Volume 62, Issue 4 Page 1005

Stanford Law Review

APPLYING THE FOURTH AMENDMENT TO THE INTERNET: A GENERAL APPROACH

Orin S. Kerr

APPLYING THE FOURTH AMENDMENT TO THE INTERNET: A GENERAL APPROACH

Orin S. Kerr*

This Article offers a general framework for applying the Fourth Amendment to the Internet. It assumes that courts will seek a technology-neutral translation of Fourth Amendment principles from physical space to cyberspace, and it considers what new distinctions in the online setting can reflect the function of Fourth Amendment protections designed for the physical world. It reaches two major conclusions. First, the traditional physical distinction between inside and outside should be replaced with the online distinction between content and non-content information. Second, courts should require a search warrant that is particularized to individuals rather than Internet accounts to collect the contents of protected Internet communications. These two principles point the way to a technology-neutral translation of the Fourth Amendment from physical space to cyberspace.

* Professor, George Washington University Law School. Thanks to Greg Lastowka, Michael Birnhack, Don Dripps, Yale Kamisar, Larry Alexander, Amy Wax, Chris Yoo, Stephanos Bibas, Shaun Martin, Leo Katz, Susan Bandes, Melanie Wilson, Katherine Strandburg, Matthew Tokson, Jonathan Bond, Kevin Bankston, Joel Reidenberg, James Grimmelmann, Herb Lin, Felix Wu, Deven Desai, and the faculties of the University of Pennsylvania, University of San Diego, Temple Law School, Rutgers-Camden, DePaul, and the University of Kansas for their very helpful comments.

INTRODUCTION

The Internet has become an essential part of daily life for millions of Americans. Unfortunately, the many benefits of the Internet have been accompanied by increasing use of the Internet to commit crimes. Use of the Internet for criminal activity poses important new questions for the law of criminal investigations. How should the Fourth Amendment apply to the Internet? What kinds of online surveillance should the Constitution permit? When should the government be allowed to monitor a criminal suspect's e-mail, web surfing, or instant messaging?

Courts have only recently begun to address these questions, and the existing legal scholarship is surprisingly sparse.[1] As the Ninth Circuit noted in a recent decision:

> [T]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.[2]

The existing scholarship tends to be either highly abstract[3] or else focuses only on discrete doctrinal questions.[4] A few scholars have pointed out that the

1. *See* discussion of existing cases *infra* Part II.C.

2. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) (applying the Fourth Amendment to copies of text messages in electronic storage), *cert. granted sub nom.* City of Ontario v. Quon, No. 08-1332, 2009 WL 1146443 (U.S. Dec. 14, 2009).

3. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 109-10 (1999) (advocating the translation of constitutional principles to the Internet).

4. For example, a few scholars have addressed whether users have a reasonable expectation of privacy in their personal e-mail accounts. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 125; Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation Of Privacy*, 8 J.

application of the Fourth Amendment to computer networks will require considerable rethinking of preexisting law,[5] but none have sketched out what that rethinking might be.

This Article presents a general approach for how the Fourth Amendment should apply to Internet communications. It argues that the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment. It then recommends two key principles to guide the application of the Fourth Amendment to the Internet. This approach does not try to settle every question in every case. At the same time, it does provide the major guidelines that should frame how courts apply the Fourth Amendment to computer networks. These guidelines create a general framework for how to translate the constitutional protection against unreasonable searches and seizures to the Internet.

The method of this Article is premised on an assumption I call "technology neutrality."[6] Technology neutrality assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world. That is, courts should try to apply the Fourth Amendment in the new environment in ways that roughly replicate the role of the Fourth Amendment in the traditional physical setting. As a result, the goal of this Article is to map the protections of the Fourth Amendment from physical space to cyberspace. It attempts to accurately translate the physical distinctions of the Fourth Amendment to the new network environment.[7]

This Article makes two basic arguments about how the Fourth Amendment should apply to the Internet. The first argument is that the contents of online communications ordinarily should receive Fourth Amendment protection but

---

TECH. L. & POL'Y 135, 135 (2003). Interestingly, the only scholarly works that have attempted to address the broader questions of the Fourth Amendment and the Internet are student notes from the mid-1990s, at the dawn of "cyberlaw" scholarship. *See, e.g.*, Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1591-92 (1997); Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1181 (1995).

5. *See, e.g.*, Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 296-99 (2005) (discussing need for new principles of Fourth Amendment protection to apply to the Internet); John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 242 (2008) (arguing that it is necessary, in light of how the Internet works, "to rethink legal protections for citizens from state surveillance in a digital age"); Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 83 (2006) (discussing need for new principles of Fourth Amendment protection online).

6. *See infra* Part I.C.

7. *Cf.* Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165, 1211-14 (1993) (discussing how legal meaning can be translated across different contexts to maintain equivalence of interpretation).

that non-content information should not be protected. This approach accurately translates the traditional physical distinction between invasion into enclosed spaces and evidence collection in public. In a physical environment, the former is a Fourth Amendment search and the latter is not. Online, that role should be played by the distinction between the content of communications and non-content information relating to those communications. Courts should hold that Internet users ordinarily have a reasonable expectation of privacy in the contents of the Internet communications but not in non-content information. Recent court decisions have pointed cautiously in this direction based on narrow analogies to the postal network and the telephone.[8] This article explains why the content/non-content distinction is not only justified by narrow analogies but also by its functional role and comparisons between the physical world and the Internet.

The second argument turns to what kinds of Fourth Amendment protection should apply once a court concludes that some Fourth Amendment protection is warranted. This Article argues that courts should apply a warrant requirement to Internet communications, but that the particularity requirement should permit warrants for individual suspects rather than individual Internet accounts. In other words, a warrant should ordinarily be required to access the contents of Internet communications. The federal statute that permits the government to compel contents with less process than a warrant in some cases is therefore unconstitutional in many applications. At the same time, when the government establishes probable cause to believe that a person has or will use the Internet to store, transmit, or receive specific evidence of criminal activity, any account that the person has or will use—and that therefore might plausibly contain the evidence sought—should be included within the scope of the warrant. Although statutory authorities may adopt a narrower approach, the constitutional particularity requirement should apply to Internet *users* instead of Internet *accounts*.

The broader goal of this Article is to imagine how the traditional rules of police investigations can translate into rules within the new environment of computer networks and computer crimes. It imagines a world in which individuals commit their crimes entirely over the Internet, and it considers how the Fourth Amendment might regulate the government investigations that will follow. It concludes that new facts will trigger the need for new rules to restore the traditional function of the law. By appreciating the differences between how physical and virtual spaces regulate human behavior, it becomes possible to see how the constitutional principles established for a traditional physical environment can apply to the new environment of computer networks.

This Article proceeds in three parts. Part I considers the factual differences between the physical world and the Internet that will require an adjustment of the traditional Fourth Amendment rules in the translation of the Fourth

8. *See infra* notes 65-90.

Amendment to the Internet. It also explains and justifies the assumption of technology neutrality. Part II argues that these differences will require replacing the inside/outside distinction in the physical world with the content/non-content distinction for Internet communications. Part III argues that the warrant requirement should nonetheless apply to Internet communications, but that the particularity requirement should allow searches through multiple accounts belonging to the same criminal suspect.

I. THE FACTS OF PHYSICAL SPACE AND THE FACTS OF THE INTERNET

Technology provides new ways to do old things more easily, more cheaply, and more quickly than before. As technology advances, legal rules designed for one state of technology begin to take on unintended consequences.[9] If technological change results in an entirely new technological environment, the old rules no longer serve the same function. New rules may be needed to reestablish the function of the old rules in the new technological environment.[10]

This Part will introduce two major factual differences between the physical world and the Internet that demand changes in how the Fourth Amendment will apply. The first difference is the elimination of the inside/outside distinction, and the second difference is the removal of physical limits on scale and locality. When paired with the assumption of technology neutrality, these differences require a translation of Fourth Amendment principles to the Internet through a rethinking of Fourth Amendment rules to ensure that the basic function of the Fourth Amendment is the same online as it is offline.

A. *The Inside/Outside Distinction*

The first important distinction between the facts of physical investigations and those of Internet investigations is the loss of the inside/outside distinction. In the physical world, the distinction between inside surveillance and outside surveillance is foundational. The law of police investigations naturally harnesses that line to distinguish between what the police can do without cause and what they need cause to do. Online, however, that same distinction no longer serves the purpose that it serves in physical world investigations. Applying the Fourth Amendment to the Internet must therefore begin by finding a new distinction to mirror the traditional physical distinction between inside and outside.

---

9. *See* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 265 (explaining that "[r]ules are devised in a particular technological context, with explicit and implicit assumptions as to what is possible" and that the effect of the rules changes when technology shifts).

10. *See id.*

1. *Outside and inside in physical investigations*

The distinction between government surveillance outside and government surveillance inside is probably the foundational distinction in Fourth Amendment law, the body of law that regulates permissible searches and seizures in criminal investigations. According to this distinction, the government does not need any cause or order to conduct surveillance outside.[11] So long as conduct is out in the open, it is not protected by the Fourth Amendment. In the argot of existing doctrine, a person cannot have a "reasonable expectation of privacy" in public, even under circumstances in which a person would reasonably think he is alone and not under surveillance.[12] As a result, the police are permitted to access anything exposed to the general public. They are permitted to walk down public streets and see and hear whatever other members of the public are permitted to see. They can traverse over "open fields," even open fields that are the property of the suspect.[13] The only kind of open spaces that officers cannot enter are the "curtilage" of the home, which is (more or less) the space so close to the home that a person can readily observe the inside of the home through open windows.[14]

On the other hand, entering enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment. Entering a home,[15] entering a car,[16] or opening a sealed package[17] is normally considered a search that the Fourth Amendment regulates with either a warrant requirement or probable cause. Exceptions exist, of course. If the person has been legally ejected from their home,[18] or a letter is sent Fourth Class and is open to postal inspection,[19] then no warrant or cause is needed. But in most cases, enclosed spaces receive

---

11. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.").

12. *See id.*; *see also* California v. Ciraolo, 476 U.S. 207, 223 (1986) (Powell, J., dissenting) (noting that aerial observation of outside spaces by the government is permissible, since the areas are theoretically exposed to public scrutiny, and even though "the actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent").

13. This is true even if the property is enclosed by a fence. *See* United States v. Dunn, 480 U.S. 294, 296 (1987).

14. *See id.* at 300-03 (distinguishing curtilage from open fields).

15. Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

16. *See* United States v. Ross, 456 U.S. 798, 822 (1982).

17. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

18. *See* Amezquita v. Hernandez-Colon, 518 F.2d 8, 12 (1st Cir. 1975) (holding that squatters residing on government land did not have a reasonable expectation of privacy in their homes).

19. *See* United States v. Riley, 554 F.2d 1282, 1283 (4th Cir. 1977) (holding that postal mail sent Fourth Class is not protected).

Fourth Amendment protection. In the language of the legal fiction adopted in current doctrine, a person presumptively enjoys a "reasonable expectation of privacy" in inside spaces, even if he shares the spaces with others and privacy is unlikely. In the physical world, the line that the Fourth Amendment protects is the line between inside and outside. The police can investigate crimes outside without restriction, but the Fourth Amendment regulates evidence collection inside closed spaces.

The inside/outside distinction operates sensibly in a physical investigation governed by human eyesight. Outside spaces are open to visual observation. The officer can use the surveillance tool of his eyes to see what is there. In contrast, closed spaces are closed from visual observation; the officer cannot see what is inside the enclosure. To see what is behind the barrier, the officer needs to break into the house, jimmy open the car trunk, unseal the letter, or otherwise break through the physical barrier that blocks his eyes from being able to see evidence inside.

