510, 107th Cong. § 214 (2001); Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1199 (2004) (commenting on Senator Leahy's proposal to modify the Pen Register Act).

60. Howell, *supra* note 59, at 1199.

61. *Id.*

62. *See id.*

the police have either probable cause or no suspicion at all, but they almost never fall somewhere in between these extremes. Before defending this claim fully, let me offer an intuitive, albeit somewhat oversimplified version: we almost never stumble upon decontextualized e-mail addresses or IP addresses—the two most important types of evidence online. Instead, we find them attached to things like e-mail messages and logfiles, and thanks to some characteristics of the Internet, they are almost never "somewhat suspicious" or "out of place," "kind of fishy" or "just not right." Instead, when the police find an e-mail address or IP address that they think is related to a crime, they almost always know that a request for more information about the address will lead either to information relevant to the investigation or to a dead end.

It is tough to prove this claim, because one can always dream up a hypothetical story of a police officer who might someday want to investigate an e-mail address or IP address with less than probable cause. I am not claiming to have uncovered a universal truth about the Internet, or a structural impossibility. Instead, I am making a claim about overwhelming tendencies based on behavior that flows from what the Internet makes possible. I present two partial proofs: the first is structural, highlighting how the technological architecture of the Internet collapses the differences between reasonable suspicion and probable cause that exist in the physical world. The second is empirical: no court opinion I could find has held that the police lacked probable cause to investigate an e-mail address or IP address, and even when the Ninth Circuit shifted from a mere relevance to a probable cause standard for access to e-mail, the Justice Department seemed hardly to mind.

A. STRUCTURE

Internet crime scenes are always hot or cold, but never warm. In this way, they are very different from the sidewalk streetscape in *Terry*, and they differ in ways that make it highly unlikely the police will ever have reasonable suspicion but not probable cause online.

1. Sample Investigations

To start, think about how the police gather evidence at crime scenes in the real world and online, and consider how they accumulate suspicion in each case. First, consider two thefts. Imagine the police respond to a report of an armed rob-

bery at Max's Liquor Store on Main Street. They arrive to a scene of chaos: broken glass litters the shop floor; a shopper sits with nose bloodied talking to paramedics; the cash register sits open and empty; and the traumatized shopkeeper stammers in the corner. The police begin systematically wading through a sea of ambiguous leads, hoping to find a clue as to the identity of the thief. They interview everybody on the scene: the shopkeeper, shoppers, neighbors, and passersby. They dust the scene for fingerprints, most likely turning up many in this public space. If they are lucky, the shop has a surveillance camera and the police take the tape hoping to get a look at the thief. Back at the office, they pore through records of past crimes in the area matching this one, and they might "round up the usual suspects."

Now, imagine the equivalent crime scene online. An important company server owned by MaxCo has been hacked and from it valuable trade secrets have been stolen. The police who arrive on scene encounter a much calmer environment, an air-conditioned machine room in the bowels of MaxCo's headquarters. A technician shows the officers the hacked server, and an agent who specializes in computer investigations takes originals and copies of the data on the computer and other computers connected to it. Most importantly, the technician hopes to find logfiles, automated records kept by the company recording the IP addresses used to access the computer during the time of the attack.

Next, consider two death threats. In the real world, Susan, a local businesswoman, receives an envelope in the mail containing a handwritten death threat. The police called to investigate are hard pressed to find many clues on the note itself. They dust it for fingerprints but find none. From clues on the envelope, they determine the part of the city from which the letter was sent, and they interview the letter carriers and post office employees from that area, trying to find somebody who recalls the letter or the person who sent it. As a long-shot, they may show the letter to a handwriting analyst or personality profiler who will try to make guesses about the type of person who sent it.

Compare instead a death threat sent to Jim via e-mail. The crime scene is Jim's e-mail inbox, the contents of which police technicians copy carefully for later analysis. Compared to the real-world message, the e-mail message itself is a goldmine, providing leads to the identity of the sender, most importantly

in the message headers like the "To" line and the "Received" lines that show the path the message took across the Internet.

2. How Suspicion Builds in the Real World and Online

Seen through the lens of police suspicion, real-world crime scenes are strikingly different from their online counterparts. In the real world, the police officer discovers evidence as a continuous stream of facts, some increasing, others decreasing, and still others not changing his or her overall level of suspicion. In the theft at Max's Liquor Store, a passerby might describe the thief as tall with short hair, a shopper might remember that he walked with a limp, and the shopkeeper might suspect a gang of neighborhood teenagers who had been hassling him. In Susan's case, the police will theorize about who might have the motive to threaten Susan, but they will find little of interest from the letter itself. In both cases, the facts settle like layers of sediment on a lake bed, building up the amount of suspicion the police have about any particular suspect.

In contrast, the shape of the line graph plotting the level of police suspicion in an online investigation is discrete and jumpy, not smooth and continuous. When an online victim reports a crime, he or she often hands over a record of the crime itself. MaxCo's administrators will turn over the network logfiles and Jim will produce the threatening e-mail message. The police explore the leads in these records, which are almost always either gold mines or dead ends, rarely something in between. Jim's e-mail message has headers, which list either the genuine e-mail address used to send the message—leading the police to the company hosting the e-mail account—or a fake e-mail address—leaving the police no lead.

When a genuine e-mail address is used, the e-mail provider can usually provide the police with the IP address from which a user has been accessing the account associated with the e-mail address, which gives the police probable cause to contact the phone company or cable provider who administers that address.[63] As with the e-mail provider, these providers will either find the next lead in their databases—a particular customer, at a particular address—or they will find nothing. Finally, with this information, the police can obtain a traditional search war-

63. *See* United States v. Perez, 484 F.3d 735, 741–42 (5th Cir. 2007) (holding that an IP address attached to an e-mail address is sufficient to establish probable cause).

rant to search the target's house and seize and search any computers found.

Online, an officer almost never encounters evidence which makes him or her a "little more suspicious" or will narrow down the suspect pool without pointing the finger directly at the target, as real-world evidence often does. An e-mail address cannot point to short men, or experienced computer users or men with moustaches. Steps in online investigations never lead to fragments of IP addresses or pieces of suspicious e-mail addresses. Internet crime scenes always provide feast or famine—they never leave the officers just a little hungry.

What explains the differences in online and real-world crime scenes? Why does evidence online emerge in bursts, not in sedimentary layers?

3. Why Online Cases are Different

In the 1993 movie *The Fugitive*, Tommy Lee Jones's federal marshal memorably directs a group of agents to look for Harrison Ford's fugitive, emphasizing the localness of the pursuit:

> Our fugitive has been on the run for ninety minutes. Average foot speed over uneven ground barring injuries is four miles an hour. That gives us a radius of six miles. What I want out of each and every one of you is a hard-target search of every gas station, residence, warehouse, farmhouse, henhouse, outhouse, and doghouse in that area. Checkpoints go up at fifteen miles.[64]

Given Hollywood's tendency to resort to implausible dramatic conventions when depicting computer crime,[65] it is not difficult to imagine a future summer blockbuster featuring the following speech by an FBI agent after a network intrusion:

> Our hacker has been in the system for ninety minutes. He entered through a 1.5 megabit per second T1 line. This means he is within 255 IP addresses. What I want from each and every one of you is a search of every router, switch, access point, virtual world, web site,

64. THE FUGITIVE (Warner Bros. 1993).

65. In Hollywood's imagination, hackers can always process screens full of text (usually green-on-black) scrolling by at a speed no human can process; government agency video specialists can turn the grainiest images into perfectly sharp video with a few clicks of the keyboard (and they never use mice); and every network can be accessed through an elegant, three-dimensional, virtual reality interface. *See* Matthew Inman, *What Code DOESN'T Do in Real Life (That it Does in the Movies)*, DRIVL, June 12, 2006, http://web.archive.org/web/20070202190507/www.drivl.com/posts/view/494; CRACKED Staff, *5 Things Hollywood Thinks Computers Can Do*, CRACKED, Sept. 13, 2007, http://www.cracked.com/article_15229_5-things-hollywood-thinks-computers-can-do.html ("#2: A Computer Might Become Self-Aware at any Moment.").

> cable headend and DSLAM in that area. Online checkpoints go up at the nearest Class-C addresses.

Such a speech would elicit guffaws from the geeks in the audience, because the Internet's placelessness makes the idea of such a localized search nonsensical. Local knowledge matters much less online than it does in the real world.[66] The police would be wasting their time if they interviewed passersby and neighbors after a computer intrusion or e-mail death threat. Sometimes they interview the computer technicians who maintain the victim's computer but usually to develop a technical picture, not to look for clues to whodunit.[67]

Suspicion builds incrementally in the real world and oscillates between probable cause and nothing online for at least five reasons. First, evidence online almost always comes surrounded by a rich context, providing a high level of built-in suspicion to a suspicious e-mail or IP address. Second, the path from victim back to suspect is fixed and often traceable. Third, the "eye witnesses" online tend to be sophisticated corporate intermediaries without relevant biases or agendas. Fourth, these intermediaries and the victims themselves deploy pervasive systems of surveillance. Fifth, these surveillance systems record precise, unambiguous evidence.

a. Rich Contextualization

First, and most importantly, online evidence such as e-mail addresses and IP addresses almost always come to the police wrapped in rich contexts of suspicion. The IP address supplied by MaxCo is relevant only because it is tied directly to the intrusion; the e-mail address supplied by Jim is likewise stamped directly on the threatening e-mail message. Police officers almost never focus on IP addresses or e-mail addresses without a direct and unambiguous link to the crime under investigation.

