Harvard Journal of Law & Technology
Volume 30, Number 1 Fall 2016

IT'S TOO COMPLICATED: HOW THE INTERNET UPENDS *KATZ*, *SMITH*, AND ELECTRONIC SURVEILLANCE LAW

*Steven M. Bellovin, Matt Blaze, Susan Landau, & Stephanie K. Pell**

TABLE OF CONTENTS

---

* Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University. The views expressed are the author's personal views and do not represent the position of Columbia University or any agency of the US government. Matt Blaze is an Associate Professor of Computer and Information Science at University of Pennsylvania. Susan Landau is the Professor of Cybersecurity Policy at Worcester Polytechnic Institute and Visiting Professor, Department of Computer Science, University College London. Stephanie K. Pell is an Assistant Professor and Cyber Ethics Fellow at West Point's Army Cyber Institute and in the Department of English & Philosophy. She is also an Affiliate Scholar at Stanford Law School's Center for Internet & Society. The views expressed are the author's personal views and do not represent the position of West Point, the Army or the US Government.

Authors are listed alphabetically.

The authors would like to thank Susan Freiwald, Stephen Henderson, Orin Kerr, Peter Swire, and participants in the Privacy Law Scholars Conference 2015 workshop of this Article, all of whom provided useful comments on an earlier draft of this paper.

I. INTRODUCTION

For more than forty years, electronic surveillance law in the United States has drawn a strong distinction between the protections afforded to communications "content" and those afforded to the "non-content" — also known as "metadata" — associated with it. The legal framework for surveillance law was developed largely in the context of the mid-twentieth century telephone system, which itself treated content and metadata as cleanly distinct technical concepts. In an era of relative stability in telephone services and technologies, the constitutional and statutory legal principles, once established, were usually straightforward to apply to individual cases, even as the technology incrementally improved.

The Internet, a great disrupter in so many ways, challenges bedrock assumptions on which several principles of modern surveillance law rest. The network's open and dynamic architecture creates a communication environment where an individual unit of data may change its status — from content to non-content or vice versa — as it travels across the Internet's layered structures from sender to recipient. The unstable, transient status of data traversing the Internet is compounded by the fact that the content or non-content status of any individual unit of data may also depend upon where in the network that unit resides when the question is asked. In this digitized, Internet Protocol ("IP")-based communications environment, the once stable legal distinction between content and non-content has steadily eroded to the point of collapse, decimating in its wake any meaningful appli-

cation of the third-party doctrine.[1] Simply put, the world of *Katz*,[2] *Smith*,[3] the corresponding statutes that codify the content/non-content distinction, and the third-party doctrine are no longer capable of accounting for and regulating law enforcement access to data in an IP-mediated communications environment.

This Article examines why and how we now find ourselves bereft of the once reliable support these foundational legal structures provided and demonstrates the urgent need for the development of new rules and principles capable of regulating law enforcement access to Internet communications data.

The physical separation of metadata from message instructs the Court's reasoning in *Ex parte Jackson.*[4] When examining the communication technology of postal correspondence, the Court provided Fourth Amendment protections to the interior matter contained in packages and sealed letters but exempted the "outward form and weight" of the parcels from the umbra of these protections.[5] The physical structure of the letter or package allowed for a clear constitutional rule that separates inner content from outer, publicly exposed, address information.[6]

Fourth Amendment protections for the content of telephone conversations were first recognized in 1967 in *Katz*. Specifically, the Court held that law enforcement's interception of the content of telephone conversations was a search and, accordingly, a warrant authorizing the collection was required.[7] Because *Katz* involved law enforcement collection of telephone conversations through a listening device affixed to the outside of a telephone booth, the Court did not encounter the question of whether constitutional protections should apply to non-content information associated with the content of telephone calls in the possession of a "third party" (such as the telephone company).

That question did not reach the Court until 1979, twelve years after *Katz*. In *Smith v. Maryland*, the Court found that government collection of dialed digits with a pen register device did not constitute a search.[8] The Court reasoned that the information was voluntarily conveyed to a third party (the telephone company, for the purpose of connecting the call) and that, unlike the voice conversations considered in

---

1. For discussion of the third-party doctrine, *see infra* Section II.C.

2. *See generally* Katz v. United States, 389 U.S. 347 (1967). For a discussion of *Katz*, *see infra* Section II.C.

3. *See generally* Smith v. Maryland, 442 U.S. 735 (1979). For a discussion of *Smith, see infra* Section II.C.

4. *See generally Ex parte* Jackson, 96 U.S. 727 (1878).

5. *See id.* at 733.

6. *See id.*

7. *See generally* Katz, 389 U.S. at 347.

8. *See* Smith, 442 U.S. at 745–46.

Katz, dialed digits themselves did not comprise communications content.[9]

By 1979, *Katz* and *Smith* had thus established the foundation of two major tenets of electronic surveillance law: the *content/non-content distinction* and the *third-party doctrine*. Congress first codified these principles in Title III of the Omnibus Crime Control and Safe Streets Act[10] ("Wiretap Act"), providing the strong protections for communications content that exist today; it then followed with the Pen/Trap statute,[11] providing lesser protections for specific kinds of non-content information. These principles were forged, however, during a time when communications technology was synonymous with the use of the wireline telephone and thus, comparatively speaking, were not very complex.[12] Indeed, the architecture of the communications technology itself was not a complicating factor to any constitutional or statutory analysis.

But the simplicity of the telephone network deployed and used at the time of *Smith* was short lived. Not long after *Smith* — and unrelated to the decision — MCI and Sprint sought to offer less expensive residential long-distance service than that provided by AT&T, the monopoly carrier at the time.[13] Until the consent decree and subsequent breakup of AT&T,[14] consumers wishing to use these cheaper services had to dial a local number for their carrier, an account code, and then the actual number desired.[15] This dialing structure meant that some of the dialed numbers were now the content of a call.[16] By the late 1980s, telephones began conveying not just dialing information, but also content of various sorts (e.g., bank account and prescription numbers). The legal distinctions between content and non-content established by *Katz* and *Smith* began to erode.

Since that time, communications technology has grown far more complex. The real challenge, though, arrived with IP-based communications. The telephone, whose system design we briefly discuss in Part III, was developed principally to ensure good voice transmission;

---

9. *See id*.

10. Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, §§ 2510–2520, 82 Stat. 197, 211–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2530 (2012)).

11. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 3121–3126, 100 Stat. 1848, 1868–1873 (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

12. *Id.* The Electronic Communications Privacy Act of 1986 did deal with wireless transmissions, including pagers, and restrictions on access to stored electronic communications. Its sections on Pen/Trap, however, were exclusively focused on the telephony world.

13. *See* PHILIP L. CANTELON, HISTORY OF MCI, 1968-1988: THE EARLY YEARS 291, 293 (1993).

14. *See* United States v. Am. Tel. and Tel. Co., 552 F. Supp. 131 (D.D.C. 1982).

15. *Id.* at 197 ("Long distance calls may presently be placed over the AT&T network by dialing ten or eleven digits while twenty-two or twenty-three digits are necessary to use the facilities of the other interexchange carriers.").

16. To the local carrier, the account number and the actual number to be called were communications content being provided to the alternate carrier.

this constrained the possible design space. Despite a century of high-quality services provided by AT&T, the network did not offer a wide array of services — telephone network design and the lack of competition precluded that possibility.[17]

The Internet is different. From its beginning, the Internet was designed as an open architecture that could run over a wide range of underlying links.[18] Flexibility was inherent in the system design, in which "the choice of any individual network technology . . . [is] not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture.'"[19] One natural consequence of such a malleable network is that it enables — and requires — "end-to-end frameworks," that is, a system in which endpoint applications manage their own functionality because they cannot make strong assumptions about the underlying networks.[20] The end-to-end structure of Internet applications enabled a remarkable blossoming of innovation on the Internet but also brought a new, dynamic communications environment of unprecedented complexity. That complexity is hostile to the stability of communications law generally, but particularly to surveillance: the variety of link types and the multiplicity of operators create an incentive for encryption while complicating governments' task of finding stable places from which to tap.

Our thesis is that the complexity of IP-based communications technology undermines two foundational tenets of surveillance law established by *Katz* and *Smith*. Through examples in a variety of domains, we show that IP-based communications: (1) render content/non-content distinctions functionally meaningless; and (2) make it almost impossible to discover, much less identify, when data is being shared with a third party, thus disrupting application of the third-party doctrine.

We are not the first to recognize that IP-based communications complicate the application and interpretation of communications surveillance law. A number of scholars have asserted that the third-party doctrine is ill-suited to regulate privacy protections in the context of modern communication technologies.[21] Others have questioned how to apply current legal definitions of content and non-content to information such as Uniform Resource Locators ("URLs").[22] This Article

17. *See also infra* Section III.A.

18. Barry M. Leiner et al., *A Brief History of the Internet*, 39 ACM SIGCOMM COMPUTER COMM. REV 24 (2009).

19. *Id.*

20. Jerome H. Saltzer et al., *End-to-end Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS (TOCS) 277, 277–88 (1984).

21. *See infra*, Section II.B.

22. *See infra* Sections II.A & II.B.

looks at the same issues but through a very different lens. Our vantage point is from the ground level of Internet technology itself; by examining the architecture of the Internet and the complexity of IP-based communications, we demonstrate how the *Katz/Smith* distinctions, foundational to forty years of communications surveillance law, are no longer viable. We do not, however, offer a new interpretation of the reasonable expectation of privacy ("REP") test[23] or construct new analogies to the *Katz*/*Smith* distinctions for an IP-based communications environment.

At the time of *Smith*, the phone network connected people around the world, but its user functionality was relatively limited. The Internet allows a far richer set of functionalities — email, web browsing, etc. — with far more complex interfaces. The architecture of the Internet and the derivative complexity of IP-based communication services combine to blur the traditional content/non-content distinction found in US surveillance law. In this Article, we analyze this phenomenon, along with its corresponding effects upon the traditional application of the third-party doctrine, in a rigorous, technologically driven argument.

One issue is "architecture." Modern communication systems often employ vastly different designs from their predecessors, relying on a much more varied and fluid relationship between communicating devices and the services that move the data between them. A second is "position," including position in the network stack. Communications services and applications increasingly rely on models that layer interacting services atop one another.

We introduce the concept of "architectural content" to denote the unexamined transportation of a unit of data between two given points in the network by entities other than the sender and receiver. Here, content is a product of how the network was designed to function as a transport system for application data — that is, how different components of the Internet are intended to communicate with each other.[24] We contrast this form of content with the familiar "communicative content" (as recognized by the Wiretap Act) that is based on the semantic meaning of a communication.[25] These dual but not mutually exclusive forms of content (a given unit of data can simultaneously exist as both architectural and communicative content) are critical concepts for understanding how the legal distinctions between content

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

24. The same concept can be applied to the phone network: the phone company transports voice but does not examine it.

25. *See also infra* Section III.C.

and metadata have become untenable in an IP-based communications environment.[26]

Architectural content at one layer will be architectural metadata at another.[27] Whether something is content thus depends on exactly where in the system the question is being asked. Accordingly, the legal standard governing law enforcement access to information may depend on where that information exists in the system — what may require legal process under a relevance or reasonable suspicion standard at one point in the system may require a probable cause warrant at another. Finally, as the "substance, purport or meaning of [a] communication"[28] becomes increasingly derivable from what we might at first glance be tempted to dismiss as innocuous, unrevealing metadata, the distinction between communicative content and metadata blurs.

We apply the concepts of communicative content, architectural content, and architectural metadata to specific kinds of IP-based communications and protocols. These examples illustrate how the content/non-content distinction and the third-party doctrine generally become unworkable rules in an IP-based communications environment. We show that the addressing information in one protocol — the "From:" in the email "envelope" — may be different from the "From:" that the user sees within the message header, meaning that the latter is architectural content rather than addressing information.[29] URLs also present legal challenges for discerning what is content and what is metadata and, accordingly, what levels of protections are afforded to the various portions of a URL when it is collected in real-time or when it is obtained from stored data. We discuss how communicative content can also be inferred indirectly, such as from ad networks. Finally, we examine mapping services, which provide users with maps, directions, etc. This case study illustrates how information conveyed to the mapping provider is dependent on the architecture of the service and thus essentially opaque to the user. Mapping services provide a clear example of how, in an IP-based communications environment, the concept of a voluntary conveyance under *Smith*[30] is, at best, a legal fiction.

---

26. We note that just because a particular piece of data may be architectural content does not alone determine whether or not the data is afforded Fourth Amendment protections.

27. The definition of "architectural metadata" will be discussed after we have developed the technical background for the concept.

28. 18 U.S.C. § 2510(8) (2012) (from the Wiretap Act's original definition of "contents").

29. This fact has been observed by others as well. *See* Ross Anderson & Stephen J. Murdoch, *What's Next After Anonymity*, SECURITY PROTOCOLS XVI 220–22 (2008) ("Of course a thoughtful boss can write 'Dear Fred, You're fired!' but this is less than optimal as it breaks a level of abstraction. This is a much more common problem than one might think, as a name at one layer in the stack might be an address at the next, and so on.").

30. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

Our analysis of these and other examples leads us to conclude that in an IP-based communications environment:

(1) The concept of metadata, as a category of communication information that is wholly distinguishable from communications content, is outdated;

(2) The traditional physical and legal distinction between content and non-content, which has generally provided a consistent, reliable method for discerning more sensitive or revealing aspects of communication information worthy of Fourth Amendment protections, is too difficult to apply;

(3) The application of traditional content/non-content distinctions leads to inconsistent and anomalous results; and

(4) The general notion that a user "voluntarily convey[s]" information — as contemplated in *Smith*[31] — in the context of a complex, IP-mediated communications environment is an unsustainable legal fiction.

These conclusions suggest that courts will find it increasingly difficult to construe and uphold the two foundational principles of surveillance law that have governed US law over the last forty years. Moreover, this situation foreshadows an unstable set of affairs where courts, without intervening statutory guidance from Congress, will be left to apply the reasonable expectation of privacy test to myriad situations without the benefit of the traditional proxies of the content/non-content distinction and the third-party doctrine.

Let us be clear about what we are not saying. We are not suggesting that it is impossible to draw meaningful privacy-related distinctions between various kinds of communications data in various domains. Rather, we are illustrating how the simple divisions of old are no longer viable in a complex, IP-based communications system. Consider, for example, the coming Internet of Things, in which devices from smart thermostats to pacemakers to tire pressure sensors all communicate over the network.[32] In this all-encompassing networked environment, notification of a communication may be the entirety of the communication — the metadata and the message are one and the same. New rules and principles, freed from the traditional content/non-content distinction and third-party doctrine, are needed to discern more sensitive aspects of communications data in various domains.

---

31. *Id.*

32. *See generally ITU Internet Reports: The Internet of Things*, International Telecommunications Union, November 2005.

Big Data collection and the ready availability of personal data — peoples' GPS locations, Facebook likes,[33] etc. — are now pervasive, even ubiquitous sources of information, most often in the possession of private companies offering consumers all kinds of IP-based services and products. This personal data and information has also become an important tool in criminal and national security investigations, as evidenced by the long and contentious ongoing legislative effort to regulate law enforcement access to location data.[34]

Although certain debates about law enforcement access standards for metadata have been going on for years, the exploration of the legal issues raised in this Article is taking on a new urgency. The increasing availability of encryption tools, including systems that are set by default to encrypt communications end-to-end, has complicated law enforcement's wiretapping practices.[35] According to the Director of the FBI, these various new encryption tools are causing communications to be "Going Dark."[36] More specifically, under certain circumstances, law enforcement will no longer enjoy the easy access to the plain text of written and voice communications that it once did. New surveillance strategies, such as hacking into devices and a greater reliance on metadata, are likely to emerge.[37]

These new "Crypto Wars" — the debates over whether companies offering various IP-based communications services should be required to build wiretapping capabilities into their products[38] — are not the subject of this Article. It is clear, however, that in this new

---

33. Social graphs, likes, etc., can be quite revelatory of an individual's characteristics, even when these are not explicitly revealed. *See, e.g.*, C. Jernigan & B. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14 FIRST MONDAY (Oct. 5, 2009), http://journals.uic.edu/ojs/index.php/fm/article/view/2611/2302 [https://perma.cc/9CFF-KVDC].

34. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 119–20, 122–25, 151–56 (2012) (describing how location data has become a powerful investigative tool in law enforcement investigations, and explaining how the disagreement among the various stakeholders with respect to the appropriate standard for law enforcement access to location data manifested in the legislative process beginning in 2010).

35. *Encryption Tightrope: Balancing Americans Security and Privacy*, *Hearing Before H. Comm. on the Judiciary*, 114th Cong. 9–98 (2016) (statement of James Comey, Director, Federal Bureau of Investigation).

36. *Id*.

37. *See* Steven M. Bellovin et al., *Going Bright: Wiretapping without Weakening Communications Infrastructure*, 11 IEEE SECURITY AND PRIVACY, no. 1, 2013, at 62; Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) [hereinafter *Lawful Hacking*]; *see also* Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELECTRONIC FRONTIER FOUND. (Apr. 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government [https://perma.cc/JCL9-RXEQ] (describing an FBI software package that uses hacking tools for investigations).

38. *See* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT, SAVING PRIVACY IN THE DIGITAL AGE (2001) at 297.

communications environment, the collection of metadata takes on greater importance for law enforcement investigations. Metadata that reveals, for example, what activities might be taking place inside a target's home,[39] will become even more important to law enforcement investigations. We do not argue that law enforcement should never have access to this and other rich, revelatory metadata. However, understanding the limitations and, in many cases, the inapplicability of the current legal framework to an IP-based communications environment is the first necessary step towards conceptualizing new rules and principles for regulating law enforcement access to IP-based communications data.

There are a number of related topics that this Article is not about. First and foremost, we are not questioning the general applicability of the third-party doctrine. Rather, we are demonstrating that in the context of a complex IP-based communications environment, it is no longer a relevant, meaningful legal concept for regulating law enforcement access to data.[40] Second, we are restricting our attention to criminal law. Though the technical issues we raise are much the same with respect to intelligence collection, we do not discuss how these issues may impact interpretation and application of the Foreign Intelligence Surveillance Act and related statutes.[41] Third, we do not address the complex topic of location data, which includes the question of how it should be categorized (content, metadata, or something else entirely) and what standards should govern law enforcement access.[42] Finally, we do not evaluate[43] or offer a new interpretation of the "reasonable expectation of privacy" or construe new analogies to the *Katz*/*Smith* distinctions specifically calibrated for an IP-based communications environment. All of these matters are significant topics in their own right — all deserve (and many have received) careful consideration in other articles.

---

39. *See infra* Section IV.E.

40. The third-party doctrine is a controversial rule. *See*, *e.g.*, Orin S. Kerr*, The Case for the Third-Party Doctrine,* 107 MICH. L. REV. 561, 563 n.5 (2009*)* ("A list of every article or book that has criticized the doctrine would make . . . the world's longest law review footnote.").

41. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. § 1801 (2012)).

42. *See, e.g.*, Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 681, 717 (2011) (arguing that courts should require a warrant for access to location data in all cases because such acquisition is a search under the Fourth Amendment); Pell & Soghoian, *supra* note 34 (proposing model legislation for law enforcement access to location data). We note that although this article does discuss mapping services, our focus is on the very different behaviors of apparently similar services. We do not address the fundamental question of whether or not location services should always receive full Fourth Amendment protection.

43. *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007).