The line between inside and outside also serves an essential function for Fourth Amendment law. The inside/outside distinction exposes to government observation some basic information about what people did and where they went while simultaneously shielding their most personal information from police scrutiny absent cause. This is true because individuals do not usually leave their personal or sensitive belongings out in the open.[20] Instead, they hide them from view by putting them inside in an enclosed space. The inside/outside distinction therefore reveals where people are and where they are going while shielding their most private thoughts and speech from government view.[21]

This division in turn ensures a basic balance of Fourth Amendment protection.[22] If the Fourth Amendment protected everything, then the police would have great difficulty solving crimes; even walking down the street with eyes open would require probable cause. On the other hand, if the Fourth Amendment protected nothing, we would be inadequately protected against abusive government invasions of our homes and private spaces.[23] The inside/outside distinction strikes one of several possible middle grounds. The police can watch a person out in public, but ordinarily they cannot enter the kinds of private spaces where individuals typically hide their more sensitive belongings.

---

20. Of course, it is possible to leave private materials out in the open, in which case the private materials are not protected. But most people try to protect private materials by hiding them from view.

21. That is, the public aspect of a person's conduct occurs outside, and generally is limited to where a person is, what they look like, and what they are doing.

22. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574-75 (2009).

23. *See* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (reasoning that without a reasonable expectation of privacy, even the home would not be protected by the Fourth Amendment).

2. *Outside and inside in Internet investigations*

If the facts of criminal investigations switch from those of the physical world to those of the Internet, the inside/outside distinction no longer works. On the Internet, almost everything is enclosed. Everything is "inside." The entirety of the Internet is packed into wires and storage devices, and those wires transfer and store Internet communications without generally exposing communications to open observation. Instead of a physical world where visual surveillance reigns and many things are out in the open, we now have an enclosed environment in which eyes no longer "see" any "outside" of the network.[24]

This doesn't necessarily mean that all Internet communications are inside. Internet communications are often transmitted over the airwaves through wireless networks. Communications sent over wireless networks are "outside" in the sense that they can be intercepted in the open; the communications do not pass through enclosed wires but rather are sent through the air like radio waves.[25] At the same time, the Internet setting renders the practical meaning of inside and outside very different online than in the case of the physical world. The distinction between wired and wireless communication is an accident of technology, not a fundamental dividing line separating what can be observed from what cannot be observed.[26] The inside/outside distinction no longer serves the basic function in the Internet setting that it serves in the physical world. Some new distinction is needed online to capture the basic balance of Fourth Amendment protection that the inside/outside line provides in the physical world.

B. *Physicality Limits Scale and Location*

The second important difference between physical and digital environments for criminal investigations is that physical environments generally limit the scale and location of evidence but digital environments normally do not. In the physical world, the amount and location of evidence is

24. *See* K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J.L. & TECH. 128, 143-46 (2007) (describing the process of modern communications surveillance).

25. *See generally* Nicole A. Ozer, *No Such Thing As "Free" Internet: Safeguarding Privacy and Free Speech in Municipal Wireless Systems*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 519 (2008) (discussing the widespread use of public wireless networks).

26. The experience of using the network stays the same regardless of whether communications are sent over wires or wirelessly. Here the comparison between landline telephones and cellular phones is helpful: although cell phone calls are transmitted through the open air, users consider cell phone calls just as private as landline calls. Indeed, the Wiretap Act protects the two types of communications in precisely the same way. *See* 18 U.S.C. § 2510(1) (2006) (defining "wire communication" without regard to whether the intercepted part of the communication is passed over wires at the point of interception).

limited. Its location tends to be predictable. Traditional Fourth Amendment rules have been crafted in light of those assumptions; the rules generally are scale- and location-specific. Those assumptions do not hold in the Internet environment. In a world of data, third-party services can always provide more data, and the data can be anywhere. No limit exists on the number, size, or location of accounts, services, or data one person can control that might contain the evidence that the government seeks.

1. *Physicality, scale, and the Fourth Amendment*

It is easy to overlook how the physical world limits the scale and location of evidence. Identifying the evidentiary characteristics of the physical world is a bit like describing the taste of water. But it is important to step back and see how physicality limits evidence. Physicality imposes limits on evidence, its amount, and its location. It limits where evidence can be located, how much there can be, how quickly it can be moved, and how many different places can store it.

The reason why is obvious. Physical evidence is bulky. It has weight. It requires energy to move it and effort to hide it. It must be stored in a safe location, and those physical storage places must be rented, bought, or borrowed. These requirements limit how much evidence can exist, how much loot can be taken, how quickly it can be moved, and where it can be located. As a result, inherent limits exist on how much evidence can exist and where it can be located. Evidence tends to be in a specific place, usually near the crime scene, and that specific place is usually somewhat predictable and all in one physical location. In the physical world, spaces where a person can safely hide evidence are relatively limited; to avoid detection, wrongdoers will generally store evidence only in the few spaces that they physically control, such as their homes.

An example may be helpful, so imagine a robber tries to rob a bank. He walks in, pulls out a gun, and fills up a bag with cash before running out the door and hopping in the getaway car. Officers are called to investigate. The officers must rely on the fact that the robber's location, the location of the stolen loot, and the amount of that loot will be limited by the realities of physical asportation. The robber can only fit so many bills in the bag, and he can only be as far away from the bank as his getaway car will allow. The loot will likely be all together, and will likely be where the bank robber actually put it. If it is divided up, it will likely be divided up in only a few parts. For investigators, this means that the locations where the robber and the loot could be located are limited and relatively predictable.

Further, the scale of physical places tends to be predictable. Consider the canonical example of a home. A home might be a studio apartment or a fifteen-room mansion, but the variation in size normally stays within an order of magnitude. Most houses will have a kitchen, a bathroom or two, and a few

bedrooms. Further, most individuals will have one home. Some lucky folks will have more, but the costs of home ownership ensure that most have only one. The physicality and scale of the physical world tends to generate ready hypotheses of how much evidence exists and where it can be found.

Existing Fourth Amendment rules and search and seizure practices harness these physical limits. For example, the scope of permitted searches is generally keyed to physical concepts. Physical scale limits how far searches can go. A search incident to arrest includes the physically grabbable area near the arrestee, but generally no further.[27] A search warrant must describe the physical place to be searched with particularity, generally approving searches the physical scale of a single home or property but rarely more.[28] Search warrants issued by judges in a particular district have traditionally been limited to places and evidence in that district.[29] These limitations make perfect sense in a world of physical evidence; physicality limits the scale and location of evidence, so Fourth Amendment rules can harness those restrictions and limit government invasions using physical limitations.

2. *Physicality and scale in Internet investigations*

A very different dynamic exists with electronic data. Data sent, stored, and received over the Internet can be copied repeatedly, instantly, and freely. It can be zipped around the world in a split second, and it can be stored anywhere and without cost. The data does not occupy any physical space, and it can be divided up and distributed anywhere.

Unlike physical evidence, electronic data has no inherent limitations on how much can exist, where it can be located, and where it can be stored. In the physical world, physicality limits scale. If a suspect is believed to have evidence stored at home, that suspect will likely have one home, that home will be in only one location, and the size of the home will be finite. In the Internet setting, by contrast, no such limitations exist. A suspect could have hundreds of Internet accounts, could store evidence in any or all of them, the accounts could be anywhere, and there are essentially no limits on how large the accounts might be. Over time, these differences are becoming starker. Consider the online activity of a typical Internet user. A decade ago, a typical Internet user

---

27. *See, e.g.*, New York v. Belton, 453 U.S. 454, 460 (1981).

28. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 479 (1976).

29. *See* FED. R. CRIM. P. 41(b)(1) (stating that "a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district"). Traditionally, narrow exceptions have existed for property outside the district. However, those exceptions were recently expanded as part of the recent amendments to the Federal Rules of Criminal Procedure. *See generally* U.S. SUPREME COURT, AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE (2008), *available at* http:// www.supremecourtus.gov/orders/courtorders/frcr08p.pdf.

might have one or two e-mail accounts. Today, a typical user might have four or five e-mail accounts, a Facebook account, two or three chat accounts, several registrations with websites that host internal messaging, and several additional sites for remote online storage. As the Internet matures, the number of accounts appears to be rising exponentially.[30]

The key difference is that the absence of physical limits means that Internet services merely require bandwidth: the only limit is computer capacity or "bandwidth," both of storage and transmission. But computer bandwidth has proven so far to be a relatively low cost: unlike physical space, computer network operators can always add more, and it is relatively inexpensive to do so. As a result, there are few if any limits as to how many services a particular person can control or use or where that evidence might be.

Physical scale and location no longer limits where evidence might be, or how much might exist, probable cause to believe evidence exists no longer generally presupposes cause to believe it is located in a specific physical place. Fourth Amendment rules will need to account for the switch.

C. *The Assumption of Technology Neutrality*

Up to now, this Article has shown how the facts of the physical world and the Internet are different in ways that change the evidence that exists and how it might be collected. The question is: how should the Fourth Amendment respond? In other words, why do these changes matter? As explained in the Introduction, this Article will assume that the Fourth Amendment is "technology-neutral." It then uses that assumption to imagine what a new Fourth Amendment might look like in the online environment. But what is technology neutrality, and why is it a useful assumption? This Part explains the assumption and justifies its use.

The assumption of technology neutrality posits that judges will interpret the Fourth Amendment in the online environment so that it has roughly the same role in new Internet crime investigations that it has established in traditional physical investigations. That is, the Fourth Amendment will remain technology-neutral in the sense that the overall amount and function of Fourth Amendment protection will be roughly the same regardless of whether a wrongdoer commits his crime entirely online, entirely in the physical world, or

30. A decade ago, individuals ordinarily had one type of Internet message system—e-mail—and generally had accounts from either work, school, or their Internet service providers such as America Online. Today, however, most individuals have many different types of services for sending, receiving, and remotely storing communications. E-mail has been supplemented by Facebook, Google Chat, and the like, and most users have many accounts within various services. Unfortunately, it seems that documentation for this changing social practice is difficult to find. However, I submit it matches the social understanding of the majority of individuals who have been regularly using the Internet for the last decade.

using a mix of the two. New facts will trigger new rules, but the role of the Constitution should remain constant regardless of technology.[31] As a result, as more and more criminal conduct shifts from physical crimes to electronic crimes, and more and more cases are solved by digital evidence instead of physical evidence, the overarching function of the Fourth Amendment will not change.

This is not the only way to apply the Fourth Amendment. Constitutional theorists might apply any one among the many constitutional modalities—or a mix of them—to argue for a particular normative approach. Under these methods, it is possible to make a normative argument that the Fourth Amendment should apply either more broadly or more narrowly to the Internet than to the physical world.[32] These are important arguments, and I have contributed to such debates myself.[33] This particular Article seeks to sidestep that debate, however, and instead will simply assume technology neutrality. That is, this Article will not make an affirmative case that technology neutrality is normatively the most desirable approach to the interpretation of the Fourth Amendment. Instead, it uses technology neutrality as a baseline and considers what a technology-neutral Fourth Amendment might look like when applied to the Internet.

I believe this assumption is justified by the deeply entrenched judicial consensus—albeit one arguably more implicit than explicit—that technology neutrality is the proper approach to the Fourth Amendment. Put simply, judges today *think* that this is what the Fourth Amendment requires, and this belief seems unshakeable for the foreseeable future. That intuition likely follows from the 1960s-era development of the Fourth Amendment, and in particular the decisive victory of the Warren Court Justices over Justice Black's and Justice Douglas's impassioned originalist and textualist dissents in the wiretapping case of *Berger v. New York*,[34] the bugging case of *Katz v. United States*,[35] and the mere evidence case of *Warden v. Hayden*.[36] That trio of cases in 1967 cases forced the Supreme Court to choose between two competing conceptions of the Fourth Amendment: one as specific prohibition of specific historical practices, and the other as pragmatic regulator of police investigations.[37] In 1967, the

31. *See generally* LESSIG, *supra* note 3 (discussing how translating constitutional protections can maintain fidelity as technology changes).