The police officer in *Terry*, Officer Martin McFadden, walked a neighborhood beat and kept a watchful eye for people and behavior that did not belong.[68] Today, when Officer

66. *Cf.* Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1 (discussing the changing procedures and practices of criminal investigations with the advancement of the Internet).

67. There are, of course, exceptions. Sometimes, the hacker is a disgruntled ex-employee, and death threats online often come from people who also know the victim in the real world. But local knowledge like this is much more likely to be irrelevant.

68. Terry v. Ohio, 392 U.S. 1, 5 (1967) (testifying that "he had been as-

McFadden logs onto the Internet, he no longer walks a beat, because crimes are being committed away from public scrutiny, in private e-mail inboxes and servers.[69] There are no sidewalks online. Officer McFadden no longer finds crime; victims of crime find him, and they come bearing bundles of digital evidence that link the crime directly to an e-mail or IP address.[70]

b. Fixed Points

Tommy Lee Jones's marshal had to check every "henhouse, outhouse, and doghouse" inside a six-mile radius, because he lacked evidence of directionality.[71] Harrison Ford's character could have fled in any direction on the compass, and he might have zigged and zagged to throw his pursuers off his trail.[72]

In contrast, police officers retracing an online criminal's steps from an original e-mail message or log file entry will find themselves tracing their way through a fixed series of upstream points.[73] From every point there will be one, and only one, next point upstream leading inexorably back to the criminal, and if there is any evidence of that next point, it leads in one accurate direction.[74] An e-mail message arrives at a victim's inbox after being handed off from e-mail server to e-mail server along a series of fixed points. A hacker sends damaging payload to a victim's computer over a series of links along a similar series of fixed points.

This is not to say that the police will always be able to trace the series of fixed points from sender to receiver. For one thing, some of the points may sit in foreign countries whose service providers will not be amenable to requests from U.S.

signed to patrol this vicinity of downtown Cleveland for shoplifters and pickpockets for [thirty] years").

69. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 575 (2009) ("[Third-party internet services] act as remote agents that permit wrongdoers to commit crimes entirely in private.").

70. *See, e.g.*, *id.* at 562 (explaining that wrongdoers sometimes expose evidence through e-mail, "creat[ing] an important opportunity for criminal investigators").

71. THE FUGITIVE, *supra* note 64.

72. *Id.*

73. *Cf.* Solove, *supra* note 47, at 1265 (discussing the ease with which e-mail messages and other electronic communications can be discovered).

74. For an example of this investigative process, see Matthew Sedensky, *Investigators Followed Digital Trail in Pregnant Woman's Killing*, SEATTLE TIMES, Dec. 21, 2004, http://seattletimes.nwsource.com/html/nationworld/2002125795_baby21.html.

law enforcement agents.[75] Also, criminals sometimes use technologies like anonymizing proxies or onion-routing protocols to make it difficult, if not impossible, to find the next step upstream.[76] Even though a single series of fixed points always exists from sender to recipient, sometimes the police might not be able to trace it.[77]

That communications travel through the Internet along a traceable series of fixed points might seem at odds with popular understandings of how the Internet works. Readers should not be confused by the fact that the Internet's pathways shift over time, and packets that travel from Point *A* to Point *B* today might take a very different route than those that travel from Point *A* to Point *B* tomorrow.[78] While true, the shifting routes of the Internet almost never make a difference in a criminal case,[79] because the only thing the officer cares about is that the attack on Point *B* originated from Point *A*.[80] It is the same

75. *See* Will Sturgeon, *Federal Agent Raps ISPs Over Cybercrime*, CNET NEWS.COM, Jan. 25, 2005, http://news.cnet.com/Federal-agent-raps-ISPs-over-cybercrime/2100-7348_3-5549723.html (recounting FBI official's complaint about how American ISPs respond slowly to requests from UK law enforcement).

76. *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 274–76 (2008) (discussing how technologies that conceal user identities can "hinder law enforcement").

77. *See id.* at 274–75 (explaining various techniques criminals can use to evade tracking of their Internet use).

78. To get a bit more technical about things, at the transport layer, Internet Service Providers use routing protocols that adapt to outages and congestion by pushing data along better routes. *E.g.*, 1 DOUGLAS E. COMER, INTERNETWORKING WITH TCP/IP 115 (4th ed. 2000). Perhaps the most important routing protocol is the Border Gateway Protocol, or BGP. *See generally* THE INTERNET SOCIETY, A BORDER GATEWAY PROTOCOL 4 (BGP-4) (2006), http://www.tools.ietf.org/pdf/rfc4271 (providing an in-depth discussion of the purpose and uses of BGP-4).

79. In an early and influential article on computer crime, Neal Katyal placed far too much emphasis on how packets and shifting Internet routes hinder law enforcement. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1072 (2001) ("Unlike a criminal who needs to escape down a particular road, a criminal in cyberspace could be on any road, and these roads are not linked together in any meaningful fashion."). Katyal errs because he focuses too much on the shifting nature at the packet layer, even though almost all criminal investigation online occurs at higher layers. *See id.*

80. While Point *A*'s importance stems from clues it provides about the wrongdoer, electronic routes can bear on criminal cases in other ways, such as satisfying jurisdictional requirements. *See* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (holding that an electronic bomb threat sent and received in Utah nevertheless satisfied an interstate commerce requirement because the message passed through a server in Virginia).

thing in the real world. In the case of the death threat delivered by postal mail, what route the mailman took from the post office to the victim's house does not matter, because what we care about is who sent the letter upstream. Similarly, a police officer investigating a death threat from badguy@gmail.com will go to gmail.com and could not care less what route the message traveled from gmail.com to the victim's inbox.[81]

c. Reliable Witnesses

The eyewitnesses of the Internet are sophisticated corporate intermediaries.[82] Almost all Internet communications are intermediated by at least one corporation, and most are intermediated by more than one.[83] ISPs, like direct subscriber line (DSL) and cable modem providers, carry communications over the "last mile" from homes and businesses; backbone providers carry communications over long distances, across continents and under seas; web hosting companies provide access to websites; search engines locate relevant content; and e-mail providers, social networking sites, and blogging platforms host and deliver individual messages.[84] Police investigators in the online crime scene can often rely on these corporations to serve as sophisticated and unbiased witnesses of online crime.[85] The traumatized victim of an armed robbery in the real world can be an unreliable witness; the corporate record keeper of a large cable company is much less likely to be so.[86]

In fact, the intermediated Internet is becoming even more intermediated. Pick your favorite buzz phrase for this phenomenon—Web 2.0,[87] cloud computing—but they all mean that service providers are beginning to replace the computer pro-

81. *E.g.*, Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 179–80 (D. Conn. 2005) (describing how police requested user information from an Internet service provider following an electronic threat, but did not inquire as to the route it traveled).

82. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 70 (2006) (discussing the evolution of Internet intermediaries).

83. *See id.* at 70–71 (noting the pervasiveness of intermediaries).

84. *See id.* at 70 (calling ISPs, search engines, browsers, the physical network, and financial intermediaries the most important intermediaries).

85. *E.g.*, *Freedman*, 412 F. Supp. 2d at 180 (discussing how police relied on an ISP's records).

86. *Cf.* FED. R. EVID. 803(6) (providing an exception to the hearsay rule for business records).

87. *See generally* Tim O'Reilly, *What is Web 2.0?*, O'REILLY, Sept. 30, 2005, http://oreilly.com/web2/archive/what-is-web-20.html (recounting a brainstorming session that produced the phrase "Web 2.0").

grams we used to run on our personal computers with programs hosted on corporate computers and delivered over the Internet.[88] Google Docs replaces our computers' word processors and spreadsheets;[89] Google Calendar lets us throw away our desktop calendar and pen-and-paper day planner.[90] Services like Amazon's EC2 can replace our powerful servers themselves, by giving us a virtual computer in the cloud we can use to perform computations and run programs.[91]

Cloud computing brings obvious benefits to users—no longer must we install our own software fixes or copy files to a flash drive when we hit the road—but cloud computing will also aid law enforcement. As we move more of our conduct onto intermediated websites, we will leave behind much more detailed and accurate evidence of our conduct, accessible from the unbiased intermediary itself. Just as the transition from phone to e-mail has made it easier to track certain kinds of crimes, so too will the move from offline to online word processing and calendaring.

d. Pervasive Surveillance

The Internet abounds with systems of pervasive surveillance.[92] Most web servers record detailed information about every computer requesting information for thirty days and often longer; e-mail servers memorialize every hop taken by every message at the top of each message itself; and ISPs remember which customers are assigned which IP addresses, when, and for how long.[93] These records are not kept at the behest of some global law enforcement cabal, but instead, they help the human beings who administer these systems track

88. *See* Geoffrey A. Fowler & Ben Worthen, *The Internet Industry Is on a Cloud—Whatever That May Mean*, WALL ST. J., Mar. 26, 2009, at A1 (discussing the meaning of the phrase "cloud computing").