This Article is organized as follows: In Part II, we discuss the relevant constitutional cases and statutes that establish and develop the content/non-content distinction and the third-party doctrine. In Part III, we provide the technical background on IP-based communications necessary to explain the examples of Part IV. In Part IV, the heart of our paper, we discuss a series of examples illustrating that the content/non-content distinction and the third-party doctrine are no longer workable rules for an IP-based communications environment. The challenges we describe in the earlier parts of the paper suggest that new legislation is needed to establish new rules and standards for law enforcement access to communications data that do not depend upon the traditional content/non-content distinction or the third-party doctrine. While an all-encompassing statute is beyond the scope of this paper, in Part V, we present some principles that could guide future legislation to regulate law enforcement access to data in an IP-based communications environment that includes the implications of Big Data analytic techniques and the Internet of Things. We also provide some interim guidance to courts and to the Department of Justice, under the existing content/non-content distinction and third-party rule, on how to analyze and adjudicate applications for Pen/Trap orders in an IP-based communications environment. Finally, we present our conclusions in Part VI.

II. LEGAL BACKGROUND AND ANALYSIS

For decades, constitutional and statutory frameworks governing surveillance of wire and electronic communications have recognized a distinction between content and non-content components of those communications.[44] A second related but distinct tenet of electronic surveillance law dictates that when electronic communications are shared with third parties, non-content or metadata is subject to the controversial third-party doctrine.[45] Taken in its strongest expression, this rule affords no Fourth Amendment protection to information revealed to a third-party.[46] In anticipation of our general thesis that the technical complexities of IP-based communications both (1) render content/non-content distinctions no longer meaningful and (2) make it impossible to discover, much less identify, when data is being shared with a third-party, this Part will explain the relevant constitutional cases and statutes that establish and define these two separate, but related, tenets of electronic surveillance law.[47]

---

44. *See infra* Section II.A.
45. *See infra* Section II.C.
46. *See id.*
47. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law,* 50 WM. & MARY L. REV. 2105, 2124–25 (2009) ("Determining whether different types of Internet

This Part will also explore how other scholars have begun to question the applicability of the content/non-content distinction to IP-based communications, even if some ultimately choose to stay the content/non-content course. Moreover, for some time now, scholars have made credible arguments for a "limited" third-party doctrine — a reading of the third-party rule that "only removes constitutional protection from information when provided for a third-party's use."[48] This interpretation suggests that the third-party doctrine does not apply "where the third-party is a mere conduit or bailee."[49] This interpretation is pertinent to our argument that the third-party rule will cease to have relevance in an IP-mediated communications world where users of electronic communications will become increasingly unable to perceive if, when, and how they have disclosed information to a third-party. This blunting of consumer perception undermines the concept, articulated in *Smith v. Maryland*,[50] that a voluntary, knowing disclosure is implicit in any use of data by a third-party.

A. Content/Non-Content Constitutional Distinctions & Statutory Definitions

Understanding definitions of content and non-content in surveillance law requires examination of both case law and statutory definitions, as well as how they operate in tandem. The Supreme Court's dual decisions in 1967 — *Berger*[51] and *Katz*[52] — established that the content of telephone calls is protected by the Fourth Amendment. In each of these cases, authorities recorded conversations without any form of judicial authorization, using listening devices installed on private property (*Berger*[53]) and to the outside wall of a public tele-

communication information are content requires decoupling the question of content/non-content status from the question of whether the information is protected under *Smith*. . . . But conflating *Smith*'s analysis of the content/non-content distinction in telephone calls with its analysis of a reasonable expectation of privacy in such calls risks obscuring the question of what 'content' actually is.").

48. Stephen Henderson, *After United States v. Jones*, 14 N.C. J.L. & TECH. 431, 437 (2013).

49. *Id*. at 438.

50. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

51. *See* Berger v. New York, 388 U.S. 41, 51 (1967).

52. *See* Katz v. United States, 389 U.S. 347, 511 (1967). As Professor Stephen Henderson has observed, however, neither *Berger* nor *Katz* involved law enforcement obtaining the content of the phone conversations from a third-party telephone company. *See* Henderson, *supra* note 48, at 437. While arguing for a "limited" third-party doctrine in his scholarship, Henderson notes that Professor Orin Kerr, at least in 2004, posited that "Fourth Amendment protection of telephone conversations is actually less certain than perhaps we assume it to be." *Id.*

53. *See Berger*, 388 U.S. at 45.

phone booth (*Katz*.[54]). In response to the constitutional rule established in these cases, Congress, in 1968, passed the Wiretap Act,[55] a statutory scheme intended to create uniform rules that would comply with the Fourth Amendment for government interception of "wire"[56] and "oral"[57] communications in criminal investigations.[58] As previously noted, the Wiretap Act originally defined "contents" as "any information concerning the identity of the parties to the communication" or "the existence, substance, purport, or meaning of that communication."[59]

Almost ten years after the enactment of the Wiretap Act, the Supreme Court relied on Title III's legislative history and statutory language to distinguish a Title III wiretap from a pen register device.[60] Specifically, in *New York Telephone Company,* the Court distinguished the Title III definition of an "intercept"[61] ("the aural acquisition of the *contents* of any wire or oral communication through the use of any electronic, mechanical or other device")[62] from the operation of a pen register, which the Court characterized as "decod[ing] outgoing telephone numbers by responding to changes in electrical voltage caused by the turning of the telephone dial (or the pressing of buttons on pushbutton telephones) and present[ing] the information in a form to be interpreted by sight rather than by hearing."[63] In contrast to a wiretap's ability to collect and reveal communications content, the Court noted that pen register devices "do not hear sound" and disclose "only the telephone numbers that have been dialed."[64] Accordingly, this technology results in no disclosure of the "purport of any communications between the caller and the recipient of the call, their identities, nor whether the call was even completed."[65] Simply put, "pen registers do not accomplish the 'aural acquisition' of anything"

54. *See Katz*, 389 U.S. at 348. As both *Berger* and *Katz* involved listening devices, no consideration was given to any distinctions among the kinds of information that may or may not be disclosed to a telephone company.

55. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 2510–20, 82 Stat. 197, 211–15 [hereinafter Wiretap Act] (codified as amended at 18 U.S.C. §§ 2510–2530 (2012)).

56. 18 U.S.C. § 2510(1) (2012).

57. 18 U.S.C. § 2510(2) (2012).

58. 18 U.S.C. § 2518 (2012) (establishing procedures for wire, oral, or electronic communications by law enforcement officers).

59. Wiretap Act, *supra* note 55, at § 2510(8).

60. *See* United States v. N. Y. Tel. Co., 434 U.S. 159, 166–68 (1977).

61. *Id*. at 166.

62. *Id*. at 166–67 (quoting 18 U.S.C. § 2510(4)).

63. *Id*. at 167.

64. *Id.*

65. *Id.*

and there was "no congressional intent to subject pen registers to the requirements of Title III."[66]

Two years later, in *Smith v. Maryland*, the Court considered whether a petitioner had a constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system.[67] As part of its determination that a Fourth Amendment search had not occurred, the Court distinguished the state's use of a pen register device from the content-acquiring listening device employed in *Katz* by citing the description of the pen register found in *New York Telephone Company*: a device that "do[es] not hear sound" and that does not disclose "the purport of any communications between the caller and the recipient of the call" or "their identities."[68] As discussed in Parts I and III of this Article, the phone system in existence at the time of *Smith* could, for the most part, separate the transmission of the content of communications between parties from non-content signaling (such as numbers dialed) and switching (actually routing the call) data. At the time of *Smith*, therefore, the technical architecture of telephone networks supported a legal analysis and framework that distinguished content from non-content.

Congress first dealt with regulating law enforcement use of pen registers and associated trap-and-trace devices ("Pen/Trap")[69] in 1986,

---

66. *Id*. (citing S. REP. NO. 90-1097, at 90 (1968)) ("Paragraph 4 [of § 2510] defines 'intercept' to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. . . . The proposed legislation is not designed to prevent the tracing of phone calls. The use of a 'pen register,' for example, would be permissible.").

The Court was not quite technically correct about how pen registers collected dialed digits. By the time of New York Telephone, two kinds of telephone dialed digit signaling were in use. The first (and oldest) was "dial pulse signaling," in which dialed digits were encoded by briefly interrupting the DC telephone loop circuit a number of times corresponding to the digits dialed (e.g., one interruption pulse encoded the digit "1," while two pulses encoded the digit "2," etc.). A second form of signaling, called Dual-Tone Multi-Frequency (DTMF), was introduced commercially in 1963 under the "TouchTone" trademark. DTMF encodes dialed digits as audio tones that are sent over the voice path — that is, the part of the phone network that carries aural information — instead of as DC pulses.

Crucially, DTMF signaling can be used not just to convey dialed digits to the phone company, but also to encode content itself once the call has been established. For example, DTMF signals are often used to allow customers to route calls to an appropriate department of a large business ("press 1 for English, 2 for Spanish," etc.). These "post cut through" dialed digits are "content" and can be recorded by a pen register that is intended to collect only the digits sent to the telephone company. *But see infra* Section IV.D (discussing a ruling by the Foreign Intelligence Surveillance Court of Review on whether "post cut through dialed digits" are content).

67. *See* Smith v. Maryland, 442 U.S. 735, 738 (1979).

68. *See id*. at 741 (quoting *N.Y. Tel. Co.*, 434 U.S. at 167).

69. A trap-and-trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(4) (2012).

when it passed the Electronic Communications Privacy Act[70] ("ECPA"). What is now commonly known as the Pen/Trap statute[71] only applied, at that time, to "numbers dialed or otherwise transmitted" or "the originating number of an instrument or device."[72] Although the Stored Communications Act ("SCA"), Title II of the ECPA, was an attempt to regulate law enforcement access to dial-up email and information stored in the limited forms of electronic storage services of the time,[73] this Pen/Trap telephone-specific definition appears consistent with — and indeed carries forward — the content/non-content distinction suggested by the telephone network architecture in existence at the time of *Smith*.

With the passage of the ECPA, Congress also amended the Wiretap Act's definition of content, specifically extending Title III's protections to include "electronic communications" (along with wire and oral communications).[74] As David McPhie observes, "in an apparent effort to make clear the distinction between Title III and the pen register regulation schemes . . . [Congress] modified Title III's definition of 'contents' [by] eliminate[ing] from its scope the 'identity of parties' and mere 'existence' of communication."[75] Indeed, the Senate Report appears to evince Congress' intent to codify the Supreme

---

70. Electronics Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) [hereinafter ECPA]. This Article uses the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I ("Interception of Communications and Related Matters"), 100 Stat. at 1848, which amended the Wiretap Act; Title II ("Stored Wire and Electronic Communications and Transactional Records Access"), commonly referred to as the Stored Communications Act (SCA), § 201, 100 Stat. at 1860–1868 (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)); Title III ("Pen Registers and Trap and Trace Devices"), § 301, 100 Stat. at 1868–1873 (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

71. 18 U.S.C. §§ 3121–3127 (2012) [hereinafter Pen/Trap statute]. While a Wiretap Order has been called a "super warrant," *see* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630–31 (2003), due to its incorporation of the probable cause standard and several other requirements that must be demonstrated to a judge, 18 U.S.C. §§ 2518 (1)–(4) (2012), the Pen/Trap statute permits law enforcement to acquire data under a mere certification standard. Specifically, law enforcement must only "certify" to a court that the information sought is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2) (2012).

72. Title III of the ECPA describes a pen register as "a device or process which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." ECPA, § 301, 100 Stat. at 1871 (codified as amended as 18 U.S.C. § 3127(3) (2012)); *see also* 18 U.S.C. § 3127(4) (2012), *supra* note 69, for definition of "trap and trace device."

73. Congress passed the ECPA at a time when current technologies facilitating electronic communications did not exist. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (recognizing that the ECPA is "ill suited to address modern forms of communication" since it "was written prior to the advent of the Internet and the World Wide Web" (quoting Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002))).

74. 18 U.S.C. § 2511 (2012).

75. David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 STAN. TECH. L. REV. 1, ¶ 10 (2005).

Court's analysis in *New York Telephone Company* and *Smith*[76]: "[t]he Supreme Court has clearly indicated that the use of pen registers does not violate either [Title III] or the [F]ourth [A]mendment. Subsection 101(a)(5) of this legislation [amending the definition of "contents"] makes that policy clear.'"[77] The ECPA's definition of content, forged with specific reference to the telephone network architecture of the 1970s, but still legally applicable to modern IP-based communications,[78] includes "any information concerning the substance, purport, or meaning of that communication."[79]

Following the September 11th attacks, Congress expanded the categories of non-content information that could be acquired under the Pen/Trap statute by amending the statute via the USA PATRIOT Act.[80] Although the events of September 11th ultimately provided the impetus for amending the Pen/Trap statute, there were earlier efforts to update the statute's "antiquated statutory language and legal procedures."[81] As Beryl A. Howell, General Counsel for the Senate Judici-

---

76. *See id.*

77. *Id*. (alteration in original) (quoting S. REP. NO. 99-541, at 13 (1986)).

78. Data communications in 1986 was nothing like today's Internet. The ARPAnet — the ancestor of today's Internet — did exist. But in order to prevent a government-funded offering from competing with the nascent commercial companies, the ability to connect to it was severely restricted. There were several such companies that did networking and email, including Telenet, Compuserve, Tymnet, and MCI Mail. There was also the rather anarchic Usenet network that linked many universities and some private companies around the world. In addition, there were many "bulletin boards" run by hobbyists on early microcomputers. Most of these networks used dial-up modems operating at 300 or 1200 bits per second, though there was some employment of the X.25 packet-switching protocol. Usenet was unofficially (and arguably improperly) connected to the ARPAnet in several places; the ARPAnet was also reachable officially via a National Science Foundation-sponsored dial-up network known as CSnet.

All of these systems worked. Most, except for the Usenet/CSnet/ARPAnet linkup, were effectively closed environments; they did not communicate with each other. Furthermore, given how rare email usage was, it was effectively impossible to reach someone at another company because it was improbable that the intended recipient even used email, let alone the same email service.

The user experience was very different, too. Everything was done by command line interfaces, generally from dumb terminals with no local storage or computational ability; graphical user interfaces were all but unknown. Disk space was expensive and hence extremely limited. Unlike today's systems, where a variety of mail clients can have temporary copies of mail stored on a central server, mail was retrieved directly from a dedicated store. It was quite plausible that mail left on a server for more than 180 days had been abandoned; neither the price of disk space nor the user interfaces of the time in any way encouraged leaving email on the system. The SCA applies a more stringent law enforcement access standard to content that is less than 180 days old. *See* 18 U.S.C. § 2703(a) (2012).

79. 18 U.S.C. § 2510(8) (2012). The full definition reads as follows: "'contents', when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.*

80. *See* Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, §§ 2–1016, 115 Stat. 272, 272–402 (2011)*; see also* 147 CONG. REC. S9402 (daily ed. Sept. 13, 2001).

81. Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act,* 72 GEO. WASH. L. REV. 1145, 1194 (2004).

ary Committee during the passage of the PATRIOT Act, explains, Congress intended to "clarify, consistent with long-standing federal law enforcement practice sanctioned by the courts, that such devices may be used on computer transmissions to obtain electronic addresses, not just on telephones."[82] To codify this practice, the PATRIOT Act struck "call processing information" from the statute to emphasize that a pen register device "could be used to 'identify the origination or destination of wire and electronic communications'" and struck "references to 'telephone line' to make clear that the device may obtain 'signaling information that identifies the destination of wire or electronic communications transmitted by an instrument or facility to which device or process is attached or applied.'"[83]

While Congress apparently intended to clarify that the Pen/Trap statute could be used to collect information on the Internet, certain new terms it chose to define the types of collectable information are, at best, less than clear. More specifically, the terms "routing" and "addressing" were added, although the Bush Administration "refused" to define them.[84] This definitional vagueness raised concerns that those terms could be read to encompass Constitutionally-protected content,[85] which would require the government to obtain a Title III super warrant,[86] not a mere Pen/Trap order, to obtain these categories of information.[87] Recognizing potential situations where certain kinds of communications data might contain both content and non-content, the Department of Justice ("DOJ") "conceded that 'reasonable minds may differ as to whether, and at what stage, URL[88] information may be construed as content.'"[89]

The PATRIOT Act also added the term "signaling information" to the Pen/Trap statute, but, as was the case with other new terms, did not define it.[90] From the DOJ's perspective, signaling information was

82. *Id.* at 1194–95.

83. *Id.* at 1197.

84. *Id*.

85. As a result of negotiations with Senate Judiciary Committee member Patrick Leahy, section 216 of the PATRIOT Act excludes Pen/Traps from collecting "the contents of any wire or electronic communications." *Id.* at 1198.

86. *See* 18 U.S.C. § 2518 (2012) (providing a procedure for interception of wire, oral, or electronic communications). The term "super" warrant is often used colloquially to describe Wiretap Act procedures because of application requirements such as "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.*

87. *See* Howell, *supra* note 81, at 1197.

88. *See infra* Section IV.C for an explanation of Uniform Resource Locators (URLs).

89. Howell, *supra* note 81, at 1197 (citing Letter from Daniel A. Bryant, Assistant Attorney General, to Patrick J. Leahy, Chairman, Committee on the Judiciary (Nov. 29, 2001)). The DOJ further noted that "a file path identifying the location of a requested document may 'at a certain point along a URL . . . become too specific to be appropriately collected by a Pen/Trap order.'" *Id*.

90. 18 U.S.C. § 3127(3) (2012) (defining pen register as "a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an

broader than dialed numbers; it was to encompass "other kinds of non-content information used by a communication system to process communications."[91] But with respect to data related to cellular communications, the DOJ instructs prosecutors that the new pen register definition "appears to encompass *all* of the non-content [information that passes] between a cell phone and a provider's tower."[92] Moreover, the DOJ's 2005 Electronic Surveillance Manual notes that the "scant legislative history" accompanying the PATRIOT Act indicates that the new definitions should apply to "all communications media."[93] Does the DOJ's generous interpretation of signaling information include "*all* of the non-content [information]" in IP-based communications? Further guidance is not found in the 2005 manual.[94]

---

instrument or facility from which a wire or electronic communication is transmitted"). "Signaling" is a well-recognized technical term in telephony; *see generally* MEMBERS OF THE TECH. STAFF AND THE TECH. PUBL'N DEP'T, AT&T BELL LABORATORIES, ENGINEERING AND OPERATIONS IN THE BELL SYSTEM, 265 (R.F. Rey, 2d ed. 1983) [hereinafter Rey]. The term is not generally used on the Internet, except when describing telephony-like protocols. *See infra* discussion Section III.D.

91. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS, 46 (2005) [hereinafter ELECTRONIC SURVEILLANCE MANUAL], https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [https://perma.cc/RXX5-W7CF]. At some point in time, the DOJ inserted a statement in the Electronic Surveillance Manual indicating that the question of what legal authorities are required to locate cellular telephones "has been the subject of extensive litigation recently." *Id.* at 42. The DOJ therefore instructs readers that the information contained in the 2005 manual on that topic is no longer current. *Id.* The information we cite from this part of the of the 2005 Electronic Surveillance Manual may relate to the question of what legal authorities permit the government to locate cellular telephones, but we do not cite it for that purpose. We cite it to illustrate the DOJ's expansive reading of the of the Pen/Trap statute's terms and definitions, which carries forward to the 2009 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. *See infra* note 95.

92. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, at 42 (emphasis added). Similarly, the definition of "trap and trace" device, which originally included only "the originating number of an instrument or device," Pub. L. No. 99-508 100 Stat. 1872 (1986), expanded to include "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4) (2012). Like the expanded definition of pen register, the DOJ instructs that the new trap and trace definition now "appears to include such information as the transmission of a MIN [or other type of unique identifying number], which identifies the source of a communication." Electronic Surveillance Manual, *supra* note 91, at 46–47. *See also id.* at 46–48 (further explaining the DOJ's reasoning supporting its interpretation of the Pen/Trap statute).

93. *Id.* at 47. Relying on the House Report, the DOJ suggests that when passing the final bill "Congress intended that the statute would apply to all technologies." *Id.* "Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain any non-content information — 'dialing, routing, addressing, and signaling information' — utilized in the processing and transmitting of wire or electronic communications. . . . This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media . . . ([and includes] packets that merely request a telnet connection in the Internet context)." *Id.* (emphasis in original) (alteration in original) (quoting H.R. REP. NO. 107-236, at 52–53 (2001)).

94. In a different context, attorneys from the DOJ's National Security Division and the FBI's National Security Law Bureau told an Inspector General that "terms used to define

But, in a different, more recent 2009 publication on searching and seizing evidence from computers, the DOJ takes the position that the Pen/Trap "definitions' inclusion of all 'dialing, routing, addressing, [and/or] signaling information' encompasses almost all non-content information in a communication."[95] Some of the DOJ's guidance with respect to specific types of non-content information that can be collected under the Pen/Trap statute is, we argue, incorrect — we will return to this issue in Part III and Section IV.B.

The ECPA's amendments to the Wiretap Act's definition of content and the PATRIOT Act's amendments to the Pen/Trap statute give us the most current legal definitions of content and non-content. These apply to today's IP-based communications. But Professor Orin Kerr, noting that the "Wiretap Act itself does not define 'contents' clearly,"[96] questions whether "there is a third category of information outside of 'contents' and 'dialing, routing, addressing, and signaling' information."[97] Kerr, who raises this question in the context of discussing whether "URLs that include search terms and other websurfing addresses can contain 'content,'"[98] asserts that the question of whether or not a third category of information exists outside of statutory definitions of content and non-content is "not clearly answered by the Patriot Act."[99] As we have previously referenced, the DOJ interprets the Pen/Trap definitions post PATRIOT Act to apply broadly to the Internet, but Kerr and other scholars disagree, and they have begun to grapple with the difficulties of applying legal definitions of content and non-content to the Internet. As a precursor to our argument that IP-based communications render our legal content/non-content distinctions essentially meaningless, we discuss certain questions and analyses raised by several scholars.

---

metadata themselves lack standardized definitions and that applying them to rapidly changing technology can be difficult." OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS: ASSESSMENT OF PROGRESS IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 THROUGH 2009, at 24 (2015), https://oig.justice.gov/reports/2015/o1505.pdf#page=1 [https://perma.cc/U2ZD-5EA9].

95. DEP'T OF JUSTICE, 2009 SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 154 [hereinafter 2009 SEARCH MANUAL], https://www.justice.gov/sites/default/files/criminal-ccips/leacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/7TCC-SA74].

96. Kerr, *supra* note 71, at 645 (discussing questions raised by surveillance of websurfing and internet search terms).

97. *Id.* at 645 n.186.

98. *Id.* at 645. For a more in-depth discussion of URLs, *see infra* Section IV.C.

99. *Id.* at 645 n.186.

B. What Other Scholars Have Said and Done

The Wiretap Act's definition of content — any information concerning the substance, purport, or meaning of that communication — is arguably very broad. Professor Matthew Tokson asserts that this definition is expansive and "would include the overall gist of the message contained, or even the general subject matter discussed."[100] As limited, expansive, or unclear[101] as the definition of content may be, McPhie poses the more complex question of *how* to discern the "exact relationship between the positive and negative definitions of 'content' (substance and meaning versus addressing or signaling data)."[102] Are they even mutually exclusive terms?[103]

McPhie posits three possibilities for ascertaining the positive and negative definitions of content: (1) "content might include all data that is not 'signaling and addressing information'"; (2) some signaling and addressing information could also be considered content; and (3) as Kerr considered, some data may neither be content nor addressing and signaling information.[104] To illustrate one aspect of this categorization problem, McPhie notes that pen registers can record call length, which is arguably neither call content nor addressing or signaling information.[105] If call length does not fit into either category, and if each category is "comprehensive and mutually exclusive," then why should the length of a call be treated legally as non-content rather than content?[106]

Kerr also recognizes the possibility that addressing or signaling information could be considered content in certain situations.[107] He argues that this "difficulty [is] latent in *Smith*":[108]

> In *Smith*, the Court analogized dialing a phone number to contacting an operator and asking the operator to connect the call. Because disclosing the number to

100. Tokson, *supra* note 47, at 2126 (citing 18 U.S.C. § 2510(8) (2006)).

101. *See* Kerr, *supra* note 71, at 645.

102. McPhie, *supra* note 75, at ¶ 26.

103. *See id.* at ¶ 26 n.55. (referencing "Senator Leahy's criticism of the vagueness of the 'addressing and signaling' terms").

104. *See id*. As acknowledged by McPhie and Kerr, the statutory definition of "content" and the Pen/Trap reference to "dialing, routing, addressing, and signaling" (DRAS) do not fully describe all of the kinds of information contained in IP-mediated communications. Professor Susan Freiwald argues that "web traffic data," which she defines as "the information . . . we generate when we use the World Wide Web" does not constitute DRAS information. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 10, 51 (2004). We explore these issues further in Part IV.

105. *See* McPhie, *supra* note 75, at ¶ 26.

106. *See id.* For a more in-depth discussion of packet lengths and what they can reveal, *see infra* Section IV.E.

107. Kerr, *supra* note 71, at 628.

108. *Id.* at 646 n.190.

> an operator would eliminate the speaker's reasonable expectation of privacy in the information, so did disclosing the information to the phone company's computer. So far, so good. The difficulty is that if a speaker calls the operator and places that request, then that request constitutes the *contents* of the communication between the speaker and the operator. The contents of the conversation between the speaker and the operator becomes the addressing information for the ensuing conversation between the speaker and the person he wishes to call. As a result, it is difficult in the abstract to say whether that initial communication should be considered addressing information or contents.[109]

Both McPhie[110] and Kerr[111] acknowledge that these categorization problems become more profound in the context of the packet-switched communications environment of the Internet. Consistent with the difficulty latent in *Smith*, Kerr raises the question of how to categorize commands sent by a human to a computer.[112] Specifically, when a user surfs the web using his keyboard and mouse, are these inputs: (1) the "'content' of the communication between the user and his computer"; or (2) "merely 'addressing information' that the user entered into his computer" to tell it where to go and what to do?[113]

1. To Distinguish and Categorize or Not?

Tokson also examines the complex legal and technical questions raised when applying the traditional content/non-content distinction to IP-based communications.[114] At the outset of Tokson's analysis, how-

---

109. *Id.* (internal citation omitted).

110. McPhie, *supra* note 75, at ¶ 27 ("This categorization problem is only multiplied in the Internet context. Internet packets contain a large quantity of discrete and potentially revealing pieces of data, and for each type of data, its availability for collection under a pen register order depends upon this interplay of the 'content' and 'addressing and signaling information' requirements. Variations in the interpretation of these terms yield radically different pictures of what the government can get its hands on without a Title III warrant.").

111. *See* Kerr, *supra* note 71, at 645–46.

112. *Id.* at 646.

113. *Id.* at 646 n.190 ("noting that '[n]o court has yet considered' whether digital signals entered by a user to a computer over a telephone line are contents and stating that 'it may be that a Title III warrant is required'" (alterations in original) (citing United States Telecomm. Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000)).

114. Tokson, *supra* note 47, at 2124. ("[W]e lack a robust conceptual framework for determining whether new forms of communications information, such as web surfing data, should be classified as content or noncontent. . . . [P]erhaps it is simply because determining whether web surfing "communications" are content or not — and sorting out what that

ever, he asserts, notwithstanding the logic of any arguments for abandonment of the content/non-content distinction, that "[it] is firmly established in communications surveillance law, and any attempt to dislodge it would likely be quixotic."[115] With this maxim as a guidepost, Tokson embarks on developing "a legal framework for distinguishing content from [non-content] envelope information in unique areas of Internet communications."[116] Ultimately, in an effort to uphold the distinction, Tokson proposes a "*content-revealing*" rule: "electronic information that can reveal the underlying text or subject matter of an Internet communication must be classified as content."[117] He believes that stronger Internet privacy protections will come from recognizing "the breadth of Internet communications data that should be classified as content under constitutional and statutory law."[118]

Recognizing the value of these and other scholarly contributions to the effort of determining how to apply the content/non-content distinction to IP-based communications,[119] we come at the issue from a very different perspective. As addressed in Parts III and IV, we argue that, from a technological vantage point, it is and will become increasingly more difficult to draw content/non-content distinctions in an IP-based communications world, or at least too difficult for courts to construe and apply consistently. But before engaging in that argument, this Part examines the significant cases establishing the third-party doctrine and Professor Henderson's argument that it is, in fact, a limited rule.

C. Third Party Doctrine Complications

1. *United States v. Warshak*

The SCA, Title II of the ECPA, governs law enforcement access to data stored by specific kinds of third parties.[120] While the Wiretap Act requires the government to establish that there is "probable cause

---

would mean in terms of the Fourth Amendment and the ECPA — presents a complex legal and technical question.").

115. *Id*. at 2112.

116. *Id*. at 2105.

117. *Id*. In his examination of URLs, for example, Tokson cautions against trying to draw a legal distinction between URLs that contain search terms, and therefore are easily identified as content, and those that do not. *Id.* at 2135–36. Specifically, he suggests that those URLs not containing search terms reveal the same magnitude of content as those containing search terms because they both "expos[e] the website content requested by and sent to users." *Id*. at 2137.

118. *Id*. at 2124.

119. *See, e.g.*, Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1020–23 (2007) (explaining why the content/non-content distinction does not easily apply to location data).

120. *See* 18 U.S.C. §§ 2101–2712(3) (2012).

for belief that an individual is committing, has committed, or is about to commit a particular offense"[121] in order to collect the content of communications in real-time, the SCA allows the government to compel disclosure of stored content communications under lower standards. Indeed, law enforcement can compel stored content under what is often described as a reasonable suspicion standard[122] or even a mere relevance showing.[123] The compelled disclosure of email content under standards lower than a Fourth Amendment "probable cause" showing has, however, been found unconstitutional by the Sixth Circuit in *United States v. Warshak*.[124] Specifically, *Warshak* held that the Fourth Amendment protects the contents of email held by an ISP.[125] The court reasoned:

> If we accept that email is analogous to a letter or phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient.[126] Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call — unless they get a warrant, that is.[127]

While the contours of the *Warshak* decision have not been fully explored and tested, it is reasonably clear that *Warshak* extends Fourth Amendment protection to communications content when the service provider functions as a mere "intermediary" akin to the post

---

121. 18 U.S.C. § 2518(3)(a) (2012).

122. *See* 18 U.S.C. §§ 2703(b)(B)(ii), 2703(d) (allowing law enforcement to compel communications content from ECPA-covered third parties via a court order finding that there are 'specific and articulable facts' that the information sought is "relevant and material to an ongoing criminal investigation.").

123. *See* 18 U.S.C. § 2703(b)(B)(i) (allowing the use of an administrative, grand jury or trial subpoena to compel communications content from ECPA-covered third parties).

124. 631 F.3d 266, 274 (6th Cir. 2010).

125. *Id.* at 282 ("We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails.").

126. The court misunderstood the situation. As explained in Part IV, the functional equivalent of a post office is a mail server, which need not be operated by an ISP. *See infra*, Part IV.

127. *Warshak*, 631 F.3d at 286 (citing United States v. Jacobsen, 466 U.S. 109, 114 (1984); Katz v. United States, 389 U.S. 347, 353 (1967)).

office or a telephone company.[128] The "mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[129] Thus, a "subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'"[130]

It remains unclear, however, whether and under what circumstances an ISP's "expresse[d] . . . intention[s] to 'audit, inspect and monitor' its subscriber's emails" could be enough "to render an expectation of privacy unreasonable."[131] The court suggested that there might be some kind of notice, agreement, or interaction with the data that could defeat the Fourth Amendment protection afforded to the content of communications in the possession of ISPs or, presumably, other kinds of communications service providers in the growing world of IP-based communications.[132]

Put another way, what can a subscriber reasonably be expected to discover or know about how various kinds of third parties might be accessing and using that subscriber's communications content? How might that discovery or knowledge affect the constitutional status of communications content? The fact that the ISP contractually reserved the right to access Warshak's emails for certain purposes did not defeat Warshak's reasonable expectation of privacy.[133] The court, however, did not rule out the fact that under some yet-undefined set of circumstances, the mere content status of specific communications data may not suffice to invoke Fourth Amendment protection.

If constitutional protections for communications content in the possession of third-party providers do not, in all circumstances, turn

---

128. *Warshak*, 631 F.3d at 288 (emphasis omitted) (quoting Patricia Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 165 (2008) ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests." (alteration in original)).

129. *Id.* at 286–87.

130. *Id*. at 288 (citing Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) [hereinafter *Warshak 2007*]).

131. *Id*. at 287 (citing *Warshak 2007*, 490 F.3d at 472–73 (quoting United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000))).

132. *See id.* at 286–87.

133. *Id.* ("While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, we doubt that will be the case in most situations, and it is certainly not the case here.") (internal citations omitted). In the instant case, "the ISP's 'control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy.'" *Id.* at 287 (alteration in original) (quoting *Warshak 2007*, 490 F.3d at 473).

upon the content status of the communications data in question,[134] what might that suggest about the analysis of the constitutional status of non-content data or, most exacting of all, data that cannot be easily classified as either content or non-content? To explore these questions we must examine the third-party doctrine, as expressed in *United States v. Miller*[135] and *Smith v. Maryland*[136].

2. *Miller* & *Smith*

The third-party doctrine, taken in its strongest expression in *United States v. Miller*, suggests that, once data is disclosed to a third party, it no longer receives Fourth Amendment protection:

> The [bank] depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[137]

In *Warshak*, the court distinguished the relevant facts in the case at hand (an ISP in possession of emails as a mere intermediary, not the recipient of the emails) from the facts in *Miller* (a bank depositor disclosing the contents of "bank documents, 'including financial statements and deposit slips . . . voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.'").[138] Specifically, the *Warshak* court noted that the information at issue in *Miller* "involved simple business records" in contrast to the "potentially unlimited variety of 'confidential communications' at issue" in *Warshak*.[139] While the court asserted that one kind of content is more confidential and sensitive than another, it is equally important to note

134. *See* Tokson, *supra* note 47, at 2117 ("[I]t remains difficult to predict whether the content/non-content distinction will remain the central determinant of constitutional protection for email and website communications.").

135. 425 U.S. 435 (1976).

136. 442 U.S. 735 (1979).

137. *Miller*, 425 U.S at 443 (1976) (citations omitted).

138. *Warshak*, 631 F.3d at 287–88 (quoting *Miller*, 425 U.S. at 422).

139. *Id*. at 288.

the *Warshak* court's focus on the documents in *Miller* as voluntarily conveyed for the bank's use.[140]

We see this same language and analysis in *Smith*. There the Court found that society was not prepared to recognize the existence of a reasonable expectation of privacy in dialed phone numbers because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[141] In his examination of the reach and scope of the third-party doctrine, Professor Stephen Henderson argues that what we consequently have is "a 'limited' third-party doctrine that only removes constitutional protection from information provided for a third party's use."[142] Henderson asserts, for example, that the Court may not have intended the doctrine to apply "where the third party is a mere conduit or bailee," as in the case of *Warshak*.[143] As previously noted, the Sixth Circuit recognized Fourth Amendment protection for email in the possession of an ISP, notwithstanding its use of algorithms to scan email content and its disclosure of that fact to subscribers.[144]

In *Miller*, the financial information at issue was "negotiable instruments to be used in commercial transactions" that were "exposed to [bank] employees in the ordinary course of business."[145] In *Smith*, the phone numbers at issue were recorded by the phone company "for a variety of legitimate business purposes."[146] But what would third-party *use* mean in context of the packet-switched Internet and the growing numbers and types of IP-mediated communications its structure and operations imply? *Warshak* examines a specific situation where a commercial ISP had access to the content of a subscriber's email, then goes on to characterize this particular kind of access and control as analogous to "the functional equivalent of a post office or

---

140. *Id*. at 287–88 (citing *Miller*, 425 U.S. at 442). ("The Court's holding in *Miller* was based on the fact that bank documents, 'including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.'").

141. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (emphasis added) (citations omitted). In determining that the petitioner had no subjective expectation of privacy, the Court noted that: "Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id*. at 743.

142. Henderson, *supra* note 48, at 437.

143. *Id.* at 438.

144. *Id.* at 438 (citing *Warshak*, 631 F.3d at 286–87). Henderson also cites a number of cases where courts have recognized a reasonable expectation of privacy in something left with a bailee. *Id.* at 437 (citing United States v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) (bag left with store clerk); United States v. Barry, 853 F.2d 1479, 1481–84 (8th Cir. 1988) (luggage left with airline); United States v. Presler, 610 F.2d 1206, 1213–14 (4th Cir. 1979) (briefcase left with friend)).

145. *Miller,* 425 U.S. at 442.

146. *Smith*, 442 U.S. at 743.

telephone company."[147] But in acknowledging that there could be yet undefined circumstances where a third party's expressed intentions to access and use communications content would subject that data to the third party rule, *Warshak* raises — but fails to answer — the question of just what those third-party uses might be in the broader, more complicated context of an IP-mediated communications environment. Indeed, *Warshak* only defines the issue negatively, stating what third-party uses are not: the third-party rule does not apply where the third party is a mere "intermediary."[148] In stating this conclusion by defining intermediary only by analogy to a post office or telephone company, the scope of *Warshak*'s holding is, understandably, limited to the very specific facts before it.

The limited scope of *Warshak*, nevertheless, poses some questions regarding the very lines it admits it is unable to draw.[149] What if a third party converts, changes, or manipulates the data entrusted to it in the "ordinary course of business"?[150] Would this kind of third party interaction with the data dissolve its protection by operation of the third-party rule? Will courts have sufficient technical acumen to examine how various kind of third parties interact with and potentially change or manipulate data, then draw meaningful distinctions between and among these third-party data interactions for purposes of applying the third-party doctrine? In the context of the complex nature of IP-mediated communications, which we discuss in the next two parts, *Warshak* raises more questions than it answers.

There is yet another complicating factor to address regarding application of the third-party doctrine, one that has specific implications for non-content data and data not easily characterized as content or non-content. Henderson argues persuasively that operation of the third-party doctrine cannot be read as removing constitutional protections from all data provided to a third party.[151] Rather, he concludes, the scope of the doctrine is limited in its reach exclusively to data provided for a third party's use.[152] We agree with this conclusion. A further premise, still more restrictive of the doctrine's scope, is implicit everywhere in Henderson's argument: that data can be provided to a third party for its use only by means of a "voluntary conveyance."

---

147. *Warshak*, 631 F.3d at 286. Henderson anticipated *Warshak*'s holding and its analogy to a pre-Internet age telephone company. Specifically, he argued that if a court were to find that consumers had no reasonable expectation of privacy in contents of emails traveling over packet-switched networks, then such a theory would extend to packet-switched telephone calls (VoIP), as well. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 527–29 (2005).