32. *Compare* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (arguing for a modest role for the Fourth Amendment when technology is in flux), *with* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 748 (2005) (arguing for a more robust role for the Fourth Amendment in such circumstances).

33. *See* Kerr, *supra* note 32.

34. 388 U.S. 41 (1967).

35. 389 U.S. 347 (1967).

36. 387 U.S. 294 (1967).

37. *See generally* Morgan Cloud, *A Liberal House Divided: How the Warren Court*

Warren Court decisively chose the latter. [38]

That choice four decades ago has now become so deeply embedded that it has become a natural instinct among judges. Indeed, no sitting judge or justice today questions that the Fourth Amendment is a tool for imposing reasonable restrictions on police conduct. (Textualists such as Justice Scalia justify this approach by the Fourth Amendment's textual prohibition on "unreasonable searches and seizures," although it requires them to impose the modern cost-benefit concept of reasonableness on text that very likely had a quite different meaning.)[39] Different judges may disagree on what restrictions are reasonable, but their conceptual understanding of what the Fourth Amendment does is surprisingly uniform. Regardless of what theory we might like to impose on the Fourth Amendment, that understanding has become fixed and seems unlikely to change among the judges tasked with handing down Fourth Amendment decisions.

This consensus understanding has an effective corollary of technology neutrality. If judges see the Fourth Amendment as a tool for balancing privacy and security interests to require reasonable police behavior, that same balance should be sought regardless of technology. The balance struck in physical investigations should be the same balance struck in Internet investigations. The facts may change, but the balance should remain the same. Which brings us back to the core question that this Article attempts to answer: how should a technology-neutral Fourth Amendment apply to the Internet?

II. REPLACING THE INSIDE/OUTSIDE DISTINCTION WITH THE CONTENT/NON-CONTENT DISTINCTION

The combination of the factual differences between the physical world and the Internet and the assumption of technology neutrality requires courts to translate the principles of the Fourth Amendment from the former to the latter so that the law will maintain the old function in the new environment. The rules that made sense in the physical world may not make sense in the online world. New rules may be needed in light of the new environment. What new rules are needed, and what should they look like?

The first change that the Fourth Amendment will require online is replacing the inside/outside distinction. In a physical environment, the inside/outside distinction creates the basic balance of Fourth Amendment law. It creates a regime of low-privacy public spaces and high-privacy private

Dismantled the Fourth Amendment, 3 OHIO ST. J. CRIM. L. 33 (2005) (discussing the different visions of the Fourth Amendment at stake in the Warren Court's Fourth Amendment jurisprudence)

38. *See id.* at 72-73.

39. I am indebted to Professor Davies' persuasive historical work on this issue. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 555 (1999).

spaces, and thus balances the need of the police to investigate crime through surveillance in low-privacy public spaces with the needs of individuals to be free from surveillance without cause in the more private spaces. In the Internet setting, however, the inside/outside distinction no longer serves this basic function. The question is, what new distinction might replace it? What rule or standard in the online setting can serve the same basic function that is served by the inside/outside distinction in the physical world?

This Part argues that the distinction between inside and outside in the physical world should be replaced in the online setting by the distinction between content and non-content information. In the online setting, courts should treat non-content information relating to communications as if it were functionally "outside" and content information as if it were functionally "inside." Internet surveillance of non-content information should not trigger the Fourth Amendment just like surveillance of public spaces does not trigger the Fourth Amendment, and surveillance of content should presumptively trigger the Fourth Amendment in the Internet setting just like surveillance of inside spaces presumptively triggers the Fourth Amendment in the physical world.

The core reason why is that the content/non-content distinction captures the basic function of the inside/outside distinction. Outside surveillance is usually surveillance relating to identity, location, and time. By watching a person in public, the police normally can learn where he was at a particular time and where he was going. In contrast, inside surveillance more often exposes private thoughts. By breaking into a person's private spaces, the police can obtain insights into the contents of the person's mind that he normally keeps to himself or only shares with a trusted few. That distinction correlates reasonably accurately to the online distinction between content and non-content surveillance. Online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private thoughts and speech. Indeed, the function of the network itself explains the correlation of the two principles: communications networks are mechanisms for delivering contents that would otherwise have to be delivered in person, and the non-content information on the network is the information needed to deliver the communication that substitutes for the public act of delivering contents.

Importantly, this basic insight is only a first step towards applying the Fourth Amendment to the Internet. The line between content and non-content information can be difficult in some cases involving person-to-computer applications. Further, a presumption that contents of communications are protected by the Fourth Amendment is just a presumption. There will likely be many exceptions to this rule, just as there are exceptions to the presumption that inside surveillance is protected, and it is beyond the scope of this Article to identify in exactly which circumstances content surveillance should be allowed. But while this is only a first step, it is very much an important one. Recent

court decisions have pointed somewhat hesitatingly in this direction,[40] and this Part shows why this direction is correct and why courts should follow this distinction in the future.

A. *The Content/Non-Content Distinction*

Whereas the inside/outside distinction is basic to physical world investigations, the content/non-content distinction is basic to investigations occurring over communications networks. Communications networks are tools that allow their users to send and receive communications from other users and services that are also connected to the network. This role requires a distinction between addressing information and contents.[41] The addressing (or "envelope") information is the data that the network uses to deliver the communications to or from the user; the content information is the payload that the user sends or receives.[42]

Consider a few examples, starting with the postal network. The postal network permits users to send and receive letters. The addressing information for the letter is the "to" and "from" address and the postmark. This information is used to deliver the message; it tells the Post Office where the letter should go and where it should be returned if it can't be delivered, and keeps a record of where it was processed. In contrast, the contents are the letter itself. The letter itself isn't handled by the Post Office; the contents are of no concern to the Post Office, as the contents are only the concern of the sender and receiver.[43]

We can see the same distinctions at work with the telephone network. The telephone network permits users to send and receive live phone calls. The addressing information is the number dialed ("to"), the originating number ("from"), the time of the call, and its duration. Unlike the case of letters, this calling information is not visible in the same way that the envelope of a letter is.[44] At the same time, it is similar to the information derived from the envelope of a letter. In contrast, the contents are the call itself, the sound sent from the caller's microphone to the receiver's speaker and from the receiver's microphone back to the caller's speaker.

Drawing the content/non-content distinction is somewhat more complicated because the Internet is multifunctional. While the old-fashioned telephone network is just about calls, the Internet sends and delivers many different kinds of communications at once. It acts as many different services,

---

40. *See infra* notes 77- 94.

41. I have explored this distinction in Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611-14 (2003).

42. *See id*. at 611.

43. Indeed, federal law prohibits postal employees from opening the mail. *See* 39 C.F.R. § 233.11 (2009).

44. That is, the number dialed is not exposed to the public, even if it is exposed to the phone company.

not just one, meaning that the distinction may need to be drawn differently for each type of Internet program. Still, the content/non-content distinction holds in the Internet context as well. The easiest cases are human-to-human communications like e-mail and instant messages. The addressing information is the "to" and "from" e-mail address, the instant message to and from account names, and the other administrative information the computers generate in the course of delivery.[45] As in the case of letters and phone calls, the addressing information is the information that the network uses to deliver the message. In contrast, the actual message itself is the content of the communication.[46]

B. *The Content/Non-Content Distinction as a Replacement for the Inside/Outside Distinction*

The content/non-content distinction provides a natural replacement for the inside/outside distinction. To apply the Fourth Amendment to the Internet in a technologically neutral way, access to the contents of communications should be treated like access to evidence located inside. Accessing the contents of communications should ordinarily be a search. In contrast, access to non-content information should be treated like access to evidence found outside. Collection of this information should presumptively not be a search.

This translation is accurate because the distinction between content and non-content information serves the same function online that the inside/outside distinction serves in the physical world. Non-content information is analogous to outside information; it concerns where a person is and where a person is going. Consider what the police can learn by watching a suspect in public. Investigating officers can watch the suspect leave home and go to different places. They can watch him go to lunch, go to work, and go to the park; they can watch him drive home; and they can watch him park the car and go inside. In effect, this is to/from information about the person's own whereabouts.

On the other hand, content information is analogous to inside information. The contents of communications reveal the substance of our thinking when we assume no one else is around. It is the space for reflection and self-expression when we take steps to limit the audience to a specific person or even just to ourselves. The contents of Internet communications are designed to be hidden from those other than the recipients, much like property stored inside a home is hidden from those who do not live with us. Granted, others may end up with access we do not intend. The system administrator of a network might poke around and see a file on the server; a hacker might break in and rummage around our remotely stored files. But these sorts of invasions also can occur in

45. *See* Kerr, *supra* note 41 at 612.

46. *See id.*; *cf.* 18 U.S.C. § 2510(8) (2006) (defining "contents" for purposes of the Wiretap Act as "any information concerning the substance, purport, or meaning of that communication").

the home. A busybody landlord or building superintendent might enter an apartment to look around; a burglar might break in and look for something to steal. These possible invasions do not eliminate Fourth Amendment protection in the home, nor should their online equivalents eliminate that protection in virtual spaces. Storing the file on a password-protected server is the virtual equivalent of keeping it in a home.[47]

The connection between content/non-content on the Internet and inside/outside in the physical world is not a coincidence. Addressing information is itself a network substitute for outside information, and contents are a network substitute for inside information. Recall the basic function of communications networks: they are systems that send and receive communications remotely so that its users do not have to deliver or pick up the communications themselves. The non-content information is the information the network uses to deliver communications, consisting of where the communication originated, where it must be delivered, and in some cases the path of delivery. This information is generated in lieu of what would occur in public; it is information about the path and timing of delivery.[48] In contrast, the contents are the private communications themselves that would have been inside in a physical network.

Consider the postal network. In a world without the postal network, a person who wanted to deliver a letter would have to deliver it himself. He would take the letter, travel to the destination, and leave the letter there. All of this would be open to surveillance; if the police wanted to, they could watch him travel from the origin to the destination point. Envelope addressing information is the information that a person tells the postal network when he wants the postal network to do the job for him. The sender gives the postal service the information it needs, such as the "to" address and the "from" address. The postal service then does the work: the mail carrier is the one who goes out and travels from the origin to the destination, using the information provided by the sender. In effect, the use of the service of the network substitutes the previously public information about the person's whereabouts in the delivery of the letter for the addressing information of the letter's delivery.[49] The outside information turns into the addressing information, and the inside information becomes the content of the communication.

In light of this, a technologically neutral way to translate the Fourth Amendment from the physical world to the Internet would be to treat government collection of the contents of communications as analogous to the government collection of information inside and the collection of non-content information as analogous to the collection of information outside. The fact that content and non-content information are actually jumbled together as packets

47. *See* Bellia & Freiwald, *supra* note 4, at 138-39, 148.

48. *See* Kerr, *supra* note 22 at, 577-78.

49. *See id.* at 575-77.

shouldn't matter; the function of the inside/outside distinction is best captured in the network environment by recognizing the line between content and non-content information independently of the technical details of how the Internet works.

This approach would mirror the line that the Fourth Amendment imposes in the physical world. In the physical world, the inside/outside distinction strikes a sensible balance. It generally lets the government observe where people go, when they go, and to whom they are communicating while protecting the actual substance of their speech from government observation without a warrant unless the speech is made in a setting open to the public. The content/non-content distinction preserves that function. It generally lets the government observe where people go *in a virtual sense*, and to observe when and with whom communications occur. The essentially transactional information that would occur in public in a physical world has been replaced by non-content information in a network environment, and the content/non-content line preserves that treatment. At the same time, the distinction permits individuals to communicate with others in ways that keep the government at bay. The Fourth Amendment ends up respecting private areas where people can share their most private thoughts without government interference both in physical space and cyberspace alike.