89. Google Docs, http://docs.google.com (last visited Apr. 12, 2010).

90. Google Calendar, http://calendar.google.com (last visited Apr. 12, 2010).

91. Amazon EC2, http://aws.amazon.com/ec2 (last visited Apr. 12, 2010).

92. *See* Slobogin, *supra* note 39, at 140 (discussing various kinds of online surveillance).

93. *See id.* at 145–47 ("In short, even if you stay home and conduct all your business and social life via phone, e-mail and surfing the 'Net, [law enforcement] can construct what one commentator has called 'a complete mosaic' of your characteristics.").

and fix problems and improve services.[94] Increasingly, web hosts keep detailed records to help them turn their traffic into advertising contracts.[95] Many site owners keep detailed records for none of these reasons, but simply because their software does so by default.[96]

Unlike records kept in the real world, online records tend to be precise, detailed, and accurate.[97] The surveillance camera at Max's Liquor Store provides the view from one fixed vantage point, probably hampered by poor lighting or position. Human observers looking at the crime replayed will probably spot different clues and interpret different things from the same images.[98]

In contrast, an entry from a web server's access log provides precise, unambiguous information, at least to one trained to interpret it.[99] The logfile kept by a web server I operate contains this entry:

128.138.161.224 - - [24/Sep/2009:14:47:17 -0700] "GET / HTTP/1.1" 200 4028 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/2009082707 Firefox/3.0.14 (.NET CLR 3.5.30729)"

From this record, I can tell that a visitor from IP address 128.138.161.224 looked at my home page ("GET /") on September 24, 2009, at 2:47 PM PDT ("-0700"). The user appears to be on a machine running Windows, updated with the latest security patches (rv:1.9.0.14), and the Firefox web browser. This data might be cryptic, but to one trained to read it, it is not subject to the kind of ambiguities and matters of interpretation as Max's surveillance camera footage.

94. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1462–66 (discussing reasons why Internet providers monitor customers).

95. *Id.* at 1433–34.

96. *See, e.g.*, *id.* at 1474–77 (describing why web-host customers consent to be monitored by online service providers).

97. *See* Slobogin, *supra* note 39, at 149 ("Given the potential that [Internet] surveillance provides the government for . . . linking people to crime, it could well be even more useful than visual tracking of [a] person's activities . . . and eavesdropping on or hacking into a person's communications . . . .").

98. *E.g.*, Dan M. Kahan et al., *Whose Eyes Are You Going To Believe?* Scott v. Harris *and the Perils of Cognitive Illiberalism*, 122 HARV. L. REV. 837, 838–40 (2009) (describing the Supreme Court Justices' varied impressions upon viewing the same videotape).

99. ERIC T. PETERSON, WEB SITE MEASUREMENT HACKS 79–83 (2005) (explaining how to interpret web server logfiles).

e. Precise Leads

Clues found in the physical environment, like fingerprints and human recollections, can be ambiguous and misleading.[100] Imagine the vast number of fingerprints the police find at Max's Liquor Store and consider how human memories are plagued by human frailties and biases. In contrast, the online evidence stored by the systems of pervasive surveillance tends to be mechanistically precise.[101] Online evidence like stored e-mail addresses or IP addresses in logfiles tend to be the byproducts of automated software systems that do nothing but push data from point *A* to point *B*.[102] These systems perform these tasks unerringly, because the users who rely on them insist that they be perfectly precise.[103] If e-mail servers tended to occasionally mistake a lower-case *l* for the numeral 1, then users would stop using e-mail for important or sensitive messages. If web servers occasionally mistook whitehouse.com for whitehouse.gov, users would revolt. The little breadcrumbs of data that are memorialized from these accurate, inerrant processes become the accurate, inerrant breadcrumbs of evidence used by police.[104]

B. EMPIRICAL PROOF

The structural argument that the Internet is almost always a hunch-free zone is supported further by two sets of empirical, historical observations. First, I could find no case in which a court found that the police lacked probable cause in an online investigation, not even among the handful of cases calling online surveillance into question.[105] Second, in 2004, the Ninth Circuit switched from a relevance to a probable cause

100. *See* Slobogin, *supra* note 39, at 149 (arguing that online electronic surveillance is useful because it provides more precise identifying information than physical evidence).

101. *See* Rubinstein et al., *supra* note 76, at 270–74 (using cookies as an example of how precise personal information is collected online).

102. *E.g.*, *id.* at 272–73 (explaining that the programs capture the "aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result").

103. *See id.* (quoting the CEO of Google as stating that the future of Google depends on its ability to collect and use personal data).

104. *See id.* ("Taken together, this information represents a massive clickstream database . . . . [that] can be subpoenaed and used against litigants . . . .").

105. *E.g.*, Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181–84 (D. Conn. 2005) (holding that law enforcement's discovery of online information was valid not under a theory of probable cause, but because plaintiff lacked a reasonable expectation of privacy).

standard for government access to certain communications under the SCA, and the Justice Department has never sought a legislative fix to reverse this case, suggesting how little the switch has mattered to law enforcement.[106]

1. No Cases Suppressing Evidence

The claim that the police almost always have probable cause in online investigations is supported by the absence of cases in which courts have suppressed evidence in a network-crime case for lack of probable cause. After decades of computer-crime prosecutions in this country, the federal case reporters brim with court opinions from criminal cases taking place on the Internet, yet I know of none in which a court holds that the police lacked probable cause.

First consider cases construing the SCA, because under the SCA, the police can compel the production from an Internet provider of some of the contents of communications stored with the provider with less than probable cause.[107] Although the SCA offers no statutory suppression remedy, one would expect criminal defendants who have had their e-mail messages obtained upon less than a showing of probable cause to bring constitutional challenges.[108] Several defendants have, and although some courts have questioned the constitutionality of some provisions of the SCA, none of these courts has ever suggested that the police lacked probable cause in these cases.

For example, in *United States v. Kennedy*, a district court faulted the government for failing to state "specific and articulable facts" in support of its application for a d-order.[109] Despite coming to this conclusion, the court never suggested that the police failed to meet the d-order standard, an unlikely conclusion given the amount of evidence amassed by police at that stage of the investigation.[110]

106. Theofel v. Farey-Jones, 359 F.3d 1066, 1073–78 (9th Cir. 2004).

107. 18 U.S.C. § 2703(b) (2006) (authorizing compelled disclosure of contents originally maintained solely for purposes of "storage or computer processing" with subpoena or court order).

108. *Id.* § 2708.

109. United States v. Kennedy, 81 F. Supp. 2d 1103, 1109–10 (D. Kan. 2000).

110. The defendant had inadvertently configured his computer to share his files with others on the Internet, and two technicians from his ISP found what they thought was child pornography in the files. *Id.* at 1106–09 (describing the evidence obtained by police). They delivered these files to the FBI, prompting the application for the d-order. *Id.*

Similarly a district court found in *Freedman v. America Online, Inc.* that two police officers had violated the SCA by sending an unsigned search warrant to AOL, but the ruling turned only on the deficient process, not on the level of the officers' suspicion.[111] In fact, given that the officers were requesting subscriber information for an e-mail address used to send a threat, the court almost certainly would have found probable cause.[112]

Finally, consider *Warshak v. United States*, the closest a federal court has come to ruling that the SCA's procedures for access to e-mail with less than probable cause violate the Fourth Amendment.[113] In *Warshak*, a three-judge panel of the Sixth Circuit affirmed a preliminary injunction barring the government from using part of the SCA,[114] but the en banc court vacated the ruling as not ripe.[115] Although the *Warshak* case marked the most significant constitutional challenge ever lodged against the SCA, the police in the underlying case appear to have had a very high level of suspicion about the target of the surveillance, a man since convicted for fraud in the sale of dietary supplements.[116] As one measure of this fact, despite several rounds of litigation, still ongoing, and significant attention from many amici, neither Warshak nor any amicus has ever argued that the government lacked probable cause to seize the messages.[117]

In addition to my review of SCA cases, I surveyed criminal cases involving violations of the Computer Fraud and Abuse

111. Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121, 126–27 (D. Conn. 2004) (holding defendants liable irrespective of whether they "required" or "requested" information from the ISP).

112. The court described the facts in greater detail in a later opinion. Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 179–80 (D. Conn. 2005) (describing an e-mail message sent under the screen name "GoMaryGoAway" stating that "The End is Near" in a case arising out of a local political race).

113. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

114. *Id.* at 460.

115. Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (en banc).

116. *See* Press Release, Fed. Trade Comm'n, FTC Charges Sellers of Avlimil, Rogisen, and Other Dietary Supplements (Feb. 2, 2006), *available at* http://www.ftc.gov/opa/2006/02/avlimil.shtm (describing FTC action against same defendant).

117. *E.g.*, Brief of Amici Curiae Elec. Frontier Found. et al. Supporting the Appellant and Urging Acquittal or Order for New Trial at 4–14, Warshak v. United States, No. 08-4085 (6th Cir. June 10, 2009) (framing arguments against the government in the context of reasonableness instead of probable cause).

Act[118] (CFAA) and the federal child pornography laws,[119] because they often involve Internet-related investigations. Although I did not review every single reported case involving these laws, I did look at all such cases cited in a leading computer crime casebook.[120] While several cases cited in the casebook revealed searches of computers in homes that judges suggested lacked probable cause,[121] none of the cases found a lack of probable cause during the purely online parts of the investigations.[122] Of course, none of this research amounts to conclusive empirical proof, but taken together it strongly suggests that no court has ever found a lack of probable cause in an online case, for such a case surely would have been included in this casebook.

2. The *Theofel* Natural Experiment

Another way to test the claim that the police almost always have probable cause at every stage in an online investigation is to examine a natural experiment stemming from a 2004 case from the Ninth Circuit, *Theofel v. Farey-Jones*.[123]

It is unnecessary to recount fully the complicated facts or dissect the intricacies of Judge Kozinski's opinion for a unanimous panel, because only the punchline is important. Before *Theofel*, the Department of Justice had long interpreted the SCA to permit the government to access e-mail messages opened but stored on an e-mail provider's server with a subpoena or d-order.[124] In other words, under this interpretation,

118. 18 U.S.C. § 1030 (2006).

119. *Id.* §§ 2252–2252A.

120. KERR, *supra* note 38.

121. *E.g.*, United States v. Gourde, 440 F.3d 1065, 1077–79 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting) (arguing that the government's search of a home computer lacked probable cause because it was based only on defendant's paid membership to a child pornography website); United States v. Adjani, 452 F.3d 1140, 1143 (9th Cir. 2006) (holding that the government had probable cause to search a home computer, and reversing the district court's order to suppress); *cf.* United States v. Riccardi, 405 F.3d 852, 861–63 (10th Cir. 2005) (finding a search of a home computer violated the Fourth Amendment's particularity requirement).

122. Both a research assistant and I reviewed the factual description of the investigation from the full court opinion for every CFAA and child pornography case described in Professor Kerr's casebook. KERR, *supra* note 38, at 74–83, 211–49. I concluded that none seemed close to lacking in probable cause. *See* Research Summary Chart Prepared by Paul Ohm, Professor, Univ. of Colorado Law School (on file with author).

123. 359 F.3d 1066 (9th Cir. 2004).

124. Specifically, under the DOJ's interpretation, when a user opened a

government agents could compel an e-mail provider to turn over some e-mail messages with a less-than-probable cause showing.[125] This was no hypothetical power, as the government had made sub-probable-cause requests for e-mail messages on many prior occasions.[126]

Theofel rejected that interpretation.[127] It essentially read out of the SCA an entire category of the statute, forcing the DOJ to get a probable cause warrant and nothing less to obtain any stored e-mail messages.[128] *Theofel*, virtually overnight, undid over twenty years of Justice Department expectations about the SCA, changing the ground rules for law enforcement access to stored e-mail messages from a d-order to a probable cause standard.[129]

At the time *Theofel* was issued, the smart money would have been to bet that the legislative offices of the Justice Department would have mobilized immediately. The DOJ had proved repeatedly that it would not sit idly by after adverse judicial opinions narrowed its electronic surveillance authorities. Less than a year after a single magistrate judge ruled that warrants under the SCA had to be served in person and not by

piece of e-mail and then left it on the e-mail provider's server, it no longer qualified as in "electronic storage," an important SCA term of art. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 122–27 (3d ed. 2009) [hereinafter CCIPS SEARCH-AND-SEIZURE MANUAL], *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf (defining "electronic storage"). Importantly, e-mail stored but not in electronic storage could be accessed by a d-order or subpoena. *Id.* at 127–34 (outlining the government's means of compelling disclosure).

125. *Id.*

126. *See, e.g.*, *id.* (including specific cases in its discussion of compelling disclosure with less than probable cause).

127. The case involved a civil suit about a discovery request for e-mail in a prior litigation gone very bad. *Theofel*, 359 F.3d at 1071–72. It was probably not until the Justice Department filed an amicus brief urging reconsideration that the panel realized that it was upsetting years of criminal law investigation practice. *Id.* at 1076. But even faced with the import of its decision, the panel did not waver, amending its opinion to reject the government's arguments in detail and reassuring the government that it did "not lightly conclude that the government's reading is erroneous." *Id.* at 1077.

128. In response to the DOJ's argument that *Theofel* would read out the part of the statute which allowed d-order and subpoena requests, Judge Kozinski explained that ISPs that provide only "storage or computer processing services" would still be amenable to process under the provision. *Id.* at 1076–77.

129. *See* CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 124, at 123–25 (discussing the effect of *Theofel* from the DOJ's perspective).

fax machine,[130] Congress, at the Justice Department's behest, amended the SCA to make it clear that service by fax was allowed.[131] When ISPs refused to honor warrants for e-mail issued by judges outside their districts, Congress amended the SCA to provide for nationwide service of process.[132] After a few appellate courts had ruled that stored voicemail messages were protected by stricter privacy controls than stored e-mail messages,[133] Congress weakened the protection of stored voicemail.[134]

In each of these past situations, the Justice Department had related its wishes not only privately in the offices of congressional members and staffers but also publicly in Senate and House hearing rooms. Many high-ranking Justice Department officials have spent some of their limited congressional testimony time pleading for tweaks like these to ECPA whenever they have been asked to testify about computer crime.[135]

Given this record, we would have expected the Justice Department to launch an aggressive campaign on Capitol Hill to overturn *Theofel*. If the DOJ had been willing to knock on legislators' doors to protect the right of FBI agents to use fax machines, how much more motivated must it have felt to overturn a ruling that required probable cause instead of d-orders to access e-mail, particularly because the Ninth Circuit sets the law for the jurisdictions in the western United States, which include most of the nation's largest e-mail providers such as Yahoo!, MSN Hotmail, and Google?[136] Of course, this assumes

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

131. 21st Century Department of Justice Appropriations Authorization Act, Pub. L. 107-273, § 11010, 116 Stat. 1812, 1822 (2002) (codified as amended at 18 U.S.C. § 2703(g) (2006)).

132. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, § 220, 115 Stat. 272, 291 (codified as amended at 18 U.S.C. §§ 2703, 2711, 3127 (2006)).

133. *E.g.*, United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998) (allowing suppression of voice mail under the Wiretap Act).

134. USA PATRIOT Act § 209.

135. *E.g.*, *Fighting Cyber Crime: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 107th Cong. 41–48 (2001) (statement of Associate Att'y Gen. Michael Chertoff) (mentioning problems with the Pen Register Act and the Cable Act); *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 4–20 (2000) (statement of Deputy Assistant Att'y Gen. Kevin V. Di Gregory) (asking for changes to ECPA).

136. United States Court of Appeals for the Ninth Circuit, Map of the

there is a meaningful difference between the d-order standard and probable cause.

But the expected bang has not even been a whimper. No Justice Department official has ever mentioned *Theofel* in public testimony. No legislation has ever been introduced which would overturn *Theofel*. A search of the entire DOJ website for references to *Theofel* returns only four hits, most notably entries in two recent manuals.[137] In the first manual, on prosecuting computer crime, the Justice Department's Computer Crime and Intellectual Property Section (CCIPS) meekly protests that it "continues to question whether *Theofel* was correctly decided."[138] In the second manual, the so-called search-and-seizure manual, CCIPS puts up a more spirited critique of *Theofel* but ultimately seems resigned to its continued applicability in the Ninth Circuit.[139]

The Justice Department has long argued that forcing high justification standards in Internet investigations would keep critical evidence away from the police, allowing criminals to take advantage of the efficiencies of the Internet without allowing the police to respond in kind.[140] But the timid response to *Theofel* suggests the opposite. It suggests that the FBI has found a way to solve crimes even with "tighter" standards. Perhaps they have learned to turn to other investigative techniques, maybe doing things like staking out homes and digging through garbage when they once would have requested e-mail instead.

Much more likely, the *Theofel* revolution was not even a mild uprising because whenever the police have any suspicion in an online case, they have probable cause. It seems likely that

Ninth Circuit, http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000135 (last visited Apr. 12, 2010).

137. COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 90 (2007) [hereinafter CCIPS PROSECUTING COMPUTER CRIMES], *available at* http://www.usdoj.gov/criminal/cybercrime/ccmanual/ccmanual.pdf; CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 124, at 123–25.