148. *Warshak*, 631 F.3d at 286–87.

149. *Id*. at 287 (citations omitted).

150. *Miller*, 425 U.S. at 442.

151. *See* Henderson, *supra* note 48, at 437–46.

152. *Id.* at 437.

As previously noted, the concept of voluntary conveyance is derived directly from *Miller* and *Smith*, specifically in the way these Courts described the nature of the disclosure of the information at issue between the customer and the third party (bank and telephone company, respectively).[153]

For a conveyance to be made voluntarily, it must be done with intent or by design,[154] which, of course, presumes knowledge on the part of the consumer of that which is being conveyed. In both *Miller* and *Smith*, the courts' discussions included facts showing consumers knew that they were disclosing the information at issue to the respective third parties.[155]

The question of what it means to make a voluntary conveyance has been considered more recently by a number of federal appellate courts in the context of cell phone location data. Mobile phones use radio waves to communicate with a carrier's network, and thus service providers maintain large numbers of radio base stations — cell sites — spread throughout their coverage areas.[156] Whenever a user places or receives a call or sends a text message over the cell phone network, the communication is transmitted between the handset and the nearest tower.[157] If the user changes location during the course of a call, the call is handed off to the next closest tower.[158] Moreover, as part of their normal function, mobile phones periodically register and identify themselves to the nearest cell site, which is generally the station with the strongest signal, so that cell providers will know where to direct any incoming calls.[159] This "checking-in" continues even when users are not in the process of making or receiving a call.[160] These interactions produce Cell Site Location Information (CSLI), much of which subsequently is stored by service providers.[161]

---

153. *See Miller*, 425 U.S. at 442; *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979).

154. *See Definition of Voluntary by Merriam-Webster*, MERRIAM WEBSTER (Oct. 12, 2016), http://www.merriam-webster.com/dictionary/voluntary [https://perma.cc/TXS3-A3HP] ("voluntary: done by design or intention: intentional").

155. *See Miller*, 425 U.S. at 442 (noting respondent categorized his check and deposit slips disclosed to the bank as "personal records"); *see also Smith*, 442 U.S. at 743 (emphasizing that telephone users are aware that they convey numerical information to the phone company for "legitimate business purposes").

156. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 20 (2010) (statement of Professor Matt Blaze).

157. *Id*.

158. *Id*.

159. *See id*. at 13.

160. *See id*. at 13–14.

161. *See id*. at 16; Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [https://perma.cc/BHE5-FGS5].

In addressing the question of whether a cell phone user voluntarily conveys location data to a cell phone provider, the Third Circuit opined:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't 'voluntarily' exposed anything at all."[162]

This pronouncement by the Third Circuit came in response to the government's argument that *Smith* should control its compelled disclosure of location data from a third party cell phone provider.[163] Other circuit courts have disagreed with the Third Circuit's voluntary disclosure analysis. Specifically, the Fifth Circuit reasoned that a cell phone user:

> makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.[164]

Three other circuits — the Fourth,[165] Sixth,[166] and Eleventh,[167] — have also followed the Fifth Circuit's reasoning with respect to a cell phone users voluntary conveyance of CSLI. The Eleventh Circuit ventured further in its voluntary conveyance analysis, suggesting that "users could not complete their calls without necessarily exposing this

---

162. *In re* Application of the United States of America for an Order Directing A Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*,* 620 F.3d 304, 317–18 (3d Cir. 2010) (alteration in original) (emphasis in original).

163. *See id*.

164. *In re* Application of the U.S. for Historical Cell Site Data*,* 724 F.3d 600, 614 (5th Cir. 2013).

165. *See* United States v. Graham, 824 F.3d 421, 435–36 (4th Cir. 2016) (en banc).

166. *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

167. *See* United States v. Davis, 785 F.3d 498, 519 (11th Cir. 2015) (en banc).

information to the equipment of third party service providers."[168] In its reading of *Smith* and interpretation of voluntary conveyance, however, the Eleventh Circuit appears to conflate the concept of information that is "necessarily" conveyed with the concept of a knowing, voluntary conveyance.

Dissenting opinions by judges in both the Eleventh and Fourth Circuits challenge the aforementioned majority opinions' voluntary conveyance analysis. Dissenting Eleventh Circuit Judge Beverly Martin explained that cell phone users "do not affirmatively enter their location to make a call . . . [and] 'when a cell phone user *receives* a call, he hasn't voluntarily exposed anything at all.'"[169] Moreover, she observed an important distinction between the notice provided to users dialing numbers, as recognized by *Smith*, and creation and conveyance of location data:

> The *Smith* Court also emphasized that the numbers a person dials appear on the person's telephone bill and referenced the pre-automation process that required the caller to recite phone numbers out loud to a phone operator in order to make a call. Thus, the Court concluded that "[t]elephone users . . . typically *know* that they must convey numerical information to the phone company." There is not the same sort of "knowing" disclosure of cell site location data to phone companies because there is no history of cell phone users having to affirmatively disclose their location to an operator in order to make a call. The extent of voluntariness of disclosure by a user is simply lower for cell site location data than for the telephone numbers a person dials. For that reason, I don't think *Smith* controls this case.[170]

Fourth Circuit Judge James Wynn put an even finer point on what voluntary conveyance means in the context of Supreme Court precedent on the third-party doctrine. Looking at all of the relevant Supreme Court cases, including *Smith* (defendant dialed phone numbers),[171] *Miller*,[172] (defendant submitted multiple checks and de-

168. *Id.* at 512 n.12.

169. *Id.* at 534. (Martin, J., dissenting) (quoting *In re* Application of the United States of America for an Order Directing A Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010)).

170. *Id.* at 534–35 (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979) (emphasis in original)).

171. 442 U.S. at 743.

172. 425 U.S. 435, 442 (1976).

posit slips to a bank) and *Hoffa v. United States*[173] (defendant made statements to an associate disclosing endeavors to bribe [jury] members), Judge Wynn discerned that voluntary conveyance meant at least two things: (1) the defendant "knew he was communicating particular information"; and (2) the defendant "had acted in some way to submit the particular information he knew."[174] For Judge Wynn, it was crucial in all of these cases that there was an "action" (e.g. "depositing, dialing, speaking"), and "where many pieces of data were compiled into records," like in *Miller* and *Smith*, "there was presumptively a discrete action behind each piece of data."[175] Judge Wynn asserted that the Supreme Court has never suggested that the "simple act of signing up for a bank account, or a phone line, was enough to willingly turn over thousands of pages of personal data."[176] Interpreting voluntary conveyance to mean a user having knowledge of a particular piece of information that he then actively transmits, Judge Wynn concluded that CSLI is not voluntarily conveyed by the cell phone user and therefore not subject to the third-party doctrine.[177] Specifically, he asserted that the "cell phone customer neither possesses knowledge of his CSLI nor acts to disclose it" to a third party in the same patently active manner found in all relevant Supreme Court precedent.[178]

Consistent with the reasoning offered by these dissenting opinions, we demonstrate in Parts III and IV that the complexity of IP-mediated communications and services makes it difficult, if not impossible, for even the most technically sophisticated user to discover and comprehend the information she may be communicating to third parties. Unlike communications to a bank, a telephone company, or an ISP, these interactions may be completely invisible to the user in the course of her use of IP-based communication services. If a user cannot discover, much less know, what she discloses to a third party, then how will the third-party doctrine continue to be a relevant, meaningful legal concept for regulating government access to data in an IP-based communications environment?

In Parts III and IV we illustrate why and how the content/non-content distinction and the third-party doctrine are no longer workable rules for courts determining appropriate law enforcement access standards to data in a modern IP-based communications environment.

---

173. 385 U.S. 293, 302 (1966).

174. United States v. Graham, 824 F.3d 421, 443 (4th Cir. 2016) (en banc) (Wynn, J., dissenting).

175. *Id.*

176. *Id.*

177. *See id.* at 446.

178. *Id*.

III. NETWORK ARCHITECTURES

Both the Public Switched Telephone Network ("PSTN") and the Internet are communications networks, but the Internet has a very different architecture than the PSTN, especially the PSTN that existed at the time *Smith* was decided. Accordingly, in this Part, we explain some aspects of the architecture and workings of the Internet (including a basic explanation of how today's Internet operates). We do so to demonstrate how significant differences between the Internet and the PSTN preclude sustainable, workable applications of the content/non-content distinction and the third-party doctrine to IP-based communications.

For purposes of illustrating how the traditional application of the content/non-content distinction and the third-party doctrine is complicated by an IP-based communications environment, we distinguish between two types of content, "communicative content" and "architectural content." The familiar form of communicative content, as recognized in *Smith* and the Wiretap Act, is predicated upon the semantic meaning of the communication itself. Here, content is a function of the interpretation of language, symbol, and grammar, and not of architectural structure and functionality. In contrast, architectural content is best described in terms of how different layers of the Internet are, by design, intended to communicate with each other. Content is a product of how the network functions or, more specifically, how it was designed to function as a transport system for application data.

It is important to understand, however, that just because a particular unit of data is architectural content (or, of course, its complement, architectural metadata, defined in Section III.C) does not, by itself, imply that the data should or should not be afforded Fourth Amendment protections. That determination is a complex question, dependent on myriad factors particular to that unit of data. Indeed, the relevant facts and analysis can change in the course of data's transmission over the Internet.

As further illustrated in Part IV, whether a particular piece of information or data is content or non-content often depends on several different considerations. The architectural structure matters, but so does the perspective. This perspective may include which element — computer, router, network link — is monitored, and at which "stack" layer the observation takes place.[179] There are other considerations as well, notably ownership of the observation point.[180] A router in some-

179. *See* explanation of network stack, *infra* Section III.B.

180. We do not intend to address every element comprising the legal analysis of whether an individual unit of data is content or non-content or otherwise entitled to Fourth Amendment protections. But a complete legal analysis of whether or not a particular unit of data is afforded Fourth Amendment protections would, in many circumstances, require considera-

one's house, for example, is not operated by a third party, but the same type of router located in a hotel would be. In this example, the ownership of the observation point affects the determination of whether or not the third-party doctrine applies, and whether or not a particular piece of data is content or metadata.

Similarly, even within a single device, different layers may be operated by different parties. Such information is relevant to the determination of whether or not the third-party doctrine would apply when law enforcement seeks to compel data from a particular party.

We then look further at the definition of non-content found in the Pen/Trap statute, and explain how Dialing, Routing, Addressing, and Signaling ("DRAS") information[181] of the telephony world does not map well to the Internet and a rapidly innovating IP-based communications environment. Moreover, even in those circumstances where data can fairly be classified as DRAS, such categorization might not settle the question of whether the data is lawfully collected under a Pen/Trap relevance standard. As we discuss in Part IV, DRAS can be extremely revelatory. In such circumstances, the application of additional Fourth Amendment doctrine beyond the *Smith*/*Katz* distinctions may be necessary to determine the appropriate standard governing law enforcement access to that data.

These concepts are applied in Part IV, where we present a variety of examples of IP-based communications that demonstrate how current statutory and constitutional legal frameworks have become unworkable in an IP-based world. Many of these examples are technically complex. This should be no surprise. Had these issues been technically simple, the conflict between *Katz* and *Smith* and the IP-based world would long since have become apparent to courts. Yet despite problems arising from admittedly complex technical terrain, the issues raised by the examples are far from arcane. Those who legislate or adjudicate applications for law enforcement access to IP-based communications must understand, in detail, the technical aspects of the inquiry and analysis.

It is useful to begin by contrasting the Internet with the PSTN of the *Smith* era. We present a brief description, as complete characterizations of these communications networks are well beyond the scope and focus of this Article.[182]

---

tion of whether or not someone has a reasonable expectation of privacy in information *not* voluntarily given to a third party.

181. DRAS is essentially information on who is talking to whom. For an explanation of this concept in detail, see *infra* Section III.D.

182. For a detailed overview of how the PSTN worked back then, see generally Rey, *supra* note 90.

A. The Phone Network and the Internet

From the point of view of our analysis, there are two important differences between the PSTN and the Internet: where the intelligence lies and the complex layering of the Internet protocol stack.[183]

In the phone network, all intelligence is internal to the telephone company's central infrastructure: the phone switches. As the only elements of the network with any sophistication, the phone switches receive signaling information such as tones or dial pulses to complete calls." [184] At the time of the development of the telephone network, this design was a practical necessity: the phones of the time were very simple devices with no computing or storage capability, and rotary dial phones were almost completely electromechanical save for a few passive electronic components.[185] Rotary dial phones worked simply by interrupting the circuit at a rate of 10 pulses per second;[186] it was even possible to dial phone calls by tapping the hook switch at the proper rhythm.[187]

Due to this PSTN structure, the phone companies could offer only rudimentary services to their customers, notably dialing or answering a phone call. Requesting a service was easy: you took the phone off the hook and listened for a dial tone. You then dialed the number and the phone system would attempt to complete the call. This was the process understood by the justices in *Smith*.[188] It was correct up to a point.[189]

---

183. The "protocol stack" refers to how different aspects of a communication are accomplished. For more detail on the protocol stack, see infra Section III.B.

184. Modern phone switches are special-purpose computers; in 1979, though, many electromechanical phone switches were still in use. *See generally* Rey, *supra* note 90.

185. *See generally* A.H. Inglis and W.L. Tuffnell, *An Improved Telephone Set*, 30 BELL SYS. TECH. J. 239 (1951). Phones of that design still worked in the 1979 phone network and would likely still work today on classic twisted pair phone lines.

186. *See id.* at 256.

187. In 1980, Steven Bellovin designed a simple computer-controlled dialer that operated the same way: under software control. This was necessary because official ones leased from the phone company were far too expensive. This dialer was used for Usenet. *See* Sandra L. Emerson, *Usenet / A Bulletin Board for Unix Users*, BYTE, Oct. 1983, at 219, https://archive.org/stream/byte-magazine-1983-10/1983_10_BYTE_08-10_UNIX-page/n219/mode/2up [https://perma.cc/B7EA-M26U].

188. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (citing Victor S. Elgort, *Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028, 1028 n.3 (1975) (discussing the operation of pen registers)). Elgort described a pen register's function as "[a] pulsation of the dial on the line to which the pen register is attached records on a paper tape dashes equal in number to the number dialed." Elgort, at 1028 n.3 (quoting United States v. Caplan, 255 F. Supp. 805, 807 (E.D. Mich. 1966)). Though Elgort did go on to explain a touch-tone pen register, which printed out digits, other text in the note speaks almost exclusively of dial pulses, i.e., a rotary dial phone. *Id.*

189. By 1979, when *Smith* was decided, a few more sophisticated services, such as 3-way calling, were being deployed in the PSTN. *See generally* Rey, *supra* note 90.

The phone network's design meant that most services had to be provided by the telephone companies, a requirement that happened to align nicely with their business interests. A rotary dial phone's sole signaling mechanism created brief breaks in the circuit; once a call was completed, further breaks were not passed along as signaling information to the other end. An automated conference calling service couldn't exist as an endpoint (that is, as a device that connected to phone switches the way that phones themselves do), even a computerized endpoint, because there was no way for a rotary dial telephone to signal such a complex function. Elgort explains the requirements well:

> The dial pulses effectively operate within and for the benefit of the telephone company switching facilities in order to establish a connection with the desired party. Those pulses never reach the telephone of the intended recipient of the call. Moreover, if it is determined that the intended recipient of the *dial pulses* is actually the telephone company equipment, then the pulse would not be a "communication" to the intended recipient of the *conversation.*[190]

Indeed, on many phone switches, further circuit interruptions were perceived as requests for an operator to intervene in the call.[191]

Given this communications model, it was quite plausible for the courts to draw a bright line between content — a conversation, or perhaps a modem session — and metadata. Even then, though, life was not quite that simple. As many people who sought to save the cost of a call knew, the ringing of a phone could be a communication. In *United States v. Dote*, for example, the court noted that:

> The ringing of a telephone may be more than merely a signal indicating a call. Even if a call is not answered, a call at a certain time, or a certain number of rings, or repeated calls may well be a pre-arranged message or signal. *The ringing of the telephone, therefore, may of itself be a communication,* and a device, attached to the telephone line, which indicates to a third party that such a communication is taking place or is about to take place, intercepts it.[192]

---

190. *See* Elgort, *supra* note 188*,* at 1040 (emphasis in original).

191. *See* BELL LABORATORIES, BELL TELEPHONE LABORATORIES: ENGINEERING AND OPERATIONS IN THE BELL SYSTEM 690 (1st ed. 1978).

192. 371 F.2d 176, 181 (7th Cir. 1966) (emphasis added) (citation omitted).

Yet even by 1979, advanced features had started to appear in the phone network. There were speed-dialing codes, call-forwarding requests, and more. All of these services could be requested through digits dialed by a subscriber.[193] These requests, and in particular the number to which a call is forwarded, are clearly the contents of a communication with the phone company.[194]

Another relevant feature was the so-called "InWATS," an early form of today's 800 numbers.[195] InWATS was a form of call forwarding where calls to the 800 number were forwarded to a different number. The customer could designate the area from which such calls would be accepted. In addition, the number forwarded to could change with the time of day.[196] In other words, even in 1979 the numbers dialed did not necessarily correspond to the number of the instrument that actually answered.[197]

The narrowness of the functionality provided by the telephone network guided the Justices in *Smith.* But because technology was already beginning to provide more advanced services through dialed digits, the clear boundary between content and addressing information was beginning to blur. This obscuration is, however, nothing in comparison to how the Internet would collapse the traditional content/non-content distinction. We now turn to explaining briefly the underlying technology of IP-based communications.

B. An Introduction to the Network Stack

The Internet's architecture is quite distinct from that of the phone network.[198] On the Internet, the intelligence is at the edges, in the connected computers, rather than in the network itself. Colloquially, its design philosophy is often described as "smart hosts, dumb network" — the network itself is a simple "bit pipe" (in fact, network routing is quite complex).[199] While there are many factors contrib-

193. S*ee* TELCORDIA TECH., TELCORDIA NOTES ON THE NETWORKS, at 3–16 (2000); *see also* Rey, *supra* note 90, at 57, 420.

194. *In re* Application of United States for Order Authorizing Pen Register and Trap, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (questioning "[w]ould anyone doubt that . . . the government would be prohibited from obtaining this information on a pen register," though it was obtained by "post-cut-through dialed digit extraction").

195. InWATS stood for "Inward Wide Area Telephone Service." *See* U.S. Patent No. 4,191,860, at 57 (filed Jul. 13, 1978).

196. *See* Rey, *supra* note 90, at 63–64.

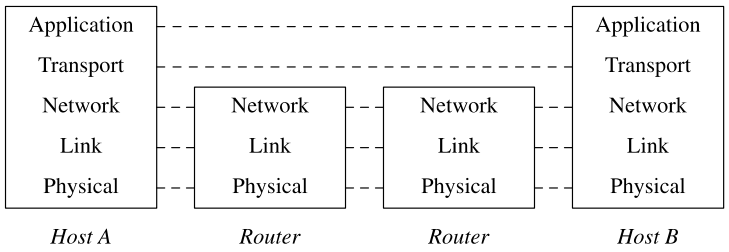
197. *Id.* Not all of these features were available on all phone switches, only the newer ESS (Electronic Switching Systems). *See id.* at 283; *see also In re* Application of the United States for an Order Authorizing the Installation of a Pen Register, 610 F.2d 1148, 1152 (3d Cir. 1979). At that time, only a small percentage of phone switches were ESS. *Id.* at 1153.