C. *Existing Law on the Content/Non-Content Distinction*

There are few Fourth Amendment cases on how the content/non-content distinction applies to the Internet. The law remains in its infancy. However, the few cases on the books have so far either hinted at or actually adopted the content/non-content distinction. The story of how courts came to adopt this distinction shows how analogical reasoning from physical cases to Internet cases produces the same result that I propose. Some of the cases in these steps have been criticized, however, and as a result the new cases applying the distinction to the Internet are at best tentative. These new cases should be encouraged, and the line between content and non-content embraced.

1. *Postal letters*

To understand the evolution of the case law, it helps to begin with the postal network and to work forward through the telephone network and only then reach the few cases on the Internet. The Fourth Amendment rules that apply to access to postal mail were settled in what may be the first Fourth Amendment case, *Ex parte Jackson.*[50] *Jackson* was a constitutional challenge to Congress's power to regulate tampering with the mail, but Justice Field took the opportunity in extensive dicta to explain the Fourth Amendment rules for

50. 96 U.S. 727 (1877).

access to postal mail. Under *Jackson*, the outside of packages is not protected by the Fourth Amendment: in the modern lingo, people do not retain a reasonable expectation of privacy in the outside of their packages.[51] In contrast, the interior of packages is protected by the Fourth Amendment: the government cannot open the package in transit without a warrant.[52]

The postal mail precedents have obvious force in the case of e-mail and other person-to-person Internet messages. The body of an e-mail message, the subject line, and the contents of any attachments are analogous to the contents inside a postal envelope or package. They constitute the message that the sender wants to share with the intended recipient. The e-mail header (minus the subject line) containing the to/from address, size of the e-mail, and mail servers that routed the message are analogous to the to/from address, dimensions, and postmark of a postal letter.[53] They are the information about the communication that the network learns when it has possession of the communication and that it uses to deliver the communication. In both cases, the non-content addressing information is unprotected while the content information is presumptively protected.

2. *The telephone*

The Supreme Court has reached similar results in the case of the telephone, although its decisions have been controversial and (in one case) initially took a wrong turn. The move from the postal service to the telephone was nonobvious for the same reason that the move to the Internet is nonobvious: unlike the postal service, the telephone network does not follow the inside/outside distinction. In the case of postal letters, *Ex parte Jackson* nicely tracks the same inside/outside line that was true in the physical world. Addressing information is public because it appears on the outside of the package, exposed, if not to the public, then at least to government postal employees. In contrast, the contents of sealed letters and packages are sealed away, free from inspection, and thus functionally inside. This isn't true with telephone calls. Both the numbers dialed and contents of the call are together, inside the wires in one physical sense and yet out in the open in the sense of passing through publicly visible and accessible wires in city streets.

When the Supreme Court first considered the question, it held in *Olmstead v. United States*[54] that content wiretapping was not protected by the Fourth Amendment. Chief Justice Taft naturally relied on the inside/outside distinction

51. *Id*. at 733.

52. Even then, there is an exception: if the package or letter is sent through the mail in an open format, such as a postcard or as fourth class mail that can be inspected by the government, then the contents do not receive Fourth Amendment protection. *See* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.2(a) (3d ed. 2007).

53. *See* Kerr, *supra* note 41, at 611-13.

54. 277 U.S. 438 (1928).

in support of his claim. According to Taft, the government had tapped the defendant's telephone by tapping the wires leaving his home and his work from a public vantage point. Olmstead had no privacy rights against wiretapping because he had broadcast his call into the world, "quite outside,"[55] much as if he had shouted in a public space.[56] Justice Brandeis's famous dissent construed the telephone conversation as inside, not outside: according to Brandeis, a telephone user entered a virtual private space, and tapping the phone effectively entered the virtual space.[57]

The Supreme Court famously reversed course four decades later in *Katz v. United States*.[58] *Katz* agreed with Justice Brandeis that listening to a private phone call was like entering a private space: Justice Harlan, whose concurrence announced the "reasonable expectation of privacy" test, thought that the "critical fact" was that a phone booth where a person makes a call is "a temporarily private place" that was intruded on by eavesdropping.[59] As a result, the contents of phone calls are protected by the Fourth Amendment. Lower court cases have narrowed this holding a bit in ways that mirror how the Fourth Amendment treats access to postal mail.[60] But the basic rule is that the contents of phone calls ordinarily receive full Fourth Amendment protection.[61]

In *Smith v. Maryland*,[62] the Supreme Court completed the picture by ruling that the numbers dialed from a telephone call were not subject to Fourth Amendment protection. Unlike the contents of the call, the number dialed was just information that the caller sent to the phone company so the phone company could complete the call.[63] The *Smith* opinion is poorly written and reasoned, but the result is consistent with the postal service cases. The non-content addressing information for a call is treated just like the non-content addressing information for a letter or package. Just as the address on a letter is exposed to the carrier so the carrier can deliver it to the proper address, so is the

---

55. *Id.* at 466.

56. *See id.* ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.").

57. *See id.* at 474-76 (Brandeis, J., dissenting).

58. 389 U.S. 347 (1967).

59. *Id.* at 361 (Harlan, J., concurring).

60. Courts have decided a number of cases involving cordless phone calls, which broadcast their signal between the handset and the base. Courts have held that listening in on the broadcast calls using receivers is not regulated by the Fourth Amendment: just as the contents of postcards and fourth class mailings are open to inspection, so are the broadcast phone calls. *See, e.g.*, McKamey v. Roach, 55 F.3d 1236, 1239-40 (6th Cir. 1995) (broadcast cordless phone calls); United States v. Riley, 554 F.2d 1282, 1283 (4th Cir. 1977) (fourth class mailings).

61. *See, e.g.*, 2 LAFAVE, *supra* note 52, § 4.3(a), at 450-51.

62. 442 U.S. 735 (1979).

63. *Id.* at 742.

number dialed exposed to the phone company so the phone company can complete the call. The contents of the communication receive Fourth Amendment protection while the metadata used to complete the call does not.

3. *Internet communications*

Case law on how the Fourth Amendment applies to Internet communications remains remarkably sparse.[64] The reasons why are a bit murky, although two explanations are likely the most important. First, Congress extended the electronic surveillance statutes to computer and e-mail communications in 1986 when it passed the Electronic Communications Privacy Act.[65] Although the statute provides lesser protections in some ways than would the Fourth Amendment, the existence of clear statutory protections has likely drawn attention away from possible constitutional challenges. Second, the most common type of computer crime prosecuted in the last decade, child pornography offenses, do not require online surveillance and instead mostly focus on the search and seizure of stand-alone computers.[66] As a result, the Fourth Amendment rules governing online surveillance have remained largely unexplored.

Indeed, before 2007, only a few courts had touched on any part of how the Fourth Amendment should apply to the Internet. In 1996, an Article I military court ruled in *United States v. Maxwell*[67] that the Fourth Amendment applied to e-mail messages shared among America Online users. The decision specifically excluded "Internet e-mail" from its ruling, however, suggesting that "Internet e-mail" might receive different treatment.[68] In 2001, the Sixth Circuit decided *Guest v. Leis*, a Fourth Amendment challenge to government

64. See 2 LAFAVE, *supra* note 52, § 4.4(a), at 456-57 ("How the Fourth Amendment applies to the government surveillance of Internet communications is presently highly unsettled.").

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

66. Child pornography cases ordinarily are investigated by gathering probable cause to search a home, and then executing a warrant at the home that then leads to the recovery of a computer containing contraband images.

67. 45 M.J. 406, 417-19 (C.A.A.F. 1996) (analogizing America Online e-mails to letters).

68. *Id.* at 417 ("AOL differs from other systems, specifically the Internet, in that e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank located in Vienna, Virginia." (citation omitted)). The somewhat puzzling distinction between "AOL e-mail" and "Internet e-mail" appears to refer to the distinction between messages among AOL users that never leave AOL's facilities and e-mail that must travel across the network from server to server. *See id.* ("Just for comparison, the Internet has a less secure e-mail system, in which messages must pass through a series of computers in order to reach the intended recipient.").

access to an online Bulletin Board Service.[69] The court did not reach the question, however, after finding that a valid warrant had been obtained.[70] In 2002, the Eighth Circuit handed down a ruling in *United States v. Bach*[71] on executing a search warrant for Yahoo! e-mail. The court noted the uncertainty as to whether the Fourth Amendment protected e-mail, but simply assumed without deciding that e-mail received Fourth Amendment protection and upheld the search.[72] And in 2004, the Supreme Court of Wisconsin held that Wisconsin legislators could challenge a subpoena asking for backup tapes of the legislature's e-mail server, ruling along the way that state legislators had privacy rights in their government e-mail.[73] However, that decision applied the sui generis framework for government employee rights, and therefore did not address the broader question of Fourth Amendment rights in e-mail.[74]

The only Fourth Amendment fact pattern that courts reached concerning Internet investigations before 2007 considered the disclosure of basic subscriber information for Internet users. This has proved to be a recurring issue in child pornography investigations: in these cases, investigators learn that an individual has been using a specific Internet account or Internet protocol (IP) address to distribute or seek images of child pornography. Investigators then subpoena the Internet service provider (ISP) associated with that address to obtain the name and home address associated with that account, and they use that information as part of the probable cause to obtain a warrant to search the home associated with the address.[75] After a search warrant reveals contraband images and leads to charges, the defendant challenges the collection of his home address. Courts began to decide such cases in the late 1990s and have uniformly concluded that the Fourth Amendment does not protect it.[76] This conclusion did not require any intellectual heavy lifting, however: it has been long established that the Fourth Amendment doesn't apply to basic subscriber information for telephone accounts,[77] Western Union accounts,[78] and other

69. 255 F.3d 325 (6th Cir. 2001).

70. *Id.* at 333-35.

71. 310 F.3d 1063 (8th Cir. 2002).

72. *Id.* at 1066 ("While it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution.") (dictum).

73. *In re* John Doe Proceeding, 680 N.W.2d 792 (Wis. 2004).

74. *See id.* at 805-06.

75. *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

76. *See, e.g.*, *Kennedy*, 81 F. Supp. at 1110 (finding no Fourth Amendment protection for network account holder's basic subscriber information obtained from Internet service provider); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (same).

77. *See, e.g.*, United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (telephone accounts).

78. *See, e.g.*, *In re* Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987) (Western Union accounts).

similar third-party accounts, and it is difficult to articulate a reason why the name and address of an Internet account should receive a different rule.

In 2007, however, significant cases finally started to appear. First, a panel of the Sixth Circuit handed down a remarkable decision in *Warshak v. United States*.[79] Stephen Warshak was a suspect in a massive fraud investigation who sought a preliminary injunction to stop the federal government from obtaining e-mail without a warrant in the Southern District of Ohio. The initial Sixth Circuit panel upheld the injunction, using the case as an opportunity to write a mini-treatise on how the Fourth Amendment applied to commercial e-mail.[80] The panel's decision was quickly vacated, and the en banc court overturned the injunction on procedural grounds without addressing the merits of how the Fourth Amendment applied.[81] But while some of the panel's conclusions were quirky and hard to reconcile with the case law,[82] the court did reach a clear ruling that e-mail ordinarily receives Fourth Amendment protection just like telephone calls: "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP."[83] The court explained its conclusion largely by analogy to the social role of Internet communications: "like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[84]

Although the *Warshak* panel ruling remained in effect for only a few months, the Ninth Circuit handed down a pair of important decisions in 2008 addressing how the Fourth Amendment applies to the Internet. First, in *United States v. Forrester*,[85] the Ninth Circuit held that the government did not trigger the Fourth Amendment when it had a target's Internet service provider install a monitoring device that recorded the IP address, to/from address for e-mails, and volume sent from the account. In an opinion by Judge Fisher, the Ninth Circuit held that this non-content monitoring did not trigger the Fourth Amendment under *Smith v. Maryland*.[86]

The court's opinion adhered closely to the analogy to the pen register

79. 490 F.3d 455 (6th Cir. 2007).

80. *Id.* at 469-76.

81. The panel opinion was vacated on October 7, 2007, and the en banc decision was handed down in July 2008. *See* Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc).