138. CCIPS PROSECUTING COMPUTER CRIMES, *supra* note 137, at 81. I worked for the Computer Crime and Intellectual Property Section when *Theofel* was decided. This discussion, however, rests only on the public record and my personal interpretations of events.

139. CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 124, at 125 ("[P]rosecutors within the Ninth Circuit are bound by *Theofel* . . . .").

140. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1067–77 (9th Cir. 2004) (discussing the government's arguments aimed at maintaining lower justification standards).

the only difference between pre-*Theofel* and post-*Theofel* practice has been more agent time spent at the word processor because a search warrant requires a bit more paperwork than a d-order. It appears that not only has the new rule in *Theofel* never derailed an entire case—for surely we would have heard all about it—but also perhaps *Theofel* has not even changed any investigative tactics.

More broadly, the Justice Department's legislative inaction strongly suggests that the difference between probable cause and reasonable suspicion is not all that it has been cracked up to be. This is true even if the Justice Department suddenly decides to try to amend ECPA to overturn *Theofel*, perhaps after reading this Article, as we will have learned plenty from more than five years of inattention.

C. EXCEPTIONS

As I have said, I am not claiming to have uncovered a universal truth about the Internet or online crime investigation; I have not unearthed a structural barrier to making a hunch online. With just a bit of creativity, one can construct hypothetical after hypothetical that could conceivably arise in which the government would want electronic evidence from a provider despite having less than probable cause. A close scrutiny of these hypothetical cases, however, demonstrates why they are probably unusual examples, possible in the abstract but unlikely to happen frequently. We should not get too hung up considering these cases, unless evidence suggests that one category is likely to happen or has happened in the past repeatedly. These hypotheticals fall into three categories.

1. Fishing Expeditions

First, the police might engage in a fishing expedition, which I define as a request based on no suspicion whatsoever. In a fishing expedition, the police seek evidence on a lark, casting about aimlessly, hoping to crack a case with a lucky break. Those who worry most about the SCA's below-probable-cause standard seem to worry most about government fishing expeditions.[141]

141. Posting of Nicole Wong, Associate General Counsel, Google, Inc., to Official Google Blog, http://googleblog.blogspot.com/2006/02/response-to-doj-motion.html (Feb. 17, 2006, 15:55 PST) (asserting that the government requested "untold millions of search queries" which would "do nothing to further the Government's case in the underlying action").

As an example, when the government asks an online intermediary to troll its database of information about users looking for particular characteristics of completed crime, or even worse, characteristics of inchoate crime or potential crime, this behavior tends to fall outside the structural explanations listed in Part II.

It cannot be denied that the police sometimes engage in fishing expeditions. Every so often, the government has sent wildly overbroad requests to Internet service providers. For example, the Civil Division of the Department of Justice has been engaged in civil litigation for several years seeking to defend the constitutionality of the Children's Online Protection Act (COPA).[142] As part of the case, in 2005, Justice Department lawyers sent subpoenas to several prominent search engine companies including Google, Microsoft, America Online, and Yahoo!, seeking two months' worth of user search queries to be used by government experts to estimate the spread of materials harmful to minors and to analyze the spread of filtering software.[143] While most search engines complied, Google resisted, prompting a Justice Department motion to compel.[144]

Google and other critics saw this as an abuse of the subpoena power and a possible violation of the SCA.[145] It seemed to confirm the worst conspiracy theories about the Government's disrespect for online privacy.

But the Google subpoena was idiosyncratic, surely not an example of a broader trend. Not only were the Justice Department officials not seeking evidence to admit in a criminal case, they were not seeking evidence for any case at all. The data were being requested for what essentially amounted to an academic study, albeit one useful to defending the constitutionality of COPA.[146] Although the Justice Department might have had a legal theory for why it was entitled to the data, particularly

142. 47 U.S.C. § 231 (2006).

143. *See* Hiawatha Bray, *Google Faces Order To Give Up Records*, BOSTON GLOBE, Mar. 15, 2006, at E1 (discussing the government's requests of major search engine companies in an effort to defend the COPA).

144. *See* Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1 (discussing the motion to compel).

145. *See, e.g.*, Posting of Nicole Wong, *supra* note 141 (responding to the government's motion to compel).

146. *See* Hafner & Richtel, *supra* note 144 ("[The government] is trying to establish a profile of Internet use that will help it defend the Child Online Protection Act . . . .").

given the broad interpretation given the subpoena power, prudentially and as a matter of public relations this was a disastrous and foolhardy decision. In the end, U.S. District Judge Ware ordered Google to produce a small subset of the information requested and Google complied without appeal.[147]

Even in criminal cases, sometimes the police try fishing in the deep pools of ISP logfiles. In early 2009, the FBI served a subpoena on an ISP called IndyMedia, asking the provider to record the IP address of every user who had visited an IndyMedia-hosted website.[148] After the ISP resisted the subpoena, with help from the Electronic Frontier Foundation, the government withdrew its request.[149]

Although they sometimes happen, fishing expeditions are not the exception that swallows the rule for two reasons. First, the survey of case law in Part II.B.1 suggests that fishing expeditions are rare, because no court has ever found a lack of probable cause in a case involving a request to an ISP for records (although the IndyMedia case might have been the first, had it been fully litigated). Second, since fishing expeditions are by definition built upon no suspicion whatsoever, they do not contradict my fundamental claim: when police investigate crime online they tend to have probable cause or no suspicion at all. Concerns about fishing expeditions cannot for this reason be used to argue that reasonable suspicion standards in the SCA should be raised to probable cause standards, for example. It would be odd to claim that a request based on reasonable suspicion is also a fishing expedition.

Still, we should try to structure our laws to prevent fishing expeditions and to detect them when they occur. In Part IV, I will propose a few small tweaks to ECPA to accomplish both goals.

2. Cases Touching the Real World

The second category of potential cases involving requests to ISPs from law enforcement officials not having probable cause

147. *See* Verne Kopytoff, *Google Must Divulge Data*, S.F. CHRON., Mar. 18, 2006, at C1 ("The 21-page opinion by Judge James Ware . . . puts to bed a high-profile legal battle between the most popular search engine and the Department of Justice . . . .").

148. *See* Electronic Frontier Foundation, From EFF's Secret Files: Anatomy of a Bogus Subpoena, http://www.eff.org/wp/anatomy-bogus-subpoena-indymedia (last visited Apr. 12, 2010) (reporting on the contents of the subpoena).

149. *Id.*

are cases that straddle the virtual and real worlds. Sometimes, evidence found in the real world points to the online world and sometimes evidence found online points to the real world.[150] Each situation might place an e-mail address, in particular, into a police officer's hand without giving him the context for probable cause. Consider each case in turn.

First, police officers may find Internet addresses in the real world. For example, they may find e-mail addresses scribbled in little black books.[151] When the police focus on an e-mail address only because it is associated with a suspicious person, rather than because it is stamped to the top of an incriminating e-mail, the factors that tend to give the police probable cause online may not apply at all.[152] In particular, the "rich contextualization" factor disappears in these straddling situations.[153]

Imagine, for example, that agents lawfully search and seize the smartphone of a suspected drug kingpin. The agents analyzing the device are likely to be keenly interested in the address books, the "contacts" database in the phone application and the "address book" in the e-mail application. If the agents want to request more information about the people listed in those address books, they are likely to have some suspicion, but less than probable cause, to support those requests.

Second, consider the rarer case of online evidence that points to the real world. Increasingly, the police have turned to one such type of online evidence: cell-site location data.[154] For years, mobile phone providers have kept records indicating the wireless towers used by each phone customer.[155] Because mobile phones tend to communicate with towers in closest geographic proximity, this information can be used "to track a

150. *E.g.*, United States v. Gourde, 440 F.3d 1060, 1067–68 (9th Cir. 2004) (en banc) (describing how information found online about defendant's subscription to a child pornography website led the FBI to real evidence in his home).

151. Cell phone contact lists and webmail address books are replacing the traditional "little black books." Do not be confused by the fact that the storage mechanism is electronic or online. I still put this in the category of a "real world" storage device pointing to online addresses.

152. Compare with *Gourde*, 440 F.3d at 1067–68, where the FBI had defendant's e-mail address accompanied by evidence he maintained a membership to a child pornography website.

153. *See supra* Part II.A.3.a.

154. *See* Anne Barnard, *Growing Presence in the Courtroom: Cellphone Data as Witness*, N.Y. TIMES, July 6, 2009, at A16 (discussing the role cell phone tracking now plays in law enforcement investigations).