198. *See* Andrew S. Tanenbaum & David J. Wetherall, COMPUTER NETWORKS (5th ed. 2010) at secs. 1.5.1 and 2.6.

199. The origin of this colloquialism is hard to pin down but probably derives from the slightly different formulation in David Isenberg, *The Rise of the Stupid Network*, COMPUTER

uting to the change in design, a major one is simply the progress of technology: the essential architecture of the phone network was designed at a time when putting any but the most basic functions in telephones was technically and economically inconceivable. Furthermore, the PSTN is a circuit-switched network, in which each communication builds a circuit that it uses exclusively for the duration of a call. By contrast, the Internet is a packet-switched network; communications are broken into small packets, each of which, at least in theory, may be routed a different way through the communications network. The packets are then reassembled at the communications endpoint, where they are received as, for example, an email, video, or webpage.

In the conventional description, computer network technology is organized as a "stack." A canonical depiction of the network stack on the Internet is shown below.[200]



Each "layer" in the stack offers services to the layer immediately above it and requests services from the layer below it.[201] In addition, a layer on one device talks to the corresponding layer on some other device.[202] Knowing who owns the different devices is important for

---

TELEPHONY (August 1997) at 16. It in turn is based on principles first expressed in SALTZER, JEROME H., DAVID P. REED, AND DAVID D. CLARK. *End-to-end arguments in system design.* ACM Transactions on Computer Systems (TOCS) 2, no. 4 (1984) at 277. The oldest use of the exact phrase appears to be in a 2001 talk by BELLOVIN, *Host versus Network Security*, available at https://www.cs.columbia.edu/~smb/talks/Host-vs-Net/index.htm.

200. The original stack model had seven layers; however, layers 5 and 6, the session and presentation layers, are not used in the Internet architecture. *See* Tanenbaum *supra* note 198.

201. The layer names come from the reference architecture of the Open Systems Interconnection (OSI) standard, a now obsolete set of networking standards. From the bottom up, the layers are physical, link or data link, network, transport, session, presentation, and application. Often, the layers are referred to by number, rather than by name. Though the OSI protocols are largely defunct, the terminology has lived on even though it is not a perfect match for today's Internet architecture. For example, on the Internet there are no equivalents to layers 5 (session) and 6 (presentation); however, some of the layer 6 functionality often appears as part of the application layer. *See generally* Tanenbaum *supra* note 198.

202. Generally speaking, layers do not talk directly to non-adjacent layers. If they need information from one — for example, applications may need to know an IP address, which

understanding to whom a given message is sent and hence whether or not a particular exchange involves a third party. Such understanding is often relevant to determining whether the data involved in a particular exchange is content or metadata.[203] Thus, we note that the data in the application and transport layers are not processed by intermediate routers in the Internet; the communications in those layers are end-to-end communications from Host A to Host B.

Protocols govern the communications between layers and between devices on the same layer. The Internet Protocol ("IP"), which is the "network layer," is concerned with getting packets from a source computer to a destination computer.[204] IP hands packets to and receives packets from the "link layer." The "transport layer" — usually Transmission Control Protocol ("TCP")[205] — turns the packets into a reliable stream for applications.[206]

All layers except the physical and application layers consist of a "header" and a "payload."[207] The header is the information processed by that layer; its payload is all of the higher layers. Consider an Ethernet packet (in the link layer). It has a 14-to-18 byte header; the remaining 1500 bytes of the packet are the network layer header, the transport layer header, and the application data.[208] We refer to the payload of a layer as its architectural content, explained above in Part I.

---

is a property of the network layer — the request is routed through the adjacent layer, in this case transport. *See generally* Tanenbaum *supra* note 198.

203. *See* discussion of architectural content, *supra* Part I. In order to determine whether the Wiretap Act was violated in a case where URLs were disclosed to third party sites, Kerr's examination begins with the analysis and identification of the actual parties to a communication. Kerr reasons, "I'm skeptical that URLs are non-content information in an absolute sense. If a true third party installed a monitoring tool that intercepted every URL that a person visited in the course of delivery from the user to the other party to the communication, then there's a good argument that the URLs are contents for the leg of the communication from the user to the recipient." Orin Kerr, *Websurfing and the Wiretap Act*, VOLOKH CONSPIRACY (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ [https://perma.cc/5GDJ-E9F3].

204. *See* JON POSTEL, INTERNET PROTOCOL (RFC 791) (1981), https://www.ietf.org/rfc/rfc791.txt [https://perma.cc/5KFZ-LXY8] [hereinafter RFC 791].

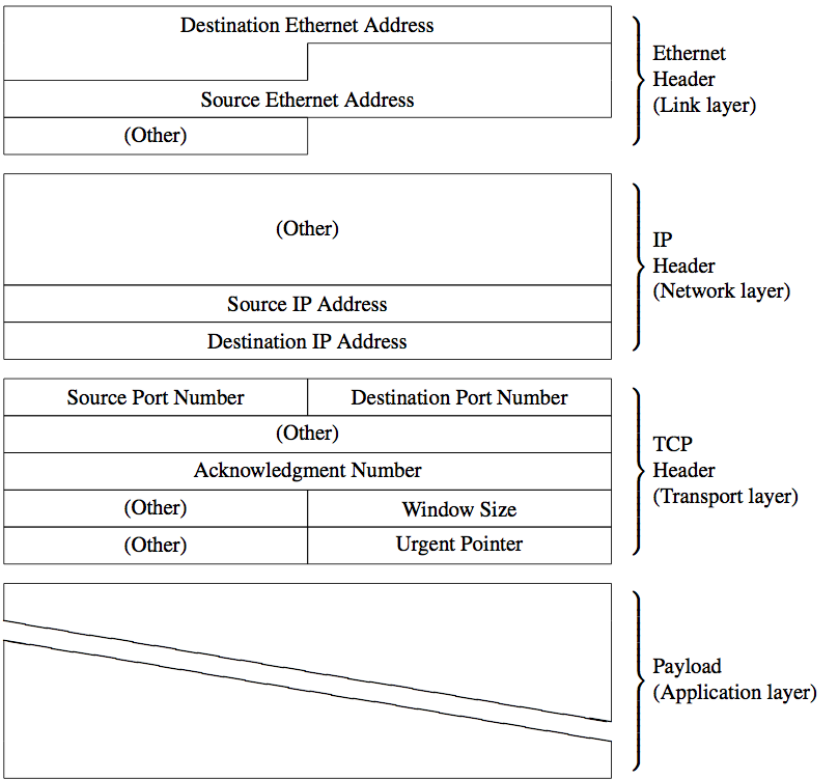
205. *See* JON POSTEL, TRANSMISSION CONTROL PROTOCOL (RFC 793) (1981), https://tools.ietf.org/rfc/rfc793.txt [https://perma.cc/3BMD-2E3B] [hereinafter RFC 793].

206. There are other, less frequently used transport protocols. The issues they present are largely similar, and we do not discuss them here. *See, e.g.*, JON POSTEL, USER DATAGRAM PROTOCOL (RFC 768) (1980), https://www.ietf.org/rfc/rfc768.txt [https://perma.cc/9MTP-A89Y].

207. Arguably, there is a physical layer header for some media; this may be used to determine where a packet actually starts. On Ethernet, for example, there is a prologue of up to 64 bits. If the application layer has sublayers, there may be headers present there, too. IEEE COMPUTER SOC'Y, IEEE STANDARD FOR ETHERNET 53 (2012).

208. Strictly speaking, Ethernet packets also have a 4-byte trailer used for error detection. *Id.*

A diagram of a typical packet is shown below.[209] There are several things worth noting. First, three different levels of the stack — the link, network, and transport layer — have addresses. However, as we explain in this Article, just because something is an "address" does not mean that it is accessible to law enforcement under the third-party doctrine. Second, all of the lower layers have fields that are neither DRAS nor "content" as defined in the Wiretap Act. Finally (and in the interests of simplicity we will omit a detailed explanation), all of these headers can contain other, optional fields that themselves may or may not be accessible via the third-party doctrine.



209. The Ethernet header is taken from the IEEE Standard for Ethernet. *See id.* at 53. The IP header is from RFC 791. *Supra* note 204, at 11. The TCP header is from RFC 793. *Supra* note 205, at 15. It is regrettable but nevertheless conventional that in stack diagrams the application layer is always shown at the top whereas in packet diagrams it is shown at the bottom.

The lowest layer of the stack, the "physical layer," covers the physics of communication: the radio frequencies used, the voltages for traditional Ethernet, and more. This part of the architecture seems innocuous enough, but radio signals emitted from different sources at this layer are subtly different; this difference can be used to "fingerprint" and thus identify transmitters.[210] While law enforcement collection of data at this layer raises potential statutory and constitutional issues, these issues involve the characteristics of radios, rather than their use in the Internet per se, and thus we do not discuss them further.

The link layer provides the protocol mechanisms needed to send and receive packets on a single network. In the cases of interest here, a "network" is typically either a Local Area Network ("LAN"), such as Wi-Fi or Ethernet, or a wireless network of the type used for mobile devices. The link layer defines the format of the packets to be sent or received. There may also be special messages defined. Wi-Fi networks, for example, use special packets to announce their existence; these contain the network names[211] that many computers make visible.

Many common networks can have multiple nodes connected to them. Accordingly, link layers frequently contain source and destination identifiers. Because link-layer addresses are identifiers, they are subject to collection under Pen/Trap orders. They can also be used to identify which packets are authorized for collection under a specific wiretap order. The utility of Medium Access Control ("MAC") addresses (hardware addresses that uniquely identify each node on a network) for these purposes is limited, since as noted they stay on-network. Under certain circumstances, for example, if a law enforcement agent and a suspect are both using the same Wi-Fi hotspot, MAC addresses can be useful. It is important to realize that though normally these identifiers stay on-network, under certain circumstances they may be sent elsewhere.[212]

Link layers are sometimes responsible for access control to and encryption of their networks; the WPA2 encryption protocol for Wi-Fi is a well-known example. These mechanisms may also involve identi-

---

210. *See, e.g.*, Cellular Telephone Anti-Fraud System, U.S. Patent No. 5,448,760, at [57] (filed Sep. 5, 1995) (describing how to prevent cellphone cloning by looking for the fingerprint of the authorized phone); *see also* Kasper Bonne Rasmussen & Srdjan Capkun, *Implications of Radio Fingerprinting on the Security of Sensor Networks*, 3 PROC. INTERNATIONAL CONF. ON SECURITY AND PRIVACY IN COMM. NETWORKS 331 (2007).

211. Technically these are called Service Set Identifiers (SSIDs).

212. *See* S. THOMSON ET AL., IPV6 STATELESS ADDRESS AUTOCONFIGURATION (RFC 4862) 22 (2007), https://tools.ietf.org/pdf/rfc4862.pdf [https://perma.cc/JKN5-TC5E] (describing the problem); *see also* T. NARTEN ET AL., PRIVACY EXTENSIONS FOR STATELESS ADDRESS AUTOCONFIGURATION IN IPV6 (RFC 4941) at 1 (2007), https://tools.ietf.org/pdf/rfc4941.pdf [https://perma.cc/2H2G-KYTW] (describing a solution to the problem in RFC 4862).

fiers, though often the MAC address is used. In fact, even on encrypted Wi-Fi networks the MAC addresses are transmitted unencrypted; this can be useful even if the encryption conceals the IP or email addresses being transmitted or received.[213] Furthermore, under certain circumstances, Wi-Fi-connected nodes will broadcast the identifiers of networks they frequently connect to,[214] which can also identify a system.

The issue of what data is shared during transmission is more complex in IP-based communications systems than in the PSTN and thus warrants close examination. IP, the network layer, is the lowest end-to-end layer;[215] that is, the network layer and above is transmitted more or less unchanged from the sender of a packet to a recipient. The IP header contains only the information necessary to send a packet to its destination. In an ordinary Internet transmission — one that uses one or more ISPs to reach the destination — third parties must examine and, to some extent, modify the network layer header. In particular, the source and destination network layer addresses — IP addresses[216] on the Internet — are set by the sender, examined by every router along the path,[217] and received by the ultimate destination. These routers are parties to IP layer communications because they must examine these addresses. Furthermore, IP addresses were once effectively fixed:[218] a host received its IP address when it was first

213. Because the default MAC address of a Wi-Fi interface is manufactured into a device, the presence of a known MAC address on a network suggests that the device, and hence its owner, are present on that network. This could, for example, be used to confirm that a suspect's phone was in a house, though only from quite nearby. The range of Wi-Fi is about 100 meters. *See generally* IEEE 802.11: WIRELESS LAN MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL LAYER (PHY) SPECIFICATIONS (2012) [hereinafter IEEE 802.11].

214. *See* Dan Goodin, *Loose-Lipped iPhones Top the List of Smartphones Exploited by Hacker*, ARS TECHNICA (Mar. 16, 2012, 11:25 AM), http://arstechnica.com/apple/2012/03/loose-lipped-iphones-top-the-list-of-smartphones-exploited-by-hacker/ [https://perma.cc/N5YB-J4K9].

215. "End-to-end" means a communication from the original sender of a message to its ultimate recipient. The IP header fits this definition, though some of its fields may be changed en route and most of it may be inspected by routers along the path. By contrast, link layer information is not preserved by routers; the next-hop link layer headers will bear no relation to the link-layer headers of the inbound packet. *See* Tanenbaum & Wetherall, *supra* note 198, at sec. 1.4.1.

216. An IP address is analogous to the street address of a building.

217. A router is a low-level, intermediate node on the Internet. Routers link different networks; they examine the destination IP address of every packet to decide to which adjacent router the packet should be forwarded.

218. IP addresses are reused and may not be unique across the Internet at any given time. *See* B. CARPENTER ET AL., IPV4 ADDRESS BEHAVIOR TODAY (RFC 2101) at 4–8 (1997), https://tools.ietf.org/pdf/rfc2101.pdf [https://perma.cc/SH8Y-PGNG]; *see also* P. SRISURESH & K. EGEVANG, TRADITIONAL IP NETWORK ADDRESS TRANSLATOR (RFC 3022) (2001), https://tools.ietf.org/pdf/rfc3022.pdf [https://perma.cc/QU4K-WFJH] [hereinafter RFC 3022] (explaining network address translators).

attached to its local network, and this address never changed.[219] Many hosts are now mobile and thus must receive a new address when they connect to a different network; this is typically done automatically. That IP addresses are now assigned dynamically complicates the actual process of monitoring a host's traffic based on the target's IP address; the monitoring station needs to learn the proper IP addresses each time it changes.[220] All this activity points to the role of intermediate third parties in examining IP addresses.

The transport layer, which is responsible for delivery of data to applications, is strictly end-to-end. The contents of the TCP header are created by one end system and are relevant only to the peer TCP at the other end of the connection. Unlike the network layer, intermediate routers do not examine or otherwise rely on TCP. In other words, the data transmitted between peer TCP is not, from an Internet design perspective, shared with other parties. The only true party to TCP communications is the TCP peer at the other end of the connection.

For our purposes, there are two salient features of TCP. First, it contains port numbers. A port number is an address within a computer. If an IP address is similar to a building address, a port number more or less corresponds to a room in the building. Some port numbers are well known (at least to implementers). Web servers, for example, respond to requests on port 80.[221] Other port numbers are used for the other side of a connection. A TCP connection is uniquely identified by the 4-tuple (source IP address, destination IP address, source port, destination port). When a web browser, for example, connects to a web server, the browser's TCP will assign it a random port number in the range 49152-65535,[222] while the web server it is contacting will be on port 80. Second, the TCP header contains the information concerned with connection setup and maintenance. Unlike in the phone

---

219. This is slightly different for IPv6. *See* S. DEERING & R. HINDEN, INTERNET PROTOCOL, VERSION 6 (IPV6) SPECIFICATION (RFC 2460) (1998), https://tools.ietf.org/pdf/rfc2460.pdf [https://perma.cc/BD6V-GY2H]. The differences are not relevant for our purposes.

220. ISPs generally keep logs of who has been assigned a given address at a given time. Public hotspots, however, might not retain such records, especially if no login is required.

221. Well-known port numbers are assigned by the Internet Assigned Numbers Authority (IANA), s*ee Service Name and Transport Protocol Port Number Registry*, THE INTERNET ASSIGNED NUMBERS AUTHORITY (IANA), http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=2 [https://perma.cc/GD24-HHSD], under the direction of the Internet Engineering Task Force. Assignments can be looked up on its web site, though in general client programs know what port the corresponding server will use. Continuing our building analogy one can imagine that the mail room is always #25, the help desk is room #80, etc. *See supra* note 216.

222. *See* M. COTTON ET AL., INTERNET ASSIGNED NUMBERS AUTHORITY (IANA) PROCEDURES FOR THE MANAGEMENT OF THE SERVICE NAME AND TRANSPORT PROTOCOL PORT NUMBER REGISTRY (RFC 6335), at 20 (2011), https://tools.ietf.org/pdf/rfc6335.pdf [https://perma.cc/5PX5-KVFK].

system, these headers are end-to-end; they are not processed by the network.

There are other, harder-to-explain fields in the TCP header. Some can be used for such arcane functions as "passive OS fingerprinting."[223] Fingerprinting can disclose how many computers are in a residence, what brands they are, and more.[224] While there may be legal questions about whether people have a reasonable expectation of privacy in the TCP header fields, it is beyond dispute that such information is not normally given voluntarily to third parties.[225] From a law enforcement perspective, however, OS fingerprinting is an important part of the "reconnaissance" necessary before trying to penetrate a system.[226]

There are a number of deep architectural principles implicit in the Internet architecture. The network — the routers and the links that connect them — is concerned solely with packet delivery from a source IP address to a destination IP address. Most importantly, applications — the programs such as mailers, web browsers, remote disk connections, and more that are most familiar to users — lie at the highest layer, and are the province of end hosts,[227] not of the network. The application layer is the one most familiar to users and of most interest to us.

An essential architectural difference between the PSTN and the Internet is that services are not provided in the network but on the "edges." This has many implications, including the fact that an ISP has less insight into the network than a telephone service provider does. If an ISP chooses to offer a mail service, its mail servers connect to the network in exactly the same way as any other mail server. The only salient difference is that there may be a higher speed, i.e., one traversing fewer routers or via faster links, to the captive offering than to a third party's offering.[228] In other words, the ISP's mail server

---

223. OS fingerprinting determines what version of what operating system a particular computer is using; passive fingerprinting does it simply by observing traffic, rather than by seeing how a computer responds to probes. *See, e.g.*, MICHAEL ZALEWSKI, P0F V3: PASSIVE FINGERPRINTER, http://lcamtuf.coredump.cx/p0f3/README [https://perma.cc/529V-VXU6].

224. There are other things that can be learned such as the income level of the owners (stemming from the fact that Macs are more expensive than Windows computers). Kyllo v. United States, 533 U.S. 27 (2001) raises related issues, but we do not discuss them in this Article.

225. The IP layer also has such fields; however, since IP is not end-to-end, *see supra* note 215, this information is generally given to third parties.

226. The subject of lawfully authorized system penetrations is very complex. Many aspects of it, including the need for a reconnaissance phase, are discussed in *Lawful Hacking*, *supra* note 37 and Section IV.D.