82. *See generally* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/2007/06/21/the-procedural-errors-of-warshak-v-united-states/ (June 21, 2007, 15:04 PST); Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/2007/06/26/warshak-and-fourth-amendment-standards-for-orders-to-compel/ (June 26, 2007, 15:17 PST).

83. *Warshak*, 490 F.3d at 473.

84. *Id.*

85. 512 F.3d 500 (9th Cir. 2008).

86. *Id.* at 509-11.

surveillance approved in *Smith*: "[w]e conclude that the surveillance techniques are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith.*"[87] Judge Fisher reasoned that both IP addresses were the Internet equivalent of telephone numbers: Internet users "should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties." Judge Fisher contrasted that with content surveillance:

> When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. . . . [T]he Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.[88]

A subsequent Ninth Circuit panel expressly adopted the flip side of the picture for contents in a case involving text messages used by government employees. Although the facts of the case technically involved a telephone-based technology, the court in *Quon v. Arch Wireless Operating Co.*[89] looked at *Forrester* and interpreted it as intuitively adopting the same content/non-content line that had appeared in the telephone setting.

> We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here. Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in *Forrester*, we also see no meaningful distinction between text messages and letters. As with letters and e-mails, it is not reasonable to expect privacy in the information used to "address" a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider.[90]

The Supreme Court granted certiorari to review the *Quon* decision in December 2009, shortly before this Article went to press. At present, its future remains uncertain.[91] However, *Forrester* and *Quon* presently are the only two federal appellate cases that directly address how the Fourth Amendment applies to computer network surveillance. Both opinions reflect cautious analogical reasoning. Neither is theoretically ambitious. Further, both opinions are narrow and limited to their facts. *Quon* only covers access to stored text messages held by a third-party provider; *Forrester* only covers real time surveillance of

87. *Id.* at 510.

88. *Id.*

89. 529 F.3d 892 (9th Cir. 2008), *cert. granted sub nom.* City of Ontario v. Quon, No. 08-1332, 2009 WL 1146443 (U.S. Dec. 14, 2009).

90. *Id.* at 905 (citation omitted).

91. *Quon*, 2009 WL 1146443.

limited types of non-content information: the IP address, to/from address for e-mails, and volume sent from the account. At the same time, *Forrester*, *Quon*, the basic holding of *Warshak*, and the cases on compelling name and address information are consistent with the content/non-content distinction.

D. *The Presumption that Contents of Communications Receive Fourth Amendment Protection*

Although the case law applying the Fourth Amendment to the Internet remains sparse, most of the cases correctly track the content/non-content line. These cases should be confirmed and expanded. They reflect an essential underlying dynamic of the switch from the physical world to the network environment. Non-content information in a network context is the rough functional equivalent of outside information in a physical context, and content information in a network context is the functional equivalent of inside information in a physical context. To apply the Fourth Amendment to the Internet and computer communications networks in a technology-neutral way, courts should adopt the content/non-content distinction as a replacement for the traditional inside/outside distinction.

This distinction should apply broadly to the contents of network communications, not just to e-mail. The Fourth Amendment should generally protect the contents of communications stored in "the cloud" of the Internet, including remotely stored files maintained on a server that is hosted for individual users. Similarly, the Fourth Amendment should ordinarily protect remotely stored text messages such as those at issue in *Quon*, the case presently before the Supreme Court. The text messages are contents, the functional equivalent of the text of a letter or the contents of a phone call. Such communications should ordinarily receive protection for the same reasons that the contents of any other communications sent over modern communications networks should be protected.[92]

Two important clarifications are in order. First, I recognize I have not given a detailed explanation of what counts as content and non-content information. Every different Internet application generates its own data, and lines must be drawn to distinguish content from non-content for each. Some

92. This does not mean that the Court should affirm the Ninth Circuit's decision in *Quon*, however. After correctly concluding that the text messages should ordinarily receive protection, the Ninth Circuit held that this expectation of privacy was not defeated by notice from the employer that no such privacy rights existed. *See Quon*, 529 F.3d at 906-08. As Judge Ikuta explained in her dissent from denial of rehearing en banc, this aspect of the *Quon* decision is difficult to square with precedents on public employee privacy rights. *See* Quon v. Arch Wireless Operating Co., 554 F.3d 769, 774-79 (9th Cir. 2009) (Ikuta, J., dissenting from denial of rehearing en banc). *See also infra* notes 96-100 and accompanying text.

cases are difficult,[93] and the best way to draw the content/non-content line in contested cases such as website uniform resource locators (URLs) is beyond the scope of this Article. However, many cases are clear. In the case of e-mail, for example, the subject line, the body of the message, and any attachments count as the contents of the communication. They are the actual message to be sent. Everything else in the e-mail, including the to/from address and the size of the e-mail, counts as non-content information. Internet IP headers provide another easy case.[94] Computers generate IP headers to deliver Internet communications, and most Internet users remain blissfully unaware of their existence.[95] The headers are therefore non-content information rather than the contents of communications. Other examples may be more difficult, but these important cases are straightforward.

Second, I must emphasize that this approach does *not* mean that all contents are protected on the Internet any more than all things indoors are protected in the physical world. Rather, my approach offers a presumption: protection exists barring special circumstances in which protection is waived. While contents of communications are ordinarily protected, that protection ends when contents are purposefully exposed. This is the same rule that applies in the physical world: if a store owner opens his store to the public, the material inside that is available to the public is no longer protected even though it is inside.[96] By analogy, someone who posts contents to the Internet that are available to the public waives any privacy rights in those contents. The analogy between physical and virtual holds, resulting in technological neutrality between the physical world and the Internet.

Because many people use the Internet to communicate with large groups, the presumption will be overcome in many cases online. For example, if an Internet user posts information on a public web page that is available to the public, the information will be unprotected.[97] If a person shares files with others on a network, the sharing ordinarily will waive the individual's

93. The most difficult and most discussed case is the URL of addresses on the World Wide Web. For a discussion of these difficulties, see Kerr, *supra* note 41, at 645-48; see also Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009).

94. Kerr, *supra* note 41, at 614-15.

95. *See id.*

96. *See* Maryland v. Macon, 472 U.S. 463, 469 (1985) ("[R]espondent did not have any reasonable expectation of privacy in areas of the store where the public was invited to enter and to transact business. . . . The officer's action in entering the bookstore and examining the wares that were intentionally exposed to all who frequent the place of business did not infringe a legitimate expectation of privacy and hence did not constitute a search within the meaning of the Fourth Amendment.").

97. *See* United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002) (concluding that a person has no Fourth Amendment rights in a photograph posted to the public on the World Wide Web).

reasonable expectation of privacy in the shared data.[98] Similarly, if a person posts a message to a large group, but a member of that group is a confidential informant, the informant can read the message and relay it to the police without violating the Fourth Amendment.[99] Terms of Service may have a role in defining Fourth Amendment rights as well, although I believe their role is in determining whether a user has consented or given the provider third-party consent rights, not whether the provisions in a Terms of Service eliminate a reasonable expectation of privacy.[100] The broader point is that content protection online is only a presumption: special circumstances can waive that protection just as special circumstances can waive the inside protections that apply in physical space.

E. *Addressing Three Important Objections*

Critics of the content/non-content line might make three basic objections to its embrace in the Internet setting. The first argument is that the ease and intrusiveness of outside surveillance in the physical world is sufficiently different from the ease and intrusiveness of non-content surveillance online that it merits different legal treatment. The second argument is that the line between content and non-content information is sufficiently blurry in the online setting that it no longer provides a useful doctrinal distinction. The third argument is that the content/non-content distinction does not faithfully apply the "reasonable expectation of privacy" test. I will consider these three arguments in turn.

---

98. *See* United States v. King, 509 F.3d 1338 (11th Cir. 2007) (posting on an open computer network).

99. *Cf.* Hoffa v. United States, 385 U.S. 293, 300-03 (1966). Further, if the location of the posting is considered the destination of the message, Fourth Amendment rights may be eliminated much like the Fourth Amendment protection enjoyed by the sender of a letter ends after the message is delivered. *See also* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (noting that a sender's expectation of privacy in a letter "terminate[s] upon delivery").

100. The breach of Terms of Service should not eliminate a reasonable expectation of privacy in an Internet account for the same reasons that the breach of a rental agreement in an apartment does not itself eliminate a tenant's reasonable expectation of privacy. *See* United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009) (noting that a landlord's authority to evict a tenant for violating the terms of the lease "cannot of itself deprive that person of an objectively reasonable expectation of privacy" in his apartment). However, agreeing to Terms of Service may in some cases confer rights on the provider to access the contents of the account or consent to a law enforcement search. *Cf.* United States v. Ziegler, 474 F.3d 1184, 1191-92 (9th Cir. 2007) (holding that an employee had a reasonable expectation of privacy in the contents of his workplace computer but that the company's right to access the machine conferred a right to consent to a government search of the computer). The difference between elimination of a reasonable expectation of privacy and consent can be an important one because consent is bounded by the scope of consent whereas elimination of a reasonable expectation of privacy eliminates all Fourth Amendment rights in the information.

1. *The "Internet is different" argument*

The argument that the ease and intrusiveness of outside surveillance is different from non-content surveillance runs as follows.[101] Non-content Internet surveillance is cheaper, easier, and more invasive than outside physical surveillance. Physical surveillance is normally conducted by human beings, and human beings are both expensive and imperfect: the government can't possibly watch everyone all the time, so public surveillance is necessarily limited in scope. Such limits don't exist in the Internet setting: the government can tap into the Internet anywhere, at anytime, with little to no cost and it can copy everything. It can also data mine what it collects, creating a comprehensive picture. As a result, non-content Internet surveillance is likely to be more invasive and all-encompassing enough to justify different Fourth Amendment rules.[102]

I find this position unpersuasive for three reasons. First, even if the content/non-content line isn't perfect, it does provide a useful line between protected and unprotected communications. *Some* line is needed. The content/non-content distinction may not draw the line perfectly, but it does so reasonably adequately: it draws the line accurately in most cases. Given the need for administrable Fourth Amendment rules that the government can apply ex ante,[103] the content/non-content distinction may be the best line even if it does not account ideally for all of the possible ways the government could abuse non-content surveillance. Critics might answer this question: if the content/non-content line is inadequate, what other line is superior? What precisely are the realistic alternatives?

Second, I am not convinced that online non-content surveillance is always or even generally easier, cheaper, and more invasive than physical outside surveillance. Online surveillance varies greatly in its ease, cost, and invasiveness: it can be cheap, easy, and highly invasive, or it can be expensive, difficult, and much less invasive than physical surveillance. For example, the government must go through a third party to conduct online surveillance, whereas it can conduct physical surveillance itself. That requires the

101. Examples of scholarship making such arguments, either implicitly or explicitly, include Palfrey, *supra* note 5; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2-7 (2004); and CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

102. *See, e.g.*, SOLOVE, *supra* note 101.

103. *See generally* New York v. Belton, 453 U.S. 454, 458 (1981) ("A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be literally impossible of application by the officer in the field. . . . [A] single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront." (citation and internal quotation marks omitted)).

cooperation of a third party, usually a business, and that business can both insist on a court order and demand that the expenses of surveillance be paid.[104] Further, Internet criminals can use encryption, proxy servers, and other tools to hide their conduct from surveillance: this will often make Internet surveillance more difficult than analogous physical surveillance, as physical disguises are not nearly as difficult to defeat.

Part of the difficulty is that the "Internet is different" argument employs a somewhat limited concept of physical outside surveillance. Outside surveillance can be highly invasive. It allows a government agent to watch a person and where he goes, monitoring his appearance, location, and his day-to-day life nonstop. Video cameras have also made physical surveillance more invasive than before, as the presence and use of closed-circuit television often allows government agents to watch a suspect's every step. The image of physical surveillance being an officer on the street with a trench coat, fedora, and sunglasses peeking out over the morning newspaper to see what the suspect is doing is deeply ingrained, but modern physical surveillance technologies have rendered it somewhat outdated. As a result, I am not convinced that a clear distinction exists between the ease and cost of non-content Internet surveillance and outside physical surveillance.