155. *Id.*

phone's location to within a radius of about two-hundred yards in urban areas and up to twenty miles in rural areas."[156] More recently, the police have tried to take advantage of these capabilities, either requesting records of past location or asking a provider to track location in real time.[157]

The government's use of cell-site location data has spurred a lot of recent litigation[158] because cell-site location tracking fits awkwardly into ECPA.[159] These cases raise a fairly technical set of ECPA issues not important here.[160] More interesting, however, is whether the police tend to have probable cause in these cases. Unfortunately, we know almost nothing about the underlying facts of these cases, since they are brought as ex parte applications involving ongoing criminal investigations. From popular reporting, these cases tend to fall in three categories: kidnapping, fugitive tracking, and drug distribution investigations.[161] One imagines that every request made during a kidnapping or while tracking a fugitive meets probable cause. Tracking drug dealers is different, however, as any viewer of the television show *The Wire* can attest. One imagines the DEA quite often would like to know where their suspected drug kingpin is traveling, even when it lacks probable cause.

Evidence like this that straddles two worlds provides an exception to my argument but does not swallow it for several reasons. First, unlike e-mail addresses, we never find IP addresses and almost never find domain names or URLs in the real world, especially not as evidence of crime. Second, although we sometimes find e-mail addresses in the real world, much more often e-mail addresses serve as evidence of a crime because they are attached to facially incriminating e-mail mes-

156. *Id.*

157. *See id.* (reporting that "wireless carriers receive hundreds of requests a month from law enforcement just for real-time tracking," according to lawyer Albert Gidari Jr.).

158. *See* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1416 n.17 (2007) (listing cases).

159. *See id.* at 1415–17 (describing the DOJ's record in cases involving ECPA).

160. *See id.* at 1418–56 (chronicling these issues).

161. *See e.g.*, Barnard, *supra* note 154 (noting the use of finding kidnappers, fugitives, and drug traffickers); Ryan Singel, *FBI E-Mail Shows Rift Over Warrantless Phone Record Grabs*, WIRED, Dec. 20, 2007, http://www.wired.com/print/politics/onlinerights/news/2007/12/fbi_cell (explaining how cell phone tracking works and is used).

sages which provide enough context for probable cause.[162] Third, although cell-site location information appears to be an increasingly important form of surveillance,[163] it is probably dwarfed by the amount of traditional communications surveillance that is the central topic of this Article.

3. Preventing Future Crimes

Finally, sometimes agents will want to work much more speculatively to try to prevent future crimes not yet completed and not even in progress. In those cases, given both the exigencies and speculativeness of the investigation, they may want to request information from ISPs based on less than probable cause.

Often, these investigations swirl around national security. Daniel Solove notes that, "national security surveillance is often not aimed at finding out about who perpetrated past crimes; it is often prospective, designed to glean information about future threats."[164] After 9/11, the Bush Administration's national security agencies began monitoring multiple communications and transaction networks, looking for patterns of future terrorist attacks. For example, the government began wiretapping telephone and Internet communications,[165] monitoring banking transactions,[166] and collecting records reporting citizens' telephone calling records.[167] By design, these investigations have nothing to do with individualized suspicion.[168] Not only do the investigators lack probable cause of evidence of a crime, they probably lack even mere relevance. If these pro-

162. *See* Solove, *supra* note 47, at 1287 (discussing how applying electronic surveillance to IP addresses and URLs makes things "fuzzy").

163. *Compare* Christopher Soghoian, Slight Paranoia, 8 Million Reasons for Real Surveillance Oversight, (Dec. 1, 2009, 7:00 AM), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (reporting eight million requests for GPS location information) (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel), *with* Comment of Matt Sullivan, Sprint Nextel, to *id.*, (Dec. 1, 2009, 23:26) (clarifying that the eight million requests amount to only "[s]everal thousand" instances of surveillance).

164. Solove, *supra* note 47, at 1301.

165. *See* James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, at A1.

166. Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A1.

167. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A.

168. *See id.* (explaining that most of the information comes from people not suspected of crimes).

grams are to be justified, it will not be by manipulating justification standards. It will instead be by recognizing that they are different situations that deserve different approvals under the national security laws.

4. An Example Involving All Three Exceptions: Data Mining

One particularly important government surveillance activity falls outside my predictions about probable cause: data mining. Data mining embodies each of the three exceptions presented above, for it describes fishing expeditions of data in the real world to try to predict future crime. For this reason, data mining often occurs with much less than probable cause, and many legal scholars have defended this practice,[169] although others have criticized it.[170] It thus might be tempting to point to data mining as the exception that swallows my rule, the example of regularly occurring government surveillance that almost never happens with probable cause.

I disagree. Data mining does not swallow the rule in this case, because as these same scholars have noted, data mining is almost entirely unregulated under current law today.[171] Current privacy law focuses almost entirely on how the government collects data, not how it uses data it lawfully already possesses.[172] In most cases, no law sets a justification standard—not probable cause, reasonable suspicion, or even mere relevance—before the government can begin data mining.[173] We

169. *See* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 96–97 (2006) (arguing that data mining does not implicate privacy at all unless a human looks at the results); Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 487–88 (2008) (endorsing a nine-pronged framework for regulating data mining with no mention of judicial standards); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 337–38 (2008) (arguing for a non-probable cause standard for some types of data mining).

170. *E.g.*, Posting of Jim Harper to Cato@Liberty, Data Mining of the Fourth Amendment?, http://www.cato-at-liberty.org/2006/08/22/data-mining-or-the-fourth-amendment/ (Aug. 22, 2006, 12:36 PM).

171. *See, e.g.*, Slobogin, *supra* note 169, at 330 ("Since virtually all information obtained through data mining comes from third-party record holders—either the government itself, commercial data brokers, or a commercial entity like a bank—its acquisition does not implicate the Fourth Amendment.").

172. *See* Kerr, *supra* note 35, at 1218–22 (discussing the disclosure requirements under the SCA).

173. The only federal law that specifically regulates data mining is the Computer Matching and Privacy Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a(o)–(r) (2006)). The law is mostly

should regulate data mining more, but whether we should and how we should falls outside the scope of this discussion. The police tend to have probable cause whenever they seek data from online Internet providers. Whether they have probable cause whenever they mine data they already possess is another question entirely.

III. REFORMING ECPA

What should we make of this observation, that the old categories of police justification collapse into two levels—nothing and probable cause—in online investigations? This Part seeks to use this observation to restructure our online surveillance debates. In such debates, advocates on every side and across the political spectrum pour energy into squabbles over where to set justification standards in surveillance statutes like the Pen Register Act and SCA. These fights take place in courtrooms, law review pages, policy debates, and most crucially, in the halls of Congress. Nobody engaged in these struggles has yet appreciated the sheer inconsequence of what he or she is arguing about. Who cares who wins or loses when either outcome will look just like the other? Because the police almost always have probable cause at every stage of every online investigation, whether we set a requirement at relevance, reasonable suspicion, or probable cause, the police will take every action at exactly the same time.

In place of the fight over justification standards, we should look for other ways to accomplish what justification standards do not: balance police need against the privacy of the citizenry. To achieve this balance, we should look to other underappreciated mechanisms, such as judicial review, statutory suppression, notice, reporting, and necessity.

A. THE IRRELEVANCE OF ECPA'S JUSTIFICATION STANDARDS

Whenever Congress is asked to set a justification standard at a particular level—probable cause, reasonable suspicion, or mere relevance—it should not waste too much time on the choice, because the choice is almost inconsequential. Instead, it should simply set the standard at whatever level is politically most expedient and turn its attention to other questions.

inapposite to this discussion because it imposes no justification standards and it expressly exempts data mining for law enforcement and intelligence purposes. 5 U.S.C. § 552a(a)(8)(B)(iii), (v)–(vi).

Interestingly, the observation that the Internet is hunch-free may be politically neutral, because either side in the debate can use it to its own advantage. On the one hand, the Justice Department might argue that because a change in the SCA, for example, from reasonable suspicion to probable cause will matter little, Congress has no reason to shift away from the status quo. On the other hand, privacy advocates asking for such a change can argue that the change should be seen only as a minor tweak, because it will not alter many outcomes and certainly will not lead to any dire consequences.

Although Congress should spend little time considering justification standards, it might want to spend enough time to address one of the exceptions to the hunch-free Internet theory: fishing expeditions. As documented above,[174] the government has engaged occasionally in fishing expeditions, albeit probably very infrequently. If Congress would like to stamp out the possibility of fishing expeditions in online investigations, it should consider removing the mere relevance standard (which most often takes the form of a subpoena standard) from the SCA and Pen Register Act. Christopher Slobogin calls the subpoena power "almost entirely unrestricted" by the Constitution.[175] William Stuntz calls the subpoena power "something akin to a blank check."[176] Although Google often boasts about how it resisted the government's fishing expedition subpoena, it almost always glosses over the fact that it ended up partly losing that case: the judge ruled against Google, in part, and ordered it to turn over thousands of users' search queries.[177] Given the way the subpoena standard has been interpreted, the loss is not surprising.

Congress can and should stamp out fishing expeditions by removing from the SCA any rule permitting government access to content or noncontent with less than a d-order standard.[178] Likewise, Congress should amend the Pen Register Act to require at least reasonable suspicion, not mere relevance as allowed now.[179] Although these changes are important, the fact

174. *See supra* Part II.C.1.

175. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 809 (2005).

176. William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001).

177. *See* Bray, *supra* note 143.

178. The SCA permits access to some records with a subpoena. 18 U.S.C. § 2703(b)(1)(B)(i), (c)(2) (2006).

179. *Id.* § 3123(a)(1)–(2).

that fishing expeditions happen so infrequently suggests that Congress should consider giving lower priority to these changes (which are sure to invite a fight from the Justice Department) than to the other changes proposed next.

B. HOW CONGRESS SHOULD AMEND ECPA

The endless debates over justification standards thus distract us from what we ultimately really care about—how to balance police need with respect for online privacy. Rather than pour so much energy into trying to change the law to force the police to obey a higher standard, we should learn the lesson of *Theofel*[180]: even if we force the police to act only with probable cause, the change will have little effect on investigations and thus little added benefit for privacy.[181] The same information from the same accounts belonging to the same people will be delivered to the police at the same time.

My goal in this Article has been mostly descriptive. I seek to shift the focus of the debates away from justification standards. If I succeed, however, it invites the inevitable response—what should we be focusing on instead? In other words, what are my normative and prescriptive recommendations for reforming ECPA?

Space does not permit me to provide a full account of my normative and prescriptive goals, but I will provide a sketch. As a threshold matter, I agree with essentially everybody who has ever written about ECPA that the law is sorely in need of reform.[182] First, ECPA is confusing; epically confusing; grand-champion-of-the-U.S. Code confusing.[183] This is not just an aesthetic complaint, because ECPA's complexities confuse judges who then make a mess of our understanding of the Act. To point to only one of the worst offenders, the courts trying to make sense of the line between the SCA and the Wiretap Act

180. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076–77 (9th Cir. 2004).

181. *See* Slobogin, *supra* note 175, at 840 (stating that information obtained through subpoenas is usually secondary information).

182. *See* Symposium, *The Future of Internet Surveillance Law: A Symposium To Discuss Internet Surveillance, Privacy, and the USA Patriot Act*, 72 GEO. WASH. L. REV. 1139 (2004). Every author who expressed an opinion about ECPA recommended changing it in fairly significant ways.

183. *See* Posting of Paul Ohm to Concurring Opinions, Which is More Confusing: ECPA or the Tax Code?, http://www.concurringopinions.com/archives/2008/08/which_is_more_c_1.html (Aug. 21, 2008, 12:42 PM).

have ended up producing a messy, counterintuitive doctrine.[184] If nothing else, ECPA should be greatly simplified.[185]

But simplification is not enough. ECPA does a very poor job balancing security and privacy, which is to say, it does a poor job doing the only thing it is supposed to do. This is in part due to the reason revealed in this Article: ECPA seeks balance through the fine calibration of justification standards, so ECPA creates the illusion of calibration but instead delivers monolithic protection.

My primary prescription is that we should more frequently use mechanisms other than justification standards in statutes like ECPA to balance privacy and security. There are many such mechanisms, some which have been raised in past debates, but many which have been ignored almost entirely. Unlike justification standards, these mechanisms will truly alter police behavior. These are the mechanisms civil liberties groups should be offering, perhaps even trading them for lowered justification standards. At the very least, every part of ECPA—the Wiretap Act, the SCA, and the Pen Register Act—should provide for some form of each of the following.

(1) *Judicial Review*. The most important way to change police behavior is to subject their actions to meaningful judicial scrutiny. An officer is likely to be more careful and thorough when he knows his words will be scrutinized by a judge than when he works without such oversight. Justice Douglas explained that the value of interposing a judge into the search warrant process was "so that an objective mind might weigh the need to invade that privacy in order to enforce the law."[186]

Judicial review is such a powerful antidote to police abuse, in fact, that it can help trump concerns about lower justification standards. For example, many commentators have expressed concern about the relevance-and-certification standard of the Pen Register Act.[187] Many critics decry this standard,

184. *See, e.g.*, United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (en banc) (interpreting the Wiretap Act); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 886 (9th Cir. 2002) (affirming the dismissal of a Wiretap Act claim, but reversing the dismissal of a Stored Communications Act claim).

185. *See* Kerr, *supra* note 35, at 1235–38 (urging Congress to simplify ECPA).

186. McDonald v. United States, 335 U.S. 451, 455 (1948).

187. *See* 18 U.S.C. § 3121 (2006) (defining the relevance-and-certification standard).

declaring it nothing but a rubber stamp on government investigations.[188]

I too worry about the Pen Register Act's lax rule. By letting an agent do nothing but "certify" the required statement,[189] the Act does not force an agent to divulge anything about the case or the surveillance, which minimizes the role of the reviewing judge.[190] Unlike affidavits for search warrants or wiretap orders, pen register affidavits are very terse documents. If the Act instead required, as the SCA does, "specific and articulable facts,"[191] this would be a huge step forward for meaningful judicial scrutiny in the binary, feast-or-famine context of online investigations.[192]

(2) *Notice*. Another important principle is notice to the user and an opportunity to object. This is the principle that the three-judge panel in *Warshak* worried most about.[193] Although the SCA requires notice when a subpoena or court order is used to obtain stored e-mail, it also provides the right to delay this notice in many cases.[194] Congress should tighten the permissible reasons for delay and add notice requirements where they do not already exist.[195]

(3) *Reporting*. Under the Wiretap Act, the Administrative Office of the U.S. Courts must prepare an annual report summarizing for each approved wiretap, among other things, the offense under investigation and the number of arrests, trials, and convictions that resulted.[196] The reports provide an illuminating window into the reach and efficacy of police wiretaps. Although the SCA and Pen Register Act require some report-

188. *See* Solove, *supra* note 47, at 1288–89.

189. *Id.* at 1288.

190. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (calling the judge's role in reviewing Pen Register Act applications "ministerial in nature").

191. 18 U.S.C. § 2703(d) (2006).

192. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 639 (2003) (explaining that the higher standard would add privacy protection).

193. *See* Warshak v. United States, 490 F.3d 455, 467 (6th Cir. 2007) (upholding an injunction for lack of a warrant or notice), *rev'd as not ripe by* 532 F.3d 521, 522 (6th Cir. 2008) (en banc).

194. *See* 18 U.S.C. § 2705(a)(1)–(2) (listing five factors justifying delay including physical safety, possible flight, evidence tampering, and witness intimidation).

195. Notice to the subscriber is not required in parts of the SCA, *id.* § 2703(b)(1)(A), (c)(1), or in the Pen Register Act, *id.* § 3123(d).

196. *Id.* § 2519(3).

ing,[197] neither requires the level of reporting of the Wiretap Act,[198] and both should.

(4) *Suppression*. Professor Kerr has argued at great length that Congress should provide a suppression remedy to all of the electronic surveillance statutes.[199] Despite his calls for this statutory change, nobody has proposed such a change in recent legislative sessions.

(5) *Necessity*. Finally, Congress should consider adding so-called necessity requirements to the Pen Register Act and SCA. The Wiretap Act already requires "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[200] In other words, given the especially invasive nature of a wiretap, the police must turn to it only as a last resort.

But necessity requirements need not be so all-or-nothing. Congress should consider adding *tiered necessity* requirements to every part of ECPA, ranking different investigative techniques into tiers by level of invasiveness and prohibiting the use of techniques in any tier until all of the techniques in all of the "less invasive" tiers have been either tried or rejected as too likely to fail or too dangerous. One can imagine, for example, a new rule that places very invasive techniques like wiretapping and the government's use of spyware[201] into the most invasive Tier *A*, access to stored e-mail content and cell-site location in a less invasive Tier *B*, and pen register and noncontent records access in the least invasive Tier *C*. Under this tiered necessity regime, the police could not access, for example, stored e-mail content (Tier *B*) until they first tried a pen register (Tier *C*) on the e-mail account.

197. *See id.* §§ 2702(d), 3126.

198. *See id.* § 2519 (describing the reporting requirements for wiretaps).

199. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 837–40 (2003).

200. 18 U.S.C. § 2518(1)(c).

201. *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 (describing the FBI's use of spyware in its law enforcement efforts).

IV. SHIFTING THE FOCUS OF THE FOURTH AMENDMENT

The recognition that the Internet is a hunch-free zone should spur more than just a new approach to ECPA reform; it should much more broadly change how we balance privacy and security through law. Most importantly, it should shift the focus of Fourth Amendment search-and-seizure law, which has always treated probable cause as the principle tool for balancing privacy and security.[202] The rise of widely used, richly intermediated, new technologies of communication challenges the underpinnings of this approach.