227. A host can be a computer of any sort: a desktop or laptop, a server, a smartphone, a specialized computer controlling an industrial process, etc.

228. To help fight spam, most ISPs restrict access to their outbound email servers. Many ISPs run their networks in such a way that a local IP address alone is sufficient authentica-

behaves just like Google's or Yahoo's, running a full network stack with mail at the application level. Architecturally, though, the connectivity is identical. Individuals can also run their own mail servers; two of the authors of this Article do precisely that. One therefore cannot assume that just because mail is being sent, a third party is involved in handling the email.

C. Architectural Content

When *Smith* was decided in 1979, the phone network seemed simple. There were roughly three things one could do with a telephone: dial, talk, or answer a ringing phone.[229] Given the state of the technology, it made sense to have different rules for government interception of the dialed numbers and actual conversations. The interpretations and definitions, then, mimicked this understanding: "pen registers do not accomplish the 'aural acquisition' of anything."[230]

The same concepts can be expressed in modern computer science terminology. The phone network has a relatively simple "interface" or "service definition": that is, how two components communicate. Such an interface will specify inputs (what one component may send to another) and outputs (what is returned in response to inputs). Note that one of the components is the telephone's user. For the phone network of the late 1960s and 1970s — the time of the *Katz* and *Smith* rulings — the services were dialing, talking, answering, and operator-assistance. There was tremendous internal complexity, but little of that was visible to ordinary users.

By contrast, the Internet has a far richer service definition.[231] Apart from the user-visible services such as email and web browsing, there are complex network and programmatic interfaces.[232] A modern,

---

tion; if there is abuse, it is easily linked to a particular account. By contrast, externally facing outbound mail servers need to rely on passwords and the like. In practice, users do not see the difference. The password they supply for retrieving email is used for sending as well. Additionally, even users of their local ISP's mail service have to use a password when sending mail if they use a laptop or phone when not at home. There is thus no perceived difference in the user experience.

229. In fact, there were more complex operations, such as busy number verification. However, most of these were performed by human operators. For the Court in *Smith*, the presence of a person made the question quite simple: "[p]etitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy." Smith v. Maryland, 442 U.S. 735, 744 (1979). Newer services, such as subscriber-controlled call forwarding, were just starting to appear; their import was likely unclear even to law enforcement. Similarly, the issue of actual dialing information appearing in the content of a call, as MCI's early offerings required, had not yet been raised. *See supra* notes 13 and 15.

230. United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977).

231. This difference is a major reason why the Internet has so many more security problems. *See* WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER xi–xii (1994).

232. The conceptual interface to TCP is given in RFC 793, *supra* note 205, at 44.

or at least updated, understanding of the difference between content and metadata must therefore follow suit. We formally define "architectural content" to mean information that — from a given point in the network and network stack — is simply transported, unexamined, even if it is not "information concerning the substance, purport, or meaning of that communication."[233] We define its complement, "architectural metadata," as information intended for the potential use of a particular layer in the stack.[234] These two concepts are at the heart of our analysis.

Content defined by structure or architecture — as opposed to by substance or meaning — is not an entirely new concept. In *Ex Parte Jackson,* the Court provided Fourth Amendment protections to the interior content contained in packages and sealed letters, but exempted the "outward form and weight" of the parcels from those protections.[235] In performing a structural analysis of a package, however, the Court only needed to recognize and account for two layers with exceedingly clear boundaries: the inside and outside of the package. As we will see in Part IV, the boundaries of the layers of the Internet stack are not always so clear.

The easiest place to understand the definitions of communicative and architectural content in the context of the Internet is through the lens of processing a TCP/IP packet in a router.[236] The TCP payload, or the data being transmitted from application to application like the contents of an email message or web page, is content even under the current statutory definition of "substance, purport, or meaning."[237] But in addition, the TCP header and payload are *architectural content*, because routers look only at the IP header. At this layer, the IP header is architectural metadata. We call this "architectural" because the boundary is defined by the architecture of the Internet and of the relevant protocols.[238] It is fundamental to the design of the Internet that TCP is end-to-end (i.e. not processed by intermediate routers). Similarly, TCP is agnostic to the characteristics of the applications that rely on it. As long as TCP's service definition is suitable — a bidirectional, reliable byte stream, with a connection setup phase and with no boundaries between messages — TCP can be used. TCP and its pay-

233. 18 U.S.C. § 2510(8) (2012). For a detailed discussion of the Wiretap Act's definition of content, *see supra* Section II.A.

234. Note that architectural metadata often includes information not directly useful for identifying an endpoint as described in the definition of a trap and trace device. *See* 18 U.S.C. § 3127(4) (2012). For example, the content of the IP Header Checksum, *see* RFC 791, *supra* note 204, at 11, 14, is completely determined by that of the other fields in the IP header; it adds no information useful in ascertaining the source or destination of a packet.

235. *Ex parte* Jackson, 96 U.S. 727, 733 (1878).

236. *See* discussion *supra* Section III.B.

237. 18 U.S.C. § 2510(8) (2012).

238. Each layer performs a different function, and only certain, limited information can pass between layers. *See generally* Tanenbaum & Wetherall, *supra* note 198, at sec 1.4.

load are thus architectural content to IP, and the application layer is architectural content to TCP.

We caution that applying this definition requires great care. In some situations, boundaries are clear, but as we illustrate in Part IV the line is fuzzier in others. In those cases, architectural content and metadata can be intermingled.

D. Defining DRAS

In this Section, we turn to technical definitions used in academic and engineering literature describing the phone network and the Internet to clarify the statute's reach. As noted in Part II, the Pen/Trap statute does not define "dialing, routing, addressing, and signaling information," save to say that they are "transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[239] In its 2005 Electronic Surveillance Manual, the DOJ argued that the new terms added to the Pen/Trap statute extended the statute's reach to essentially all technologies.[240] The rationale for this interpretation is based on the scant legislative history found in a House Report[241] and does not appear to reflect deep technical analysis or understanding of the technical meaning of these terms.

How do the DRAS terms match to the Internet? We compare PSTN and Internet versions of these functions, going in order of complexity of the Internet versions: dialing, signaling, addressing, and routing. The problem starts immediately. There is no Internet analogue to dialing. The closest analogue is an explicit user request to connect to some Internet site. However, as is discussed in detail in subsequent parts, when, if, or to where a connection is made is quite complex and often does not reflect explicit user actions. Most of the other terms similarly do not map well to the Internet domain.

Because of the Internet's layered architecture, DRAS can appear in many different places. As noted, the link, network, and transport layers all have addresses;[242] furthermore, some applications, such as email, have addresses as well.[243] Each must be considered separately.

One standard telephony work defines signaling as "the process of transferring information between two parts of a communications network to control the establishment of connections and related operations."[244] It goes on to define "customer-line signaling" as "the

239. 18 U.S.C. § 3127(3) (2012).

240. *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, at 47. Relying on the House Report, DOJ suggests that when passing the final bill "Congress intended that the statute would apply to all technologies." *Id.* (citing H.R. 107–236 at 52–53).

241. *Id*.

242. *See* discussion *supra* Section III.B.

243. *See* discussions *infra* Sections IV.B & IV.C.

244. Rey, *supra* note 90, at 265.

interaction between the customer and the switching system that serves the customer."[245] This latter description, of course, includes "dialing"; it also includes "ringing of your phone (someone is calling), dial tone (it's OK to dial), ringing (one hopes that someone will answer), etc."[246] In the phone system, the network participates in the signaling dialog. That is, the various phone switches along the path need to know about each call and to allocate resources — the "voice path" — for it.[247] The signaling messages include both the called number and the calling party number.[248] Access to these messages is sufficient to implement both pen register and trap-and-trace functionality at the phone switch, with no need to attach any equipment to any particular phone lines.

Although signaling on the Internet has the same meaning as in the PSTN — a set of messages involved in setting up or tearing down a connection — the term is not a good match for the purpose of identifying endpoints to a communication under the Pen/Trap statute. The crucial difference is that, on the Internet, routers are not involved in setting up a TCP connection. As explained above in Section III.B, TCP connections are end-to-end, from client host to server host.[249] In other words, signaling exists on the Internet, but it is end-to-end — it is part of TCP and third parties do not generally participate in the transmission of TCP fields. As part of TCP, signaling information is architectural content to the IP layer. As discussed in Part II application of the Pen/Trap statute and its relevance standard for compelling third parties to disclose information to law enforcement is based on the third-party doctrine, which depends on the existence of a third party, but there are no third parties involved in Internet signaling.

There is sometimes signaling at the link layer of the Internet. For example, Wi-Fi-connected devices "associate" with access points.[250] This association, though, is for a "session," and is unrelated to any individual connection.

It is harder to find analogues to signaling at the application layer, at least in any form useful to law enforcement. There is a short dialog

245. *Id.*

246. *See* HARRY NEWTON ET AL., NEWTON'S TELECOM DICTIONARY (27th ed. 2013) (definition of "signaling").

247. *See* Rey, *supra* note 90, at 280.

248. *See* NEWTON, *supra* note 246 (definition of "signaling information fields").

249. *See* RFC 793, *supra* note 205, at 28 (TCP connections are established by the so-called "three way handshake").

250. *See generally* IEEE 802.11, *supra* note 213, at section 6.3.7.2.

at the start of each SMTP session;[251] most of it concerns technical parameters of the connection.[252]

PSTN "addressing" is straightforward. It is "the task of specifying to the network the destination of a call";[253] an "address" is "a unique 10-digit number assigned to a main station,"[254] i.e., a phone number. On the Internet, there are relevant addresses at the link, network, transport, and application layers; all of these may be relevant.

Link layer addresses remain reasonably close to the owning computer.[255] They are most useful in confirming the presence of a particular device at a particular location such as a public Wi-Fi hotspot.

IP addresses seem more useful and more straightforward. A pair of IP addresses, that of the sending node and of the intended recipient, is in the IP header of every packet; these are used by every router along the path from its source to its destination. Reality is substantially more complex.

The first issue is that the actual destination of a packet is determined not just by its IP address but also by the port number. It is far from obvious that the "service requested" — that is, the port number — is not part of the "address."[256] For example, we type "www.example.com" or "mail.example.com," depending on whether we want to talk to the web service or the mail service of a particular organization. But the port number is in the TCP header and is thus architectural content to IP. In theory, then, it is not given to or used by intermediate routers. Again, though, reality is more complex.

Although ISPs are not given TCP port numbers, they effectively take them.[257] One example of ISPs taking architectural content is that many use the NetFlow protocol to monitor load on their networks.[258] NetFlow records include not just port numbers but also the TCP head-

---

251. *See* J. KLENSIN, SIMPLE MAIL TRANSFER PROTOCOL (RFC 5321) (2008), https://tools.ietf.org/pdf/rfc5321.pdf [https://perma.cc/QAC9-8JG8] [hereinafter RFC 5321]. SMTP is the network protocol used to transmit email messages; *see infra* Section IV.B.

252. There is an optional authentication dialog; if it is used without encryption (which is legal but unusual), law enforcement could learn the identity of someone sending email, but (from this dialog) not the recipients. It is unclear if this should even be considered signaling, since it is connection-specific and not message-specific; for that reason, and because if encryption is not used, the "From:" lines are equally visible, we will not discuss this further.

253. Rey, *supra* note 90, at 85.

254. *Id.* at 115.

255. *See* discussion *supra* Section III.B.

256. Indeed, one of the authors of this article explicitly advocated making the service part of the IP address. *See* S. BELLOVIN, ON MANY ADDRESSES PER HOST (RFC 1681) (1994), https://tools.ietf.org/html/rfc1681 [https://perma.cc/4QYV-3EUY].

257. *See, e.g.*, CISCO SYSTEMS, INC., GATEWAY SYSTEM MANUAL at 10-5, (July 1988), http://archive.computerhistory.org/resources/access/text/2013/04/102721279-05-01-acc.pdf [https://perma.cc/G8QD-EXCV].

258. *See NetFlow Services Solutions Guide*, CISCO SYSTEMS, INC. (2001), http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/netflow/nfwhite.html [https://perma.cc/WX3T-EMX7].

er bits that are used in signaling messages.[259] It is not obvious why ISPs, whose primary concern is monitoring traffic levels to determine the levels of bandwidth needed, should care about what services their customers use.[260] Some ISPs do, however, monitor this data, which means that a third party is examining architectural content. Does this make port numbers accessible via the third-party doctrine? A further complexity arises because the Internet has effectively run out of IP addresses.[261] Network Address Translators ("NATs")[262] are devices that enable a single IP available on the outside of a local network to act as multiple addresses on the inside; it is as if there were a single phone number to a company that had multiple extensions inside — but which you could only reach by dialing the main number. Most public Wi-Fi hotspots provide customers with "private IP addresses";[263] these addresses are translated at the border of the hotspot's network to "global" IP addresses. Cellular phone companies do the same for data connections from smartphones that are using their networks. The technical details of the translation are not important; what is relevant is that a NAT box operation necessarily includes examination of and modification to various TCP header fields, including the port numbers and the TCP flags field.[264] In other words, a network element run by a third party is accessing information that is architectural content, not information intentionally shared with a third party. Again, does this mean that this information is covered by the third-party doctrine?

Email addresses are, of course, of great interest to law enforcement. They are more closely tied to an individual than a device is,[265] and email is a common means of communication between multiple

---

259. *Id.* at Appendix 2. Note in particular the "tcp_flags" field. This field of the TCP header includes the so-called "SYN" (connection start) and "FIN" (connection end) bits. *Id.; see also* RFC 793, *supra* note 205, at 12, 16.

260. Recall that port numbers often indicate which services are being used. See discussion *infra* Section III.B.

261. Because it was clear in the early 1990s that the Internet would exhaust IP addresses, *see* C. PARTRIDGE & F. KASTENHOLZ, TECHNICAL CRITERIA FOR CHOOSING IP THE NEXT GENERATION (IPNG) (RFC 1726), 7 (1994), https://tools.ietf.org/pdf/rfc1726.pdf [https://perma.cc/ZB7T-B8S5], the Internet Engineering Task Force (IETF) designed and standardized IP version 6, which has a vastly larger address space. However, uptake of IPv6 has been much slower than was anticipated.

262. *See generally* RFC 3022, *supra* note 218 (explaining network address translators).

263. *See* Y. REKHTER ET AL., ADDRESS ALLOCATION FOR PRIVATE INTERNETS (RFC 1918) (1996), https://www.ietf.org/rfc/rfc1918.txt [https://perma.cc/9C57-PLVC].

264. In fact, in some circumstances a NAT box must examine and modify information that is indisputably content per the statutory definition. For example, the File Transfer Protocol has a subcommand "PORT" that contains the IP address and port number associated with a data connection. *See* J. POSTEL & J. REYNOLDS, FILE TRANSFER PROTOCOL (RFC 959), 28 (1985), https://tools.ietf.org/pdf/rfc959.pdf [https://perma.cc/M7CK-X6ZB]. These values are changed by NATs. There are other protocols with similar properties.

265. Many people use multiple devices, e.g., phones, tablets, and computers. Conversely, some devices, such as home computers or those in Internet cafes, are often shared.

parties in ongoing criminal enterprises. Equally important, they represent the technical endpoints of a communication and are often visible on third-party-operated servers.[266] For those reasons, they are specifically called out in the DOJ's electronic surveillance manual as accessible via a Pen/Trap order,[267] an issue we will discuss further in Section IV.B.

"Routing" is rather complex in the phone network. The term "routing" is used in many different places in Signaling System 7, the set of signaling protocols used for establishing and ending telephone calls.[268] However, many of these references refer to the general networking concept of routing and have nothing to do with identifying the endpoints of a given call.[269] The interest in surveillance activity has to do with determining which phone actually receives a call, as opposed to the number dialed.[270] Of course, due to various advanced switching features, which phone receives the call and which number was dialed could differ for a number of reasons, including dialing an 800 number,[271] number busy or unanswered,[272] local number portability,[273] and call forwarding;[274] this is presumably why the term was included in the pen/trap statute.

The Internet also "routes" communications through the network,[275] but the route used is a function of the state of the network at the instant a packet is sent rather than an attribute of a particular con-

---

266. *See* discussion *infra* Section IV.B.

267. *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, at 39.

268. Signaling System 7 was put into place in the 1970s and is widely used throughout the world. *See* PERFORMANCE TECHNOLOGIES, TUTORIAL ON SIGNALING SYSTEM 7 (SS7), http://www.eurecom.fr/~dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf [https://perma.cc/52C7-EUES].

269. *But cf.* 18 U.S.C. § 3127(4) (2012) (explaining that the purpose of a trap-and-trace device is to identify the endpoints of a communication). Our intention for emphasizing this part of the statute is to illustrate further how DRAS definitions do not map well to the Internet. We discuss networking routing in the context of the Internet. *See* discussion *infra* Part IV. The definition of pen register, found in 18 U.S.C. § 3127(3) (2012), however, does not contain a purpose statement.

270. *See* 18 U.S.C. § 3127(4) (2012) (defining a "trap and trace device" as a device which identifies information "likely to identify the source of a wire or electronic communication").

271. *See* PERFORMANCE TECHNOLOGIES, *supra* note 268, at 4.

272. *See id.*

273. Local number portability enables a user of a fixed line to switch service providers yet maintain the same phone number. *See How LNP Works*, NUMBER PORTABILITY ADMINISTRATION CENTER, https://www.npac.com/number-portability/how-lnp-works [https://perma.cc/AQ2T-YRRU]. The local number portability database is important to wiretaps for another reason: it indicates which phone company actually serves a given phone number, and hence which company can implement a wiretap order. *Id.*

274. *See* PERFORMANCE TECHNOLOGIES, *supra* note 268, at 3.

275. JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH 4 (6th ed. 2013) ("The sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a route or path through the network.").

nection.[276] Thus, routing messages do control the path that packets take through the Internet, but they do not concern particular connections.[277] There is often similar functionality at the link layer, with similar caveats about its lack of utility to law enforcement. There are times when law enforcement investigators might be interested in collecting routing data (e.g., for investigations regarding IP hijacking — routing IP packets to incorrect destinations by corrupting IP routing tables).[278] But collecting such information was not an identified purpose of the Pen/Trap statute.[279]

The question of email routing is more complex. We defer a detailed discussion of it until Sections IV.B and IV.D. For now, let it suffice to say that, generally speaking, email is routed through several servers, and this route is recorded in the email message itself.

There is thus some ambiguity in how signaling and addressing is or should be understood on the Internet. In the original design, port number and other TCP header fields were purely architectural content. As the Internet is run today, however, service providers take some interest in these fields, even when arguably they should not. We therefore, at times, have third parties in possession of these fields. As we will illustrate in Section IV.F, the disclosure or possession of this information by third parties (i.e., those parties which are not the peer endpoints) is generally not known by most Internet users. This situation highlights the problem of applying the third-party doctrine on the Internet; for most users, these conveyances will not be knowing and voluntary. In addition, determination of whether the information is content, and therefore appropriately collected under the Pen/Trap relevance standard, is complicated when non-end-to-end peer entities come into possession of some of these fields.[280] Neither the statutory

276. Strictly speaking, a feature called "IP source routing" can be used to control the path of individual packets. It is almost never used in today's Internet. No standard applications support specification of explicit source routes, and many sites and ISPs block it because of security concerns, *see* S.M. Bellovin, *Security Problems in the TCP/IP Protocol Suite*, 19 COMPUTER COMM. REV. 32, 35 (1989), and network performance issues.