Third, the kind of differences that may exist between outside surveillance and non-content Internet surveillance are best handled by statutory protections rather than constitutional ones. These sorts of differences are differences in degree, not differences in kind. They rest on fluid practical judgments about the likely impact of a type of surveillance that may fluctuate as technology shifts. These are exactly the kinds of differences that statutes can address, as statutory protections can be more fluid and offer specific levels of protection tailored to the sense of a particular privacy threat.[105] The existing Pen Register statute[106] and Stored Communications Act[107] provide a good example. They *already* require the government to obtain a statutory court order to order an ISP to conduct monitoring even without Fourth Amendment protection.[108] These statutes could be amended to bolster privacy protections, as I have argued elsewhere,[109] but the general effort to address non-content Internet surveillance

104. *See* 18 U.S.C. § 2706 (2006) (providing a means for cost reimbursement for ISPs ordered to comply with court orders for the disclosure of customer records).

105. *See generally* Kerr, *supra* note 32, at 864-82 (arguing that legislatures have institutional advantages over courts in protecting privacy in changing technology).

106. 18 U.S.C. §§ 3121-3127 (2006).

107. The Stored Communications Act of 1986, 18 U.S.C. §§ 2701-2711 (2006).

108. *See* 18 U.S.C.A. § 2703(c) (West 2009) (requiring an order to obtain access to stored materials); 18 U.S.C. § 3121 (2006) (regulating access to non-content information in real-time).

109. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233-35 (2004) (arguing in favor of enhanced protections under the Stored Communications Act); *see also* Kerr, *supra* note 41, at 639 (arguing that the Pen Register statute standard should be raised to reasonable

through statutes strikes me as a sound one.

I don't mean to dismiss the concerns about the broad surveillance that computers enable. These are very real concerns and should be taken very seriously. But the Fourth Amendment has traditionally regulated the role of the state as it relates to individuals, not the role of the state as it relates to society as a whole. Fourth Amendment rights are personal: each person can only seek redress of their own rights, not the rights of others.[110] Concerns of total surveillance generally raise the fear that computers may allow the government to assume a new relationship vis-à-vis its citizens: technology may allow the state to watch all of its citizens instead of just a few.[111] As much as I would oppose such a development, the Fourth Amendment doesn't provide the tools to stop it. As the Supreme Court emphasized in *Katz v. United States*,[112] the Fourth Amendment "cannot be translated into a general constitutional right to privacy. . . . [T]he protection of a person's *general* right to privacy—his right to be let alone by other people—is . . . left largely" to other sources of law outside the Constitution.[113] That holds in the Internet setting just as much as it did in the case of the telephone in *Katz*.

2. *The incoherence argument*

A second objection to the approach offered in this Part is that the line between contents and non-content information is incoherent. My colleague Daniel Solove has made this argument most strongly in the statutory context, and his argument runs as follows:[114] First, the notion that contents are private and non-contents are non-private is inaccurate. It often happens that content information has low privacy and that non-content information has a great deal of privacy stakes.[115] Relatedly, it can be difficult to distinguish between contents and non-content information in some cases, such as with Internet addresses that point to specific stories or include search query terms. Because the line can be difficult and doesn't always map accurately, some other distinction is needed.[116]

The problem with this argument is that it applies equally to the traditional distinction between inside and outside surveillance. Like the content/non-content line, the inside/outside distinction does not map perfectly between

---

suspicion).

110. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 139-40 (1978).

111. *Cf.* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

112. 389 U.S. 347 (1967).

113. *Id.* at 350-51 (citation and internal quotation marks omitted).

114. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1286-88 (2004).

115. *See id.* at 1288.

116. *See id.*

private and non-private. Outside surveillance can reveal very personal information, and inside surveillance can be non-invasive. For example, outside surveillance that observes a visit to a doctor specializing in treatment of a particular disease can suggest a specific medical condition. On the other hand, surveillance inside a home might reveal only a public newspaper on the kitchen table.[117] Much like with the line between content and non-content, the line between inside and outside does not track privacy interests every time.[118] It usually works, however, and that is generally considered enough.

Similarly, the difficulty in distinguishing between content and non-content resembles the difficulties distinguishing between inside and outside. The difficult line between outside and inside has produced many of the Supreme Court's most tricky and controversial Fourth Amendment precedents. For example, in *Kyllo v. United States*,[119] the FBI directed an infrared thermal imaging device at a suspect's home to determine if the exterior wall of the home was unusually hot, a signal that marijuana growing lamps were in use inside. The Supreme Court divided 5-4 on whether the thermal imaging device constituted inside surveillance or outside surveillance.[120] In his majority opinion, Justice Scalia characterized the thermal imaging device as a tool that monitored the temperature *inside* of the home. By obtaining information about the inside of the home, the device triggered the Fourth Amendment.[121] In his dissent, Justice Stevens considered the thermal imaging device to be a tool that merely reflected signals off the *outside* of the home. Because it only revealed information about the outside of the home, it did not trigger the Fourth Amendment.[122] The two opinions diverged on the difficult question of whether to construe infrared imaging as outside surveillance or inside surveillance.

The difficulty distinguishing between inside surveillance and outside surveillance also explains the Supreme Court's cases on hidden electronic locating devices, *United States v. Karo*[123] and *United States v. Knotts*.[124] These cases concluded that use of such devices to determine the location of an

---

117. *See* Arizona v. Hicks, 480 U.S. 321 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

118. Indeed, this is simply a matter of everyday experience.

119. 533 U.S. 27 (2001).

120. *See id.* at 31.

121. *Id.* at 35 n.2. According to Justice Scalia:

> The dissent's repeated assertion that the thermal imaging did not obtain information regarding the interior of the home is simply inaccurate. A thermal imager reveals the relative heat of various rooms in the home. The dissent may not find that information particularly private or important, but there is no basis for saying it is not information regarding the interior of the home.

Id. (citations omitted).

122. *Id.* at 42 (Stevens, J., dissenting) ("[T]his case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home.").

123. 468 U.S. 705 (1984).

124. 460 U.S. 276 (1983).

item inside a home was inside surveillance covered by the Fourth Amendment,[125] but that the use of such devices to determine the location of an item that is outside was outside surveillance that the Fourth Amendment does not protect.[126] In other words, the classification hinged on where the device was located, and thus whether the government learned of facts from inside or from outside. As with *Kyllo*, the sharp disputes in the case depended on whether the surveillance was classified as outside or inside.

Even many difficult "low-tech" cases hinge on the difficult line between inside surveillance and outside surveillance. Imagine a police officer is standing in a public street near the entrance of a suspect's home, and he decides to approach the home to look for clues. He may want to look through open windows, or he may wish to see if there is any mail in the mail slot. He may want to look in the foyer, or in the bushes near the entrance to the home. Is such surveillance "inside," on the theory that it is near enough to the home? Or is it "outside," on the theory that the police have not actually entered inside? These sorts of questions have long occupied the courts, leading to difficult doctrines like the murky four-factor test on the distinction between "open fields" and "curtilage."[127] No easy answers have emerged, even though such simple facts have been around for a century and pop up repeatedly in the cases.[128]

As these cases suggest, the line between inside surveillance and outside surveillance can be surprisingly difficult to draw. Some easy cases exist, but others are quite difficult. And yet no one suggests that the difficult cases prove that there is no real distinction between inside and outside, or that the distinction is incoherent and must be abandoned. Rather, these examples

---

125. *See Karo*, 468 U.S. at 712.

126. *See Knotts*, 460 U.S. at 282.

127. *See* United States v. Dunn, 480 U.S. 294 (1987) (offering a four-part test to distinguish open fields not protected by the Fourth Amendment from curtilage—areas very close to homes—that are). According to the Court:

> [C]urtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by. We do not suggest that combining these factors produces a finely tuned formula that, when mechanically applied, yields a "correct" answer to all extent-of-curtilage questions. Rather, these factors are useful analytical tools only to the degree that, in any given case, they bear upon the centrally relevant consideration—whether the area in question is so intimately tied to the home itself that it should be placed under the home's "umbrella" of Fourth Amendment protection.

Id. at 301 (citations omitted). Needless to say, this murky four-factor test offers little clarity in distinguishing outside from inside for Fourth Amendment purposes.

128. For example, even today courts struggle with issues such as whether the police can open screen doors when they walk up to a house with a suspect inside. *See, e.g.*, United States v. Arellano-Ochoa, 461 F.3d 1142, 1145 (9th Cir. 2006). The existence of this "Screen Door Jurisprudence" further emphasizes that the line between inside and outside can be quite complicated even in traditional circumstances.

demonstrate that there will be close line-drawing cases even for such a core Fourth Amendment distinction. In my view, the same goes for the distinction between content and non-content Internet communications. True, there are difficult cases: if courts adopt the content/non-content distinction, we can expect courts to struggle with some cases much like they have struggled with the distinction between inside and outside with physical space.[129] But the existence of difficult cases does not provide a reason that that the distinction should not be drawn.

3. *Reasonable expectations of privacy and the content/non-content line*

A third objection to my approach is that it does not faithfully apply the reasonable expectation of privacy test.[130] Some might argue that the line between content and non-content information doesn't necessarily track user expectations. Most Internet users expect privacy in both their content and non-content information, and generally do not distinguish between them. Because such widely shared understandings are reasonable, courts should recognize privacy rights in both content and non-content information. Others might argue that my approach ignores the Fourth Amendment's third-party doctrine, which holds that a person does not retain a reasonable expectation of privacy in information disclosed to a third party.[131] An Internet user discloses both content and non-content information together to third-party network providers. As a result, neither should be protected. Although these two arguments generate opposite results, they each question the content/non-content distinction based on whether it faithfully applies the "reasonable expectation of privacy" test.

The difficulty with the first version of this argument is that the "reasonable expectation of privacy" test does not simply mirror widely shared social expectations. As I have explained elsewhere, the phrase "reasonable expectation of privacy" is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment.[132] When the Justices of the Supreme Court conclude that a law enforcement practice must be regulated under the Fourth Amendment, they announce that the defendant's expectation of privacy

129. For example, courts conceivably could apply the concept of "curtilage" to Internet communications on the theory that some information that is technically non-content permits the identification of contents and thus should be treated as content.

130. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

131. *See, e.g.*, *In re* Search Warrant for Contents of Elec. Mail, 665 F.Supp.2d 1210 (D. Or. 2009) (discussing the third-party doctrine and noting that e-mail users "voluntarily conveyed to the ISPs and exposed to the ISP's employees in the ordinary course of business the contents of their e-mails").

132. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 531-32 (2007).

is reasonable; when they decide that the practice need not be regulated, they announce that no reasonable expectation of privacy exists.[133] As a result, asking what privacy most Internet users expect does not accurately represent the *Katz* test. The Fourth Amendment ensures against normatively unreasonable police practices, not surprises.

This is fortunate given that notions of privacy online remain in their infancy. When technology is new, social understandings remain contingent: we might initially misunderstand the new technology and misconstrue or diverge on its privacy implications. Some people believe Scott McNealy's famous remark that when it comes to the Internet, "You have no privacy. Get over it."[134] Others see the Internet as a vast sea of privacy, in which they can conduct their most private affairs in near perfect anonymity. These personal conclusions follow from our very limited experiences and attitudes with a new technology that is still developing rapidly. At this early stage in the Internet's history, courts should not try to pick from the emerging social attitudes and impose a rule that will apply to the Internet indefinitely.