This is not only a story about the Internet, either, because intermediation will become an even more important, more pervasive force in the near future. First, the Internet will soon be available everywhere, as millions of people each year trade in their ordinary cell phones for smart phones like the iPhone, bringing intermediated communications to the street. Second, everyday objects now communicate wirelessly through intermediated networks, giving the police new ways to track us: cars come with GPS tracking devices and hidden microphones; toll payment transponders track our movement down a highway; and many other objects embed secret wirelessly communicating RFID chips to speed consumer transactions. Jerry Kang has described this as "ubiquitous access" or "pervasive computing."[203]

The intermediaries that offer pervasive computing possess most of the attributes that make the Internet a hunch-free zone: they deploy systems of perfect surveillance that memorialize precise, contextualized leads in an unbiased way. We should thus expect the police to be able to meet higher levels of justification more often in the near future. Over time, the probable cause standard, the Fourth Amendment's great bulwark of privacy, will no longer serve as an effective barrier to police action.

There are two ways to interpret the incipient decline of the probable cause standard, one optimistic, one pessimistic. The optimist sees this as the triumph of the Founders' Fourth Amendment. The Founders were willing to cede power to the government and pierce the privacy of the citizenry when the po-

202. *See* Kerr, *supra* note 69, at 574.

203. *See, e.g.*, Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 65 WASH. & LEE L. REV. 93, 93 (2005) (describing the ideas of pervasive computing and ubiquitous access).

lice had sufficient suspicion,[204] and thanks to the wonders of modern technology and the increased intermediation of private life, we no longer need to worry about the police responding to hunches and whims, because technology assures confidence and justification. This is bad news for criminals, to be sure, but it means the innocent among us can worry a lot less about groundless, suspicionless surveillance.[205]

The pessimist focuses instead on the spread of surveillance in society. Probable cause will matter less than it once did only because we are all being watched more closely and more often than we ever have been. Intermediaries track our behavior in ways that once went untracked.

I am convinced by the pessimist's and not the optimist's story. As many other scholars have noted, Internet intermediaries watch and memorialize what we read, say, do, and even think in novel and unprecedented ways.[206] As only one example, consider the Facebook status update. Although people use status updates for many purposes, from the silly to the profound, most of the time they use them as a substitute for the stray utterances they used to say on the telephone or by the water cooler, utterances that once floated through the air and then disappeared without a trace. Today, not only are these utterances stored, but also they are accessible by a company that is not a party to the conversations.

The pessimist's interpretation of the decline of probable cause serves as a counterargument to Professor Orin Kerr's defense of the Fourth Amendment's third-party doctrine,[207] the rule that the Fourth Amendment does not apply at all to bank records[208] or records of telephone numbers dialed[209] when held by a third-party intermediary. Professor Kerr sits virtually alone in the legal academy in defense of the third-party doctrine, arguing that it prevents an "end-run around the tradi-

204. *See* U.S. CONST. amend IV.

205. This last point is another example of the well-worn "I have nothing to hide" argument, which Daniel Solove refutes. *See* Daniel J. Solove, *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 764–72 (2007).

206. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006) (stating that Fourth Amendment law fails to protect against some breaches).

207. *See* Kerr, *supra*, note 69, at 587–600.

208. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

209. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1976).

tional Fourth Amendment balance"[210] between security and privacy which results when criminals use new telecommunications technologies to plan and execute crimes in private that they once would have needed to commit in the open.[211] According to Professor Kerr, "[w]ithout the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection."[212]

A problem with this approach is that Professor Kerr focuses only on one side of the ledger, on how communications technologies have made committing crime easier. He neglects almost entirely to mention how, as this Article describes, intermediated communications technologies empower the police.[213] Although criminal co-conspirators can use Facebook to plot crimes away from the public's eye, these conversations are stored in a permanent archive, waiting for the police to come along, where once they would have disappeared.

Professor Kerr argues that because communications networks provide new methods of evasion to criminals, they justify exceptions to the Fourth Amendment's privacy protections; specifically they justify the third-party doctrine.[214] I come to almost the opposite conclusion: because communications networks make it easier for the police to track crime, we should strengthen the Fourth Amendment's privacy protections, by shifting away from justification standards toward other mechanisms for balancing privacy and security—the same types of prescriptions I offered for ECPA reform.

In essence, I am arguing for more *Berger*[215] and less *Katz*[216] in Fourth Amendment jurisprudence. When scholars talk about

210. Kerr, *supra* note 69, at 564.

211. *See id.* at 575.

212. *Id.* at 576.

213. I have other problems with Professor Kerr's argument. Most significantly, I find the approach impossible for courts to apply, because it is positively actuarial: it asks courts to construct a balance sheet measuring how changes in technology upend the constitutionally proper balance between privacy and security. When the balance sheet tips too much in favor of privacy at the cost of security, it allows courts to construct rules to restore balance. This bean-counting approach is too indeterminate to serve the purpose Professor Kerr intends, because it requires courts to quantify changes in technology and crime in ways that courts are ill-equipped to do.

214. *See id.* at 575–76 (discussing the effects of intermediaries on criminal conduct).

215. *See* Berger v. New York, 388 U.S. 41, 43–44 (1967) (striking down a New York surveillance law as too general).

the Fourth Amendment and the Internet, they focus a great deal of attention on the reasonable expectation of privacy test from *Katz v. United States*.[217] They see this as the critical fulcrum upon which the Fourth Amendment's privacy guarantees pivot; when conduct satisfies the *Katz* test, it becomes protected by the probable cause standard, the highest standard of constitutional protection.

But as this Article demonstrates, reasonable expectations of privacy and the probable cause standard are not enough to ensure a sound balance between privacy and security in the face of widespread intermediation. Scholars should shift some focus away from *Katz* to *Berger v. New York*, decided a few months earlier. In *Berger*, the Court invalidated New York's eavesdropping statute as too permissive under the Fourth Amendment.[218] Although the statute allowed eavesdropping orders only from a "neutral and detached" judge,[219] the Court found it had a "heavier responsibility"[220] to impose procedural protections for eavesdropping and wiretapping because they are so "broad in scope."[221]

The Court faulted the New York statute for permitting "indiscriminate use" of eavesdropping rather than providing "precise and discriminate requirements" to "carefully circumscribe[] invasions to privacy."[222] Specifically, the court required eavesdropping and wiretapping statutes to require the police to specify with particularity the crime under investigation and the conversations sought; authorize surveillance for limited periods of time; and provide some notice to the person surveilled or delay based on exigent circumstances.[223] It is not a coincidence

216. *See* Katz v. United States, 389 U.S. 347, 350 (1967) (refusing to recognize the Fourth Amendment as granting a general privacy right).

217. *See, e.g.*, Slobogin, *supra* note 39, at 153 (analogizing the assumption of risk that the phone company will disclose information to information gained by ISPs); Solove, *supra* note 47, at 1287 (discussing the expansion of information obtainable by the government resulting from the USA PATRIOT Act); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2114–15 (2009) (discussing the right to privacy in Internet communications).

218. *See Berger*, 388 U.S. at 64.

219. *Id.* at 54–55.

220. *Id.* at 56 (citing Osborn v. United States, 385 U.S. 323, 329 n.2 (1966)).

221. *Id.*

222. *Id.* at 58 (citations omitted).

223. *See id.* at 58–59.

that the list I propose for ECPA in Part III echoes many of the *Berger* requirements.

Given the spread of intermediation and the related decline in the importance of probable cause, courts should incorporate more *Berger*-like protections into Fourth Amendment doctrine. Susan Freiwald has made a similar suggestion.[224] Freiwald has urged courts to abandon the *Katz* reasonable expectation of privacy test for modern communications technologies.[225] In its place, she advocates a test she derives from *Berger* and also from cases in which courts of appeals have adopted *Berger*-like requirements when the police install silent video cameras in private places.[226] Under her test, whenever the police want to perform "hidden, intrusive, indiscriminate, and continuous" surveillance,[227] they must satisfy additional *Berger*-like protections.[228] Because these four factors are satisfied for stored e-mail, she argues that the police should meet the four requirements found in the video surveillance cases[229]: necessity, particularity, limited time, and minimization.[230] This is a promising approach.

CONCLUSION

On the Internet, the Constitution and other privacy laws promise to provide a balance they cannot deliver because they use the wrong mechanisms. These laws weigh police need against justification standards developed on the sidewalk that translate poorly to the Internet. Given the Internet's richly contextualized, intermediated, data-rich, perfectly surveilled architecture, the police online always have feast—probable cause—or famine—no lead at all—but almost never anything in between. This observation pushes against a widely held faith in the ability of justification standards to mediate the line between the need to fight crime and the desire for individual pri-

224. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 12, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

225. *See id.* ¶ 9.

226. *See id.* ¶¶ 51–56. Friewald cites seven silent video opinions from the Courts of Appeals. *Id.* ¶ 10 n.20.

227. *Id.* ¶ 10.

228. *See id.*

229. *See id.* ¶ 72.

230. *See id.* ¶ 54. She also would apply these requirements to real-time interception of e-mail and instant messaging and, perhaps, to surveillance of noncontent information as well. *See id.* ¶ 73.

vacy from the state. This Article urges everyone involved in debates over criminal procedure to begin focusing on other things—particularity, judicial review, notice, suppression, minimization, and necessity—that are far more likely to achieve the balance we seek.