277. This difference is a necessary consequence of the fundamental design principle stated earlier: in the Internet the network does not participate in setting up connections. Furthermore, understanding the path taken by a given packet requires detailed knowledge of not just the routing messages being sent but also the internal topologies and policies of every ISP along the path. How routing protocols work and how they interact with each other is probably the single most complex feature of the Internet.

278. *See* Pierre-Antoine Vervier et al., *Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks*, INTERNET SOC'Y (Feb. 2015), http://www.internetsociety.org/sites/default/files/NDSS2015_Mind_Your_Blocks_Stealthiness_Malicious_BGP_Attacks.pdf [https://perma.cc/CT92-T4PW].

279. *See* 18 U.S.C. § 3 (2012).

280. As is discussed in Section III.B, email is usually, but not always, relayed by third parties.

definition of "content"[281] nor our notion of "architectural content"[282] provides an adequate basis for deciding whether or not they are available under the third-party doctrine.

For the phone network, the phrase "dialing, routing, addressing, and signaling" was intended to preserve traditional surveillance abilities such as determining which phone receives the call, but in a more convenient form despite changes in telephone technology. But from our comparison of DRAS functionality in the PSTN and the Internet, it is clear that some elements of the Pen/Trap statute are difficult to directly apply to the Internet. Moreover, as we illustrate further in Part IV, the detailed behavior of important applications, such as email and web browsing, add more complexity when attempting to apply the content/non-content distinction and the third-party doctrine. It is not only unclear which parties are involved in a communication and whether or not ordinary citizens are aware of the disclosure of information to third parties, but it is also unclear how to apply the concept of architectural content in cases where architectural metadata is intermingled with end-to-end data. In fact, some applications are sufficiently complex that their network behavior reveals the content of communications or private data that is resident on a user's device; this will be shown in Section IV.E. In other words, in some cases network behavior — metadata — is equivalent to content.[283]

IV. INTERNET SERVICES AND METADATA

In this Part, we present a variety of examples to illustrate how two bedrock tenets of surveillance law — the content/non-content distinction and the third-party doctrine — are no longer meaningful, workable distinctions when applied to an IP-based communications environment. Specifically, we examine a variety of current IP-based protocols and demonstrate how these distinctions erode or collapse entirely. We do this by applying the concepts of communicative and architectural content and architectural metadata that were introduced in the previous Part.

We start by considering email. In Section IV.B, we will see that the addressing information in the protocol — the "From:" in the email protocol header — may be different from the "From:" that is displayed to the user. Next, in Section IV.C, we examine URLs, which are "addresses" for web pages. Determining which parts of URLs are content and which are non-content DRAS has proven to be a challeng-

281. *See* 18 U.S.C. § 2510(8) (2012) (defining "'contents', when used with respect to any wire, oral, or electronic communication, [as] includ[ing] any information concerning the substance, purport, or meaning of that communication").

282. *See* discussion *supra* Section III.C.

283. *See* discussions *infra* Sections IV.E & IV.G.

ing endeavor for courts and scholars. In Section IV.D, we look more deeply into "blurred boundaries," that is, situations where the concepts of architectural content and architectural metadata do not determine whether there is a third party that is given information for its use.

Notwithstanding these content-discerning issues, communicative content can also be revealed indirectly. Thus, in Section IV.E, we discuss a less direct, but quite revelatory, phenomenon: DRAS from ad networks that enables significant inferences about the user's activities. In other words, a Pen/Trap order could be used to obtain content.

In Section IV.F, we examine the case of mapping services, which illustrates that whether information is conveyed to the mapping provider varies and depends on the architecture of the service — and is thus largely opaque to the user. Mapping services provide one of the best examples for how, in an IP-based communications environment, the concept of a voluntary conveyance, as recognized in *Smith*, is little more than a legal fiction.

The systems we have analyzed here were selected either because they are already targeted by law enforcement (e.g., email and the web) or because they present especially striking examples of our thesis. Other protocols and applications present the same sorts of problems. In the interest of space and clarity, we do not present full-fledged analyses of any others; still, a brief look at a few is useful.

The examination of these examples suggests that the content/non-content distinction erodes or collapses in three primary ways:

(1) some information fits into neither statutory definition;

(2) depending on where in the network one asks the question, content may be architectural content for one party and architectural metadata or communicative content for another; and

(3) extremely revelatory information may nevertheless fail to satisfy the statutory definition of content, and thus cannot claim the privacy protections afforded content under statutory law.

In addition, the examination of these examples demonstrates how, for two primary reasons, the third-party doctrine becomes unworkable in an IP-based communications environment:

(1) most users are unable to know or discover what information they share with myriad third parties. Such obfuscation undermines the idea that the user can make a voluntary conveyance of information under *Smith*; and

(2) application of the third-party doctrine will turn on where in the network law enforcement compels access to the information.

We begin in Section IV.A by continuing the analysis started in Part III. Specifically, we explain how the services and architecture of IP-mediated communications differ from the PSTN in fundamental ways, and discuss how these differences impact application of the content/non-content distinction and the third-party doctrine.

A. Services and Architecture

New technologies challenge many of the basic assumptions underlying such principles as the third-party doctrine. Specifically, there may be no way for a user to know or even discover what kind of information she shares with third parties, many of whom are invisible to her. Similarly, traditional models of what constitutes content and what might be considered mere transactional, non-content information often yield nonsensical, indeterminate, or unsatisfying results when applied to modern technologies.

Consider the different ways that an Internet-resident teleconferencing system used for internal corporate communications might work. No matter how it is done, the actual words exchanged are clearly (communicative) content within the meaning of the Wiretap Act and the Fourth Amendment. What, though, of metadata pertaining to the identities of participants in a call? If the conferencing system is operated by a third party, *Smith* would probably apply. Indeed, this scenario is very similar to telephone networks. When connecting to a conference call, the IP addresses of participants are disclosed to the third party company running the conferencing system. If, however, the company using the system runs its own software on a computer in the cloud, the identities of the participants (e.g., email addresses) would belong to the company running the software, not to the owner of the computer. In this scenario, the identity information is an end-to-end communication between the call participants and the company providing the service. But in addition, the call participants are connecting to the owner's machine, and their IP addresses are visible to — and used by — the computer owner, again a third party. There is one final case: the company using the system might run the system on its own computers. In that case, there are no third parties as the communications between the call participants and the company would strictly be end-to-end. Significantly, in all three scenarios the same

software could be in use.[284] These scenarios illustrate that the metadata may or may not be given to third parties.

In this paper, we are concerned chiefly with communications metadata generated by applications that connect to the Internet, although precisely how (or even if) an application uses the network may be rather opaque to the user. In other words, the user will likely have no idea when she discloses metadata to a third party. For the purposes of this discussion, an application is simply any computer program that performs a visible function for the end user.

Some applications, such as those used for text messaging or electronic mail, are explicitly and obviously intended for communication, and users understand this — even if they might not appreciate all of the metadata they may disclose in the course of myriad communications or even know all possible parties to the communications. Many other applications, such as those used for photography, mapping, and games, might, however, communicate with some entity on the network. Indeed, they may do so at unexpected times and in ways that are effectively invisible to — or even deliberately hidden from — their users.[285]

As we have already explained at some length, whether and how an application communicates over the network, and the extent to which it depends on remote services on the network, are functions of architecture. They are basic decisions made by software designers about how an application functions and where it obtains and stores the data it processes and manages. While the communication architecture of some applications may be constrained by their function (e.g., a text-messaging application must have some way to send and receive text messages), designers often have a wide range of choices regarding how their software communicates over the network — or even whether it does.

In a simple architecture, an application might work entirely locally (sometimes called "offline"), making no use of network services at all. All processing is performed on the user's computer and all data used is stored locally — that is, on media such as flash memory or magnetic disk drives that are directly connected to the local computer. Using the data on another computer[286] requires physically copying or transferring the media from one device to the other.

---

284. There are software packages that are freely available as open source software but are also used as the basis for service platforms by the code's owners. Wordpress is a classic example; the company offers a blogging service on http://www.wordpress.com but makes its software available under the GPL at http://www.wordpress.org.

285. *See* discussion *infra* Section IV.F (regarding mapping applications for choices regarding network communications).

286. In this part, we use the term computer to refer to any device that runs or serves applications, whether it is in the form of a desktop workstation, a laptop computer, a touch-

As people acquire increasingly more computing devices, ensuring that their data is available from and synchronized between their various machines becomes much more difficult. "Cloud services" attempt to address this issue by enabling applications to store data to be shared among devices at a server on the network.[287] When an application uses a cloud service for storage, there is some mechanism for retrieving the current version of the user's files from the cloud service when the application is opened, and for pushing newly saved versions of data to the service when files are changed.[288]

At the far end of the spectrum from totally local applications are applications that are implemented as a service. Service-based applications perform some or all of their computation and storage on a remote computer operated by the application provider. Common service-based applications include email, search, and social networking. The user's computer serves essentially as an interface for displaying output from and sending input to the service host computer, where the actual work of the application is performed and where the user's data is stored.

Applications can make use of network services in a variety of ways and from a variety of providers. The relationship between an application, a user's data, and second or third party providers is easily obscured by the complexity of modern software systems. This lack of transparency is particularly at issue in mobile device applications that must operate in a constrained computational environment. Advertising-supported applications (currently common in the smartphone marketplace) add additional communication and relationships to the mix, and these may be implicitly or deliberately hidden from the user.[289]

---

screen tablet, or a mobile phone. For our purposes, all are computers, and we will not distinguish between them except when necessary.

287. There are many different cloud storage services. *See generally*, Anne Eisenberg, *Digital Storage Options for Workers on the Go*, NEW YORK TIMES (Jan. 17, 2009), http://www.nytimes.com/2009/01/18/business/18novel.html (last visited December 15, 2016) (describing basic storage services). *See also* Jacqui Cheng, *5 Cool Things to Sync with Dropbox on your Mac*, ARS TECHNICA (Oct. 5, 2009, 9:00 PM), http://arstechnica.com/apple/2009/10/5-cool-things-to-sync-with-dropbox-on-your-mac/ [https://perma.cc/W7RS-3Z6N] (describing how some applications can use cloud storage services).

288. Precisely when and how this happens varies depending on the application and the particular cloud service. In some cases, the user must explicitly request the files be retrieved from the cloud service, while in others there is automatic synchronization across devices. The synchronization mechanism may be built in to the application or performed by an auxiliary application or by the computers' operating systems. Also, there may be "cached" copies of data stored on local media to allow for operation when the computer is not connected to the network.

289. One of the authors recently received a fraudulent ad from a mobile app. The app vendor was completely unable to track it down; the web of relationships between the app vendor and the ultimate advertisers was too complex to do so. In other words, neither the user nor the app had *voluntarily* fetched the fraudulent page.

Whether an application's architecture is entirely local, uses cloud-based storage, or is based on a remote service is generally a choice made by the application's designer and may be indistinguishable to the end user. In fact, as we shall show, it is possible in practice for functionally identical applications to occupy radically different positions on this spectrum. A user of these applications will not necessarily know — and may find it essentially impossible to discover — how the architecture of an application affects the location and disclosure of her data to various third parties during any given transaction or user access to data. Given this unknowable, undiscoverable fluidity, a voluntary conveyance of information can rarely be said to characterize the user's disclosure of information to myriad third parties.[290] This fact undermines a meaningful application of the third-party doctrine.

Thus, whether an application's data is properly considered content or metadata and whether that distinction is even technically meaningful in modern applications has become a complex question, dictated partly by architectural choices, partly by arbitrary-seeming decisions made by implementers and system administrators,[291] partly by where in the system the question is asked, and partly by new modes of communication that blur the distinction altogether.

We illustrate these IP-driven complexities through several detailed examples. For some of our more complex examples, we start with a simplified explanation that omits deeper technical details. These descriptions are intended to provide sufficient detail to justify our legal analysis. Although our legal analysis solidly rests on the technical descriptions we present, we caution that an even deeper understanding of the technology may be necessary when drafting legislation or engaging in litigation.[292]

B. Email Headers and Envelopes

Despite the travails of snow, rain, heat, and gloom of night,[293] at some level, the delivery of physical mail is a conceptually straightforward process. The recipient's address on the package or letter is, with few exceptions, the address to which the item is to be delivered.

---

290. *See, e.g.*, Christopher Slogobin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 171 (2005).

291. These decisions are generally not, in fact, arbitrary. However, they depend on complex technical and economic issues that are rarely, if ever, known to users of the services.

292. In the past, misunderstandings of technology have led to faulty judgments. *See, e.g.*, *In re* Application of United States, 396 F. Supp. 2d 45, 48 (D. Mass. 2005). In that case, the court confused email header "From:" and "To:" lines with those in the SMTP protocol. *See* discussion *infra* Section IV.B.

293. Despite popular belief, "[n]either snow nor rain nor heat nor gloom of night stays these couriers from the swift completion of their appointed rounds," is *not* the motto of the US Post Office. The reason for such a belief may lie in the fact that the lines are carved on the outside of the US Post Office building at 8th Avenue and 33rd Street in Manhattan.

Like physical mail, email is asynchronous; someone sends an email and some time later, the recipient receives it. What is invaluable about email delivery is that although the email may be sent to a recipient at their work email (e.g., Alice@work.com), she may read it anywhere in the world via the Internet.

Delivery of email is a complicated technical process. We start with a simple explanation followed by a legal analysis.

A mail to Alice@work.com goes to her employer's inbound mail server.[294] The simplest analogy is to general delivery at a post office. With physical mail, the recipient would go to the window to pick up the letter. With email, Alice contacts the inbound mail server to download the email from it to her local machine. Alice's address as it appears to the sender is simply Alice@work.com; however, there are other addresses involved in the transmission, including those associated with her employer's inbound mail server.

This architecture is implemented by several different components. The primary ones are the transport mechanism, the basic message format,[295] and the multimedia extensions.[296] Mail transport uses the Simple Mail Transfer Protocol[297] ("SMTP") and a mail retrieval protocol.[298]

We show a typical protocol dialog for email transmission below. The shaded box contains the actual email message. We have used an italic font to denote communications from the recipient's inbound mail server; the other text is sent by the mail client (the program that is used to actually send and receive mail).

220 yyy.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03
HELO xxx.cs.columbia.edu
250 yyy.com Hello xxx.cs.columbia.edu [10.42.32.77]
MAIL FROM:<smb@xxx.cs.columbia.edu>
250 OK
RCPT TO:<smb@yyy.com>
250 Accepted
DATA

294. How a sender locates the inbound mail server for an email address is not relevant here. Let it suffice to say that there are standardized, ubiquitously used mechanisms involving the Domain Name System, which is described *infra* Section IV.G.1.

295. *See generally* P. RESNICK, INTERNET MESSAGE FORMAT (RFC 5322) (2008), https://tools.ietf.org/html/rfc5322 [https://perma.cc/AJF4-A7XA] [hereinafter RFC 5322].

296. Multimedia extensions allow transport of video, photos, etc. and requires knowledge of which program should process the format; there are many, one or more for each embedded file type such as photos or MP3s.

297. *See generally* RFC 5321, *supra* note 251. The ancestor of this protocol goes back to at least 1980 and probably earlier. *See generally* S. Sluizer & J. Postel, MAIL TRANSFER PROTOCOL (RFC 772) (1980), https://tools.ietf.org/html/rfc772 [https://perma.cc/5AP9-BX52].

298. These include IMAP and POP.

354 Enter message, ending with "." on a line by itself
From: <smb@cs.columbia.edu>
To: <smb2132@columbia.edu>
Subject: Test

This is a test
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 yyy.com closing connection

The grayed-in text, shown above, is the data ultimately displayed to the user. Notice that the grayed-in part, the message, includes a "From:" line that includes an email address. This address ("smb@cs.columbia.edu") need not be the same as the address above in the SMTP envelope ("smb@xxx.cs.columbia.edu"). We will discuss the consequences of that distinction in the legal analysis that follows this technical discussion.

The SMTP protocol does not put any requirements on the message's communicative content.[299] Thus, the communication could just as easily have been:

220 yyy.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03
HELO xxx.cs.columbia.edu
250 yyy.com Hello xxx.cs.columbia.edu [10.42.32.77]
MAIL FROM:<smb@xxx.cs.columbia.edu>
250 OK
RCPT TO:<smb@yyy.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: J. Edgar Hoover <director@fbi.gov>
To: <smb2132@columbia.edu>
Subject: Test

This is a test
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 yyy.com closing connection

299. SMTP does impose certain requirements on the *syntax* of the message, as discussed in Section IV.D *supra*.

Having different values in the envelope and header "From:" lines is by no means unusual.[300] With many mail service providers, the envelope "From:" is the identity of the account holder, while the message header version gives the user's preferred email address. Let us return to the situation of Alice receiving work mail at home. If she were to reply to that work email while reading mail through her home ISP, the process of sending email from a work account while connecting to the Internet at home might cause the email to be sent via the house's local ISP mail server, but the "From:" line would refer to the business. The envelope line[301] — typically ignored by almost all recipients — would be her residential account; the "From:" line in the header would show the work account.[302] Thus, the "From:" in the header line is architectural content, not seen by any entity other than the sender and receiver.[303]

This brings us to the next important issue: third-party mailers. Unlike the phone network or the postal system, there are a vast number of third-party mail servers. Some, such as Google and Yahoo, are well known but there is also a plethora of much smaller providers. Difficulty in applying the conventional third-party doctrine arises from the fact that mail from one person who runs his or her own mail server sent to someone else who does the same will look identical over the wire to the more common case of mail going to a user via a third party server such as Gmail or Yahoo Mail. Determining whether there is a third party involved — whether there are users of two mail servers owned by a separate party rather than the users owning the servers themselves — cannot be done until after interception has taken place. As we describe below, email presents complexities for legal analysis that are not present in PSTN Pen/Trap interceptions.

---

300. As noted above, the envelope of a letter might say "Mr. President" while the inside is addressed to "Ike."

301. The "From:" line in the SMTP dialog will often — but not always — be added to certain message header lines. However, normal mailers rarely display these header lines to users.

302. This specific scenario is becoming less common because of the behavior of some anti-spam filters. For an example of how a publication was deceived by a similar example, see Bill Barnes, *E-Mail Impersonators*, SLATE (March 12, 2002, 7:46 PM), http://www.slate.com/articles/technology/webhead/2002/03/email_impersonators.html [https://perma.cc/2TSQ-CK45].

303. Under certain circumstances, some corporate mail systems will change between internal and external address formats. In those cases, the mail originates from an outbound corporate email server, rather than from the individual who composed it. This is a matter of common practice, rather than a normative standard. *See* WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY 75 (1994).

1. Wiretap Law and Email Headers

The first legal issue to tackle is whether the "From:" information is content or DRAS within the scope of the Pen/Trap statute. The two "From:" lines, the one in the SMTP envelope, and the one in the email message itself, function quite differently. The SMTP "Mail From:" is clearly addressing information; it is used by SMTP.[304]

But the analysis is not as simple with respect to the "From:" line in the email header. In our initial technical discussion of email headers, we showed that there are several different ways in which the "From:" in the email message can differ from the "Mail From:" of the SMTP envelope. One way is if the user is mailing using a different ISP than the one that normally services the account (e.g., replying from home to a work account). Another way is if the user is using an alias, say perhaps selecting the "From:" address to make it appear that the mail is being sent from someone else, or even from themselves but in a different guise (soccermom@jonesfamily.org versus Linda@jonesfamily.com). While this capability may be interesting, the important legal issue arises from the fact that the "From:" of the email header line is not seen by anyone but the sender and receiver — it is an end-to-end communication. Thus, from the point of view of the SMTP protocol, the email header line is architectural content (what is inside the envelope), not metadata. If law enforcement were to compel disclosure of the "From:" line address from the mail service it would be seeking to collect the contents of a package, i.e., architectural content. From the perspective of the (ultimate human) sender and receiver, however, the email "From:" line is addressing information, inaccurate as it may be.