The claim that rights in the contents of communications should be waived under the third-party doctrine does not work because the same argument could be made about telephone calls and postal letters. A person who makes a telephone call discloses the contents of the call to the phone company: the electrical signal travels by wire to the phone company and the phone company routes the call to its destination. *Katz* established that the third-party doctrine does not apply in that setting. The Supreme Court has never explicitly stated why the third-party doctrine should not apply in that setting, although I have written elsewhere why I think that judgment is correct.[135] But the key point is that the third-party doctrine has not been extended to intermediaries that merely send and receive contents without needing to access or analyze those communications. Instead, courts have widely adopted the content/non-content line or a functional equivalent in cases applying the Fourth Amendment to communications networks.[136] The deep roots of the content/non-content distinction in cases applying the Fourth Amendment to earlier communications networks suggests that it should not be out of place in the setting of the Internet.

III. FOURTH AMENDMENT RULES FOR PROTECTED INTERNET DATA

With the basic distinction between content and non-content

133. *See id.* at 504-05.

134. *On the Record: Scott McNealy*, S.F. CHRON., Sept. 14, 2003, at I-1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/09/14/BU141353.DTL&type=business.

135. *See* Kerr, *supra* note 22, at 581 (arguing that *Katz* was correctly decided because the contents of communications do not create substitution effects).

136. *See supra* Part II.C.

communications in place, the next issue is how much protection the Fourth Amendment should extend to the contents of communications. First, if the Fourth Amendment protects the contents of communications, exactly what kind of protection does it offer? Does the Fourth Amendment require a warrant, or do Internet applications justify different treatment, like a probable cause requirement without a warrant? And second, if a warrant is required, how much authority should a warrant provide? Should a warrant allow a narrow search or a broad one? Should a warrant for Internet communications be limited to a single account hosted by a single provider, or should it allow for searches through multiple accounts, and if so, how many?[137]

This Part begins by arguing that the Fourth Amendment ordinarily requires a warrant for the collection of the contents of Internet communications. The Internet should not trigger a lower standard such as that found with the automobile exception. Contents stored in and transferred through Internet accounts should be protected with the same default warrant requirement that is required for access to homes, telephone calls, and postal letters. Further, the Fourth Amendment should require a narrow exception permitting the warrantless copying of data pending a warrant. Such a power would mirror similar authority to temporarily detain a package pending a warrant to open it, and would allow for a warrant requirement for access to contents of communications. Under my proposed framework, the federal privacy statute that permits the government to compel access to stored files without a warrant is unconstitutional in many of its applications.

This Part then argues that the particularity requirement should allow searches of multiple accounts with multiple providers used by the same criminal suspect instead of requiring separate warrants with separate probable cause for every individual account. The multiplicity of services in the Internet setting should lead the particularity requirement to allow one warrant for multiple accounts, much like the statutory roving wiretap authority allows one warrant for multiple telephones in the traditional telephone setting.[138] Put another way, the particularity requirement of Fourth Amendment law should be applied so the basic building block of particularity in the online environment is a specific Internet user, not a specific account or physical device.

---

137. There is a third issue that this question raises: if the Fourth Amendment ordinarily protects the contents of communications, in what circumstances are expectations to privacy in those contents waived? As a doctrinal matter, this issue should arise often in applications of the third-party consent doctrine. In particular, in what circumstances does an ISP have "common authority" over the user's files such that they can access the suspect's files at the government's request? *Compare* Stoner v. California, 376 U.S. 483, 490 (1964) (holding that a hotel clerk lacked the authority to consent to the search of a hotel room), *with* United States v. Gargiso, 456 F.2d 584, 586-87 (2d Cir. 1972) (holding that the vice president of a company who shared supervisory power over the basement with the employee could consent to the agents' search of that area for evidence of the employee's criminal activity). Such issues must be left for another day.

138. *See infra* notes 177-179 and accompanying text.

A. *Applying the Warrant Requirement to Internet Communications*

The first question to be considered is what kind of Fourth Amendment protection should apply to the contents of Internet communications. Although Fourth Amendment cases often speak of a default warrant requirement,[139] and of different rules as "exceptions" to the warrant requirement,[140] the exceptions are so common that defaults are somewhat hard to identify.[141] The warrant requirement ordinarily applies to searches of homes and of letters and packages.[142] But the Supreme Court has carved out different rules in other cases involving new technologies, and it is necessary to ask whether those different rules justify different treatment for Internet communications.

The key question is whether Internet communications should receive treatment similar to automobiles and ships, two other historical methods of transporting property and communications. In the First Congress, statutory law introduced the idea (that the courts later adopted) that no warrant was required to board and search shipping vessels.[143] In 1925, in *Carroll v. United States*, the Supreme Court expanded this rule to automobiles.[144] Carroll was traveling in his Oldsmobile Roadster on a highway between Grand Rapids and Detroit when he passed by federal Prohibition agents who were on the lookout for his car. The agents had reason to believe that Carroll was running illegal alcohol, and they caught up with him, stopped him, and searched the car. Behind the seat upholstery they found sixty-eight bottles of whiskey and gin.[145]

Chief Justice Taft made two arguments for why the search of the car without a warrant was reasonable. The first argument was originalist: the First Congress had authorized the warrantless search or seizure of naval ships and vessels to search for contraband, indicating that "goods in course of transportation and concealed in a movable vessel" were understood to be different than searches of homes that required a warrant.[146] This reflected a general sense the Framers must have shared that searching movable vessels was reasonable without a warrant, and that rule presumably would apply to cars as

---

139. *See, e.g.*, Thompson v. Louisiana, 469 U.S. 17, 20 (1984) (per curiam) ("[W]e have consistently reaffirmed our understanding that in all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate between the police and the 'persons, houses, papers, and effects' of citizens.").

140. *See id.* at 21.

141. *See* Groh v. Ramirez, 540 U.S. 551, 572-73 (2004) (Thomas, J., dissenting) ("[O]ur cases stand for the illuminating proposition that warrantless searches are *per se* unreasonable, except, of course, when they are not.").

142. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877).

143. *See* Carroll v. United States, 267 U.S. 132, 151-53 (1925) (discussing early legislation).

144. *Id.* at 153.

145. *Id.* at 134-36.

146. *Id.* at 151.

well as ships.[147] The second argument was functional: it would be impracticable to require a warrant given that an automobile could be moved while the warrant was being obtained.[148] This did not mean that no cause at all was required to search a car: such a rule would be "intolerable and unreasonable" because those "entitled to use the public highways have a right to free passage" unless there was cause to believe otherwise.[149] Rather, the probable cause requirement used in the statutes on government searches of ships should apply as a constitutional matter to car searches: such a rule was consistent with Fourth Amendment guarantees by requiring a warrant if practicable but no warrant where it was not.[150]

Under the so-called "automobile exception," subsequently made a fixture of Fourth Amendment law,[151] probable cause to believe that evidence or contraband is inside a car justifies an immediate search of the car without a warrant.[152] The fact that a car can be moved creates a sort of exigent circumstance justifying a warrantless automobile search. Like automobiles, computer data can be moved: data can be zipped around the world in a split second. Does this mean that there should be an Internet exception to the Fourth Amendment modeled on the automobile exception?

The answer is "no." The reason is that computer data moves in a very different sense than automobiles or ships move. When cars move, they disappear: the officer who leaves a car alone to go get a warrant will find that the car is gone by the time he returns. Computer data moves in a different way. First, the data don't so much move as get copied. When a file is transferred from one place to another, a new copy is generated and that new copy is sent to the new place. The old copy is ordinarily left behind. Further, when a copy is made, that copy can be controlled and protected from interference.

These differences mean that the government does not need to keep an eye on data to make sure it stays put. Instead, it can copy the data—or order a copy to be made by the server that hosts the data—and then access the copy at a later time.[153] The data can be held until a warrant is later obtained. As a result, there is no general exigency that justifies a rule that the government can access Internet communications without a warrant. At most, the exigency should

147. *Id.* at 151-53.

148. *Id.* at 153.

149. *Id.* at 153-54.

150. *Id.* at 156.

151. *See* Roger Roots, *Are Cops Constitutional?*, 11 SETON HALL CONST. L.J. 685, 746 n.391 (2001) (noting that "the 'automobile exception' has been a fixture of Fourth Amendment jurisprudence").

152. *See* California v. Acevedo, 500 U.S. 565, 580 (1991).

153. This occurred in *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001), an unusual case in which the target had left his hacker tools on a server in Russia. FBI agents in the United States remotely accessed the account, copied the folder containing the tools, and downloaded it to a file in the United States. However, the agents did not actually open the file until they had obtained a warrant. *Id.* at *1.

permit the government either to make a copy of the data and store it until a warrant is obtained or else to order a third party like an ISP to do so and hold the data pending a warrant.[154] The Supreme Court has interpreted the Fourth Amendment to allow an analogous power to temporarily detain a package sent through the mail while a warrant is obtained allowing its opening.[155] So long as the police move quickly to obtain a warrant, the temporary seizure of the package is constitutionally reasonable without a warrant. The same rule should apply to Internet communications. So long as investigators move quickly to obtain a warrant, they should be allowed to run off a copy of the data without a warrant but then not actually observe the data until a warrant is obtained.[156]

Notably, existing doctrine from the telephone setting also supports a warrant requirement for Internet communications. The key passage is the often-ignored second holding of *Katz v. United States*.[157] *Katz* is famous for holding that the Fourth Amendment applies to the bugging of a public telephone booth when it is in use. But after making that ruling, Justice Stewart's opinion then reached the question of whether a warrant was actually necessary.[158] The government argued that its telephone surveillance was entitled to an exception to the warrant requirement: because the officers could have obtained a valid warrant, the fact that no warrant was obtained should not be held against them.[159] The Supreme Court disagreed, reasoning that the warrant requirement does "not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth."[160] The warrant requirement ensured that the requirements of the Fourth Amendment were checked by judges, not by the police themselves:

> Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored "the procedure of antecedent justification . . . that is central to the Fourth Amendment," a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.[161]

This explanation is notably cryptic. It fails to explain the level of generality needed to identify what "kind" of electronic surveillance was "involved" in that case. But even so, it is difficult to articulate why collection of Internet communications might justify treatment different from audio bugging of a

154. *Cf.* 18 U.S.C.A. § 2703(f)(1) (West 2009) ("A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.").

155. *See* United States v. Van Leeuwen, 397 U.S. 249, 252-53 (1970).

156. *See Gorshkov*, 2001 WL 1024026, at *4.

157. 389 U.S. 347 (1967).

158. *See id.* at 354 ("The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards.").

159. *See id.* at 354-56.

160. *Id.* at 359.

161. *Id.*

telephone booth. The Supreme Court's forceful rejection of a warrant exception for telephone bugging seems to extend naturally to the Internet.

B. *The Unconstititionality of 18 U.S.C. § 2703(b)*

My approach has an important consequence for the constitutionality of the federal privacy statutes. It renders unconstitutional an important statute, codified at 18 U.S.C. § 2703(b), that permits the government to obtain the contents of some remotely stored Internet files with less process than a warrant.[162] Section 2703(b) was enacted in 1986 as part of the Stored Communications Act to provide privacy protection for e-mail and other remotely stored Internet files.[163] At the time, Congress had little idea of how the Fourth Amendment might apply to the Internet. Acting amidst this uncertainty, it crafted a statute that allowed the government to obtain the contents of some remotely stored Internet files with either a subpoena or a special court order based on specific and articulable facts.[164] Still on the books today, the provision allows a provider to disclose e-mail to the government without probable cause if that e-mail has been stored for more than 180 days.[165] It also allows a provider to disclose the contents of an account used for remote storage, such as those popular with cloud computing, without a warrant.[166]

Under my approach, this provision is unconstitutional in many of its applications. The Fourth Amendment ordinarily protects the contents of e-mail accounts and remotely stored files and will require a warrant before the government can access those contents. Permitting the government to compel contents with less process than a warrant therefore violates the Fourth Amendment. In specific situations where the contents are not protected by the Fourth Amendment, the statute can be used: because the Fourth Amendment will not apply, no constitutional bar exists to using less process than a warrant.

---

162. 18 U.S.C.A. § 2703(b) (West 2009) states in relevant part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . .
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

163. *See* 18 U.S.C.A. §§ 2701-2711. I have written at length about the Stored Communications Act. *See* Kerr, *supra* note 109.

164. 18 U.S.C.A. § 2703(b), (d).

165. *See id.* § 2703(a).

166. *See id.* § 2703(b).

In the routine case, however, § 2703(b) is unconstitutional.

This conclusion holds despite the lower "reasonableness" Fourth Amendment standard that regulates subpoenas.[167] Subpoenas do not require probable cause,[168] raising the prospect that the government might circumvent the warrant requirement by serving a subpoena on the third-party provider. In my view, this possibility alters the timing of the warrant requirement but does not provide a way around it. The reason is that the Fourth Amendment protects the electronic copy of the contents of the communications made pursuant to a subpoena. Third-party Internet providers ordinarily respond to a government subpoena for electronic files by sending the government a computer disk containing the contents described in the subpoena.[169] That data retains its Fourth Amendment protection: it is no different from a copy of electronic files copied from the target's own home computer. Thus the government may not need probable cause to get a copy of the contents, but it would need a warrant to access and search the contents for evidence.[170] Either way, the Fourth Amendment requires a warrant for the provider to disclose the contents to the government.

C. *Particularity for Internet Communications*

Having concluded that the Fourth Amendment will normally require a warrant to collect the contents of person-to-person Internet communications, the next question is how particular such warrants must be. The Fourth Amendment states that warrants must particularly describe the place to be searched and the persons or things to be seized,[171] a requirement that helps

---

167. *See* William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 857-58 (2001) ("[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable." (citation omitted)).

168. *See id.*

169. For an example of this process, see United States v. Bach, 310 F.3d 1063, 1065 (8th Cir. 2002).

170. *Cf.* United States v. Barr, 605 F. Supp. 114, 116-19 (S.D.N.Y. 1985) (rejecting a probable cause standard for a government subpoena to obtain mail from a third-party service for the suspect's undelivered mail, but noting that the government obtained a probable cause search warrant to open the mail). The more difficult case arises if the provider responds to a subpoena by printing out the contents in paper form. One possibility is that the stack of paper documents retains the expectation of privacy, such that the subsequent searching through the stack by law enforcement is a search requiring a warrant just like searching through the electronic documents. An alternative approach would consider whether a provider can legitimately respond to a third-party subpoena by searching through the documents and printing them out, effectively searching them under the subpoena authority. Whatever the proper resolution of these difficult questions, the straightforward case is the more common practice of responding with an electronic disk containing the documents.

171. U.S. CONST. amend. IV.

ensure that warrants are limited in practice. The basic idea is that the government can only go to specific places and look for specific things, and cannot execute a free-ranging "general warrant" such as those at common law that animated the Fourth Amendment's passage.[172] In the physical world, for example, the particularity requirement normally requires a search limited to a specific house or property: the government must have probable cause to believe that specific evidence is on a specific property, and it normally cannot try to aggregate cause over multiple properties or households and search them all.[173]

How should the particularity requirement apply to Internet communications? Unlike physical evidence, electronic data have no inherent limitations on how much can exist, where they can be located, and where they can be stored. In the physical world, physicality limits scale, and the particularity requirement is based on that scale. But the Internet is different: a suspect could have hundreds of Internet accounts, could store evidence in any or all of them, the accounts could be anywhere, and there are essentially no limits on how large the accounts might be. Does the particularity requirement require the government to get a different warrant for each account? Does it require the government to name the specific Internet accounts to be obtained? Or should the particularity requirement allow the government to get a warrant for a specific person, and to search the Internet accounts known to be used by that person? Put another way, should the particularity requirement online apply to a specific account, or to any account used by a particular person?

Although these questions may seem technical, they are very important in practice. The particularity requirement determines how far the government can search based on a particular factual predicate.[174] The more the government can search based on a particular factual predicate, the more power the government has to search and the more difficult it is for wrongdoers to hide evidence of crime. On the other hand, the less the government can search, the harder it is for the government to abuse its powers to conduct wide-ranging searches and the easier it is for suspects to keep evidence away from the police. The particularity requirement tries to strike the appropriate balance between too much government power and not enough.[175]

How should the particularity requirement apply to Internet evidence collection? The best answer is that the particularity requirement should apply to

---

172. *See generally* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." (citation omitted)).

173. The general rule is that a warrant for a building that has multiple units must specify the individual unit that is the subject of the search to satisfy the particularity requirement. *See* Jacobs v. City of Chicago, 215 F.3d 758, 767 (7th Cir. 2000).

174. *See Garrison*, 480 U.S. at 84.

175. *Id.*

a particular person rather than a specific account. When the government establishes probable cause to believe that a person has or will use the Internet to store, transmit, or receive specific evidence of criminal activity, any account that the person has or will use—and that therefore might plausibly contain the evidence sought—should be included within the scope of the warrant. In other words, the particularity requirement should apply to Internet users, not Internet accounts.

This approach offers a practical response to the fact that physicality no longer limits scale online. A suspect likely has only one home in the physical world, but can have dozens or even hundreds of Internet accounts. The particularity requirement should not remain beholden to the assumptions of the physical world. If physicality no longer limits scale, the particularity requirement should no longer track physicality. Instead, the law should key itself to the one stable element that remains constant across physical and virtual environments: the criminal suspect himself.

A contrary rule would make it far too easy for wrongdoers to hide evidence from investigators. To see why, imagine that the building block of particularity were a single Internet account. To search a particular account, the government would need probable cause to believe that evidence of crime was located in *that particular account* at that particular time.[176] A criminal might open one thousand Internet accounts, and when he committed his crime, he might randomly pick one of the accounts and send the evidence of the wrongdoing to that one account. If police later learn of the crime, they won't know which of the one thousand accounts contains the evidence. Without that knowledge, however, they will lack probable cause to search any one account. As a result, every account will remain unsearched, even if the police have probable cause to believe that the evidence is *somewhere* in one of the one thousand accounts.

Defining particularity based on the individual rather than the account would nullify this effect. It would block Internet technology from upsetting the traditional function of the particularity requirement. It would block Internet users from hiding evidence by chopping up their online conduct into as many slices as they like, each of which would require its own probable cause for the government to search with a warrant. At the same time, it would stop the government from searching the computers of multiple people who happen to have their data stored on the same physical server. In a world in which physicality no longer governs scale, the law would key to the stable criterion of an individual person rather than the arbitrary and easily manipulated standard of either a physical machine or an Internet account.

Fourth Amendment law has encountered a similar dynamic before, and the statutory and constitutional responses provide useful precedents. Consider the example of so-called "roving wiretaps."[177] Decades ago, an individual who

176. *Cf. id.*

177. *See* Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal*

used a telephone to commit crimes usually used a specific phone line. The government could then get a wiretap order for the phone number associated with that telephone line. The advent of disposable cell phones, and the general multiplicity of telephone lines, means that this assumption often is no longer true. A single person might use many phone lines, jumping from number to number, much like an Internet criminal might use many accounts, jumping from account to account. The statutory roving wiretap authority lets the government obtain a wiretap order that permits the government to tap any telephone line that the suspect uses.[178] The order allows wiretapping of the person, rather than wiretapping of the line.[179]

The courts have upheld this authority under the particularity requirement of the Fourth Amendment. For example, in *United States v. Petti*,[180] the Ninth Circuit considered the constitutionality of a roving wiretap allowing the government to wiretap telephones used to engage in a fraud and money laundering conspiracy. The order allowed the government to wiretap all of Petti's calls without specifying which telephone in particular would be tapped. The court concluded that the wiretap order satisfied the particularity requirement because "[o]nly telephone facilities actually used by an identified speaker may be subjected to surveillance"[181] and the surveillance was subject to the usual minimization requirements of wiretapping. Further, the statute only allowed the government to obtain a roving wiretap based on a showing that non-roving surveillance was impossible.[182]

The same principles should allow particularity for Internet searches that specify a particular individual rather than a specific Internet account. In the Internet setting, there are two different kinds of evidence collection: real-time wiretapping, which would be done under the Wiretap Act,[183] and access to stored materials, done pursuant to the Stored Communications Act.[184] The roving wiretap authority should be extended to electronic communications, allowing roving Internet wiretaps; and a search warrant allowing access to stored Internet contents should be permitted to allow (at least where permitted by statute) a search of all of the accounts used by a suspect when probable cause has been established.

Finally, to the extent that this approach raises the concern that it will allow the government to sift through too many of an individual's communications, exposing a suspect's entire world of communications in plain view in a way

---

Regulation of Domestic Law Enforcement Surveillance, 54 HASTINGS L.J. 751, 762-63 (2003).

178. *See* 18 U.S.C. § 2518(11)(a) (2006).

179. *See id.*

180. 973 F.2d 1441 (9th Cir. 1992).

181. *Id.* at 1445 (citation omitted).

182. *Id.*

183. 18 U.S.C.A. §§ 2510-2522 (West 2009).

184. *Id.* §§ 2701-2711.

that threatens to seem like a general warrant, I would incorporate a proposal I have made in the context of stand-alone computers to eliminate the plain view exception for Internet searches.[185] Because searches of computer data are so comprehensive, courts should not admit evidence of crimes found in a search pursuant to an Internet warrant unless the evidence under consideration falls within the scope of the warrant.[186] I have made the case for this rule in depth in the stand-alone environment,[187] and the same arguments apply fully to the case of searches through Internet accounts.[188]

CONCLUSION

Criminal investigations are increasingly moving from the physical world to computer networks. The Fourth Amendment will have to adopt new principles to maintain its longstanding function. The need for evolution is nothing new: the Fourth Amendment will adapt to how wrongdoers use the Internet just as it adapted to how wrongdoers started using postal letters, automobiles, and the telephone. At the same time, the future doctrines of Fourth Amendment law online are likely to be both more complex and more far-reaching than either the postal letter, automobile, or telephone precedents. Postal letters send and receive text from one person to another. Automobiles transport property in trunks and backseats. Telephones send and receive conversations. In contrast, computer networks are entire worlds of activity: they act as jukeboxes, libraries, stores, schools, concerts, private rooms, and hundreds of other services and virtual places. And computer networks seem to provide more and more: every passing year brings another new program, another new service, another new way in which our general-purpose computers add to the virtualization of our environments.

This Article has suggested that Fourth Amendment law should adapt to this new environment in two basic ways. The first way is by recognizing the central importance of the content/non-content distinction, and the second is by applying the warrant requirement with person-based particularity restrictions. This basic framework is not particularly inconsistent with existing doctrine: although existing precedents are tremendously sparse, this Article's

185. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 582-84 (2005).

186. *Id.*

187. *See id.*

188. In addition, courts would need to impose a time limitation on which accounts could be accessed. That is, if the police gain probable cause to believe that a person committed a crime in 2010, the police should not be able to access dormant accounts that could not have played a role in the offense. Exactly how to implement such a principle is quite complicated, however, as it is always at least conceptually possible that a dormant account might have some sort of contents that would be evidence in an offense that occurred much later. For example, a murder in 2010 could be explained by a long-brewing hatred between the murderer and his victim that is illuminated by e-mails from 2003.

conclusions are generally consistent with existing cases or at least reasonably reachable under existing precedents based on other technologies. But the important idea is that it offers a conceptual framework for why those cases and precedents can accurately translate the Fourth Amendment from the physical world to the Internet.

When the Internet ends up as a crime scene, courts will look to the Fourth Amendment to regulate police investigations involving electronic evidence much like they look to the Fourth Amendment to do the same with physical evidence in the physical world. My hope is that this Article will help both courts and scholars to offer a basic framework for the development of the Fourth Amendment in cyberspace that will accurately map the basic principles of the Fourth Amendment from the physical world to the Internet.