The content/non-content distinction changes depending on *where* in the system you ask the question — or from which entity law enforcement seeks to compel the information. While the SMTP envelope "From:" information is addressing information, the email header "From:" information is not addressing information when collected from the inbound or outbound mail servers and therefore not properly collected under a Pen/Trap order.

Conversely, the email message "From:" is communicative content for both the mail service and the sender and receiver. Accordingly, law enforcement collection of this "From:" information in real-time requires a Wiretap order. To the mail service, the "Mail From:" line in the SMTP application is architectural metadata, while the email message body "From:" is architectural content. This conclusion, crucial for determining whether the "From:" information can be obtained under a Pen/Trap order, is based on the communication's structure, not

304. *See* discussion *supra* Section III.D.

its meaning. We therefore conclude that the SMTP "Mail From:" is addressing information under the Pen/Trap statute, but the email message "From:" is content under the Wiretap Act. The latter should not be collected under a Pen/Trap order. The same is also true for the email header "To:"; the "To: smb2132@columbia.edu" could just as easily have been written "To: smb2132@columbia.edu (secret agent)", since the material in parentheses is displayed to the recipient but is ignored by email-processing software.[305] The two addresses would be functionally identical to the mail service — the parenthesized text is, as noted, ignored by the software — but may convey useful semantic information to the recipient.[306]

Given the two "From:" fields, it is not surprising that the DOJ overlooked the difference between "From:" in the SMTP envelope and the "From:" in the email message. The 2005 Electronic Surveillance Manual says, "Pen register and trap and trace devices may obtain any non-content information . . . Such information includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header."[307] However, this guidance is inconsistent with the inside/outside distinction recognized by the Court's structural analysis of a package in *Ex Parte Jackson*; the email message's "From:" field, like the inside of a package, is architectural content while the SMTP "From:" field, like the address on the

---

305. *See* RFC 5322, *supra* note 295, at 11.

306. One example is email notifications by Twitter. Consider this "From:" line received by one of the authors: "matt blaze (via Twitter) <notify@twitter.com>". The human-readable name, Matt Blaze, is that of the person whose actions caused the email to be sent. The parenthetical portion informs the reader how it was sent, i.e., via Twitter, rather than as a direct email. Finally, the machine-readable portion, "notify@twitter.com", is the actual sender.

307. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, at 39. The 2009 SEARCH MANUAL, *supra* note 95, also states that "[b]ecause Internet headers contain both 'to' and 'from' information, a device that reads the entire header (minus the subject line in the case of email headers) is both a pen register and a trap and trace device, and it is commonly referred to as a pen/trap device." *Id.* at. 154. Here again, DOJ's guidance is inconsistent with the inside/ outside distinction, as recognized by the Court's structural analysis of a package in *Ex parte* Jackson. Furthermore, we note that there are other header fields that are arguably architectural and/or communicative content. The "In-Reply-To:" and "References:" lines are one example, *see* RFC 5322, *supra* note 295, at 25–26. These headers are used to link together related messages, showing who replied to which message. ("The 'In-Reply-To:' and 'References:' fields are used when creating a reply to a message. They hold the message identifier of the original message and the message identifiers of other messages (for example, in the case of a reply to a message that was itself a reply). The 'In-Reply-To:' field may be used to identify the message (or messages) to which the new message is a reply, while the 'References:' field may be used to identify a 'thread" of conversation.'") In other words, these headers are used by the user's mailer to aid in presenting a conversation to the user; they are not used by mail servers or during mail delivery. They are thus architectural content to the SMTP sublayer, in that they are transported unexamined and unused.

With respect to communicative content, in some situations, such as a reply of "I agree" during an online dispute, the semantic context — which message does the sender agree with? — is an essential part of the meaning of the communications.

outside of the package, is addressing information (architectural metadata).

It is also understandable that some courts have missed the distinction between envelope and header lines. As one court wrote:

> That portion of the "header" which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) "cc'd" on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device. However, the information contained in the "subject" would reveal the contents of the communication and would not be properly disclosed pursuant to a pen register or trap and trace device.[308]

While this opinion distinguishes the body from header lines, the judge incorrectly assumed that the header lines were third party information rather than end-to-end architectural content. By determining that the header lines were third party information, the court concluded that collection of this information was lawful under a Pen/Trap order.[309] But because there was no third party involved in the transmission and thus no third party from whom law enforcement could compel disclosure of the information, it is unclear whether the information could lawfully be collected under the Pen/Trap relevance standard.[310] Without the availability of the third-party doctrine, which depends upon a third party to compel information from, a court would need to determine whether an individual has a reasonable expectation of privacy in the information contained in the header lines of the email at issue. Thus, the court's misunderstanding of the technology may have resulted in authorization of an improper search.

Our next concern is whether there is a third party that receives the mail for the user. Envelope data becomes third party data if, and only if, the mail servers in question are, in fact, run by third parties. Mail from one person who runs her own mail server sent to someone else who does the same will look identical over the wire to the more common case of mail going to a user via a third party server such as Gmail or Yahoo Mail. As noted, it is not possible to determine whether there is a third party involved until after interception has taken place. From

---

308. *In re* Application of United States, 396 F. Supp. 2d 45, 48 (D. Mass. 2005).

309. The fact that the judge's conclusion is consistent with the information provided in the 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, and 2009 SEARCH MANUAL, *supra* note 95, does not mean that the judge made the correct decision.

310. 18 U.S.C. § 3122(b)(2) (2012).

a statutory perspective it is unclear as to whether the Pen/Trap statute authorizes collection of metadata that is not based on the disclosure of that data to a third party.[311] From a constitutional perspective, if the third-party doctrine cannot be applied, courts will have to determine whether individuals have a reasonable expectation of privacy in the information law enforcement seeks to collect under the Pen/Trap relevance standard.[312]

This analysis of email headers and envelopes illustrates the key difficulties with applying the content/non-content distinction and third-party doctrine to email. For the content/non-content distinction, determining whether "From:" is actually collectable under the Pen/Trap statute, law enforcement must distinguish between what is architectural content and what is communicative content. We have done so for the SMTP protocol and the internal message, but this analysis is limited to a single, specific protocol; other Internet protocols could present similar problems.

If there is any truism about IP-mediated communications, it is that change is rapid. The dominant communication system of today will be replaced by a new one, and the new one will be one in which a content/non-content analysis will undoubtedly differ. The issue — what constitutes content and what constitutes addressing information — requires an analysis based on the concepts of architectural content and architectural metadata, ideas we explained in Part III and use in the current analysis.

C. The World Wide Web and URLs

URLs are familiar to anyone who has ever used a web browser. Informally, they serve as the addresses of web pages.[313] More technically, they specify the host name of a web server along with a set of additional information that, collectively, specifies a request for some resource. How and where that additional information is generated and interpreted represents a particularly complex and problematic example of the difficulty of drawing meaningful bright lines that distinguish content from non-content in modern systems.

In an ideal world, we might expect to be able to determine syntactically whether a given part of a URL should be treated as "content" or "non-content." That is, we would like a set of rules for parsing any

311. Whether the DOJ believes that the Pen/Trap statute authorizes collection of DRAS from entities that are not third parties is unclear. The 2009 SEARCH MANUAL suggests that the Pen/Trap statute encompasses almost all non-content information in a communication. *See supra* note 95.

312. 18 U.S.C. § 3122(b)(2) (2012).

313. For a description of URL syntax, see generally T. BERNERS-LEE ET AL., UNIFORM RESOURCE IDENTIFIER (URI): GENERIC SYNTAX (RFC 3986) (2005), https://www.ietf.org/rfc/rfc3986.txt [https://perma.cc/2PQ5-Y9UR] [hereinafter RFC 3986].

given URL that will mechanically yield an unambiguous and satisfactory labeling of which components should be considered content and which should not. We will show that, while some of the information beyond the hostname may be DRAS, it is always both architectural and communicative content.[314] Accordingly, as we will demonstrate, real-time collection of the path portion of the URL by law enforcement should always be governed by the Wiretap Act.

The basic URL format seems simple enough. Consider a URL for a typical static web page:

http://en.wikipedia.org/wiki/Metadata

We can parse this URL into its basic high-level components without much difficulty.[315] The "http://" heading identifies it as a standard web URL that can be obtained via the Hypertext Transfer Protocol ("HTTP"). Everything up to the next "/" — "en.wikipedia.org" — specifies the web server's host name. It is called the "authority" in URL parlance.[316] The rest of the URL — "wiki/Metadata" — specifies the particular web page or service requested from the server, and is called the "path."[317] In this case it is a Wikipedia article discussing the concept of metadata.

From a technical standpoint, the authority component appears simple at first blush. It is typically a standard domain name, which must be converted to an IP address by the user's computer at the time the web page is fetched. IP addresses are generally understood to be DRAS, squarely on the "non-content" end of the spectrum.[318]

The rest of the URL — the path — is where most of our trouble begins. In our example above, the URL path simply identifies a particular Wikipedia article on the server; it functions essentially as a file name on the web server. The path is communicated to the web server over HTTP, to be interpreted on the server itself in order to process the user's request. Viewed this way, the path might appear to be clearly and entirely on the "content" end of the spectrum, part of an end-to-end communication between the user and the website with which she wishes to interact.

---

314. *See e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015). The court noted that: "[T]o the extent that the statutory definitions and conceptual categories of content and routing information overlap, Congress expressly contemplated the possibility of such an overlap. . . . [W]e are persuaded that, under the surveillance laws, dialing, routing, addressing, and signaling information may also be content." *Id*. at 138 (internal citations omitted).

315. See RFC 3986, *supra* note 313, at 16 for a formal description of the components of a URL.

316. *Id.*

317. *Id.*

318. *See supra*, Section III.D. We will shortly see that the handling of the authority field is actually not quite so simple, but for the moment this description is sufficient.

It might then appear that a simple and entirely syntactic rule would suffice: the authority field is non-content, while anything in the path field is content. Unfortunately, appearances here can be deceptive, and this simple rule would, as often as not, have to be honored in the breach.

Our first problem is that viewing the path as a single, monolithic communication from a web browser to a web server is an oversimplification. In fact, the path consists of a number of subcomponents, some of which can be generated by or interpreted by different entities.

For example, the path can include a "query" subcomponent. This is a special part of a URL path preceded by a "?" that supplies additional information to the web server about the service being requested. In some cases, this reflects information entered by the user, such as a search query, for example:

https://www.google.com/search?q=what+is+metadata

Here, we have the URL generated by entering "what is metadata" into the Google search box. The "?q=what+is+metadata" query subcomponent reflects the text entered by the user. This is a communication from the user to the receiving web server, and we are still in "clearly content" territory (from both architectural and communicative content perspectives). But when we look at what happens next, the situation becomes much less clear.

As it happens, the first URL result returned by this Google search appears to lead to the Wikipedia article about metadata that we used in our previous example, http://en.wikipedia.org/wiki/Metadata. In fact, it does not.

The supposed Wikipedia URL returned by Google leads to another Google web page, with a Google server in the authority component and a far more complex path component:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCcQFjABahUKEwjX7d2S_4LIAhVGlYgKHRxlAqM&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FMetadata&usg=AFQjCNE3JFDxIJ647wzHKykLvYbekf5C0w

When the user clicks on this URL, her browser initially interacts not with the Wikipedia web server with which she expects to communicate, but rather back with the Google web server. Various parts of the query subcomponent of the path in this URL are used to track the request and then to generate an automatic redirection to the actual Wikipedia URL, which is itself encoded within this URL. All of this is essentially invisible to the user, who will be generally unable to

distinguish this URL from that of the Wikipedia page on which she ultimately lands. The effect here is that the path component of the Wikipedia URL has now been given, wittingly or not, to a third party (Google) on the way to the Wikipedia server.

Other scenarios add still more ambiguity and in every case depend on the architecture of the particular service used. For example, how search queries are handled varies by search provider, often involving embedded ads and requests to other servers within the domain.[319] For example, in providing information about a restaurant, a search engine might provide menus linked from one web server and location information, such as customized maps, linked from a different server. The origin of other elements of the query portion is even less clear — in particular, they may actually come from the destination server.[320]

Our next problem is that the conceptual model of a user's web browser interacting directly with a web server is another vast oversimplification.

URLs are communicated to web servers through a communication protocol, called HTTP, the Hypertext Transfer Protocol.[321] The protocol defines not just the transmission of URLs from browsers to servers, but a conversational "session" between them with data flowing in both directions.[322]

HTTP sessions are complex; they not only convey the URL authority and path, but also consist of a method,[323] a version number, a

---

319. *Ad Networks vs. Ad Exchanges: How They Stack Up*, PRINCETON CS (2010), https://www.cs.princeton.edu/courses/archive/spring13/cos448/web/docs/adnets_vs_exchanges.pdf [https://perma.cc/29GE-77N9].

320. That certain information was in the query field was a crucial element in the decision in *In re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 15–16 (1st Cir. 2003). The court noted:

> [T]he client Pharmacia used the "get" method to transmit information from a rebate form on its Detrol 11 website; the webpage was subsequently modified to use the "post" method of transmission. This was the source of the personal information collected by Pharmatrak from users of the Detrol website. . . . Since NETcompare was designed to record the full URLs of the webpages a user viewed immediately before and during a visit to a client's site, Pharmatrak recorded personal information transmitted using the get method.

321. *See generally* T. BERNERS-LEE & L. MASINTER, UNIFORM RESOURCE LOCATORS (URL) (RFC 1738) (1994), https://tools.ietf.org/html/rfc1738 [https://perma.cc/Q57J-KBLN]; R. FIELDING & J. RESCHKE, HYPERTEXT TRANSFER PROTOCOL (HTTP/1.1): MESSAGE SYNTAX AND ROUTING (RFC 7230) (2014), https://tools.ietf.org/html/rfc7230 [https://perma.cc/AVS7-WNXV] [hereinafter RFC 7230]; R. FIELDING & J. RESCHKE, HYPERTEXT TRANSFER PROTOCOL (HTTP/1.1): SEMANTICS AND CONTENT (RFC 7231) (2014), https://tools.ietf.org/html/rfc7231 [https://perma.cc/3MZ6-QBSH] [hereinafter RFC 7231].

322. *See* RFC 7230, *supra* note 321 at 18. A related protocol, HTTPS, defines HTTP over encrypted communication sessions, and, for our set of concerns, is essentially similar.

323. *See* RFC 7231, *supra* note 321, at 21. A "method" specifies what sort of HTTP operation is to be performed. The GET method specifies everything relevant in the URL;

series of header lines that supply additional information and in some cases a body. There are two common HTTP methods to retrieve a webpage, called GET and POST. These have very different communication properties, with implications for applying the third-party doctrine to web page downloads. For example, a GET command includes query information in the URL, but a POST command includes the query in the message body. What this means is that query information in a GET command might not only be logged by the receiving web server,[324] but will be visible to, and thus processed by, any middle boxes[325] used to create the connection, including those run by ISPs. On the other hand, the query lines in a POST request are invisible to any middle boxes along the way. The user, however, has no control as to whether GET or POST is used — and indeed, almost certainly cannot even discover which command has been issued.

The web hosting arrangements used by many web server operators create yet more complex and opaque ambiguities. This is true even with respect to the authority URL component, which, so far, has been steadfastly in the non-content category.

Recall that the authority component identifies the web server from which the path is retrieved. On the user's side, the authority appears to be a domain name, to be converted by the user's web browser into an IP address and used to identify the web server to the network. But the original authority hostname contained in the URL is also sent to the server as part of the HTTP request. This is to allow a single physical server to host multiple web servers for different domains. The server uses the authority field that is sent to it to determine which of the web servers it hosts should process the request. The authority component thus acts both as non-content (when it is translated to the server's IP address and used to establish network communication) and as content (when the original host name from the URL string is sent to the web server).

If the hosting web server is dedicated exclusively to web sites owned by a single entity, for example, a corporate web site hosted in-house, there may be no new third parties involved with the authority component,[326] but if a server is shared among different entities, as it often is in commercial services, there will be. In other words, whether or not there is actually a third party present between the user and the receiving web server depends on decisions made by the hosting ser-

---

Google queries use GET. The other common method, POST, is frequently used for uploading data such as email messages or pictures.

324. For this reason, web developers are generally taught to avoid putting sensitive information, such as social security numbers or passwords, into GET requests. *See* R. FIELDING ET AL., HYPERTEXT TRANSFER PROTOCOL —HTTP/1.1 (RFC 2616), at 52–53 (1999), https://tools.ietf.org/html/rfc2616 [https://perma.cc/ZD4V-WJAR].

325. *See infra* Section IV.G.4.

326. At least one of the authors of this article owns and operates such a web server.

vice *operator*. This is not information the user could possibly know. Or imagine a multisite customer of a commercial hosting service. As the customer's business grows, it may need more and more web server capacity; to accommodate these extra demands, the hosting service might move other customers to different physical computers. Whether or not the authority field is shared depends on technical and economic decisions made by an outside party — and even the site owner may not know these details.

1. Wiretap Law and URLs

It is telling that the DOJ instructs prosecutors in the field not to use a Pen/Trap order to collect any URLs without first consulting the Computer Crime and Intellectual Property Section ("CCIPS") at Main Justice.[327] While the DOJ asserts that the PATRIOT Act gives law enforcement authority to collect non-content information associated with Internet communications, the DOJ acknowledges that the use of Pen/Trap to collect URLs raises "privacy and other concerns."[328] The DOJ is right to be cautious, as trying to assign a single rule, or even a set of rules, to apply to all portions of the URL could lead to the collection of content with a Pen/Trap order.

Let's begin with the path portion of the URL: "wiki/Metadata." As previously explained, it functions much like a file name on a web server. It therefore reveals communicative content because it describes what the user is requesting from a website.[329] The path portion is also architectural content in that it is a request for a resource from the user to another system. The authority — the hostname — is the recipient of the message; the path is the message.

The fact that the path portion of the URL is always communicative content,[330] however, makes at least a portion of the legal analysis

---

327. *See* U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-7.500, http://www.justice.gov/usam/usam-9-7000-electronic-surveillance [https://perma.cc/MG4X-CNH3].

328. *Id*.

329. *See In re* Google Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 139 (3d Cir. 2015) ("For instance, the domain name portion of the URL — everything before the '.com' — instructs a centralized web server to . . . a particular website, but post-domain portions of the URL [i.e., the path] are designed to communicate to the visited website which webpage content to send the user.").

330. As Orin Kerr notes, *In re Google Cookie Placement Consumer Privacy Litigation* suggests that everything after the domain name in a URL is content. *See supra* note 329. But, as Kerr observes, the Third Circuit's discussion is not a holding. Kerr cites a footnote to illustrate the court's "backing away" from a universal, determinative holding:

> We need not make a global determination as to what is content, and why, in the context of queried URLs. Lack of consensus, the complexity and rapid pace of change associated with the delivery of modern communications, and the facileness of direct analogy to mail and telephone cases counsel the utmost care in considering what is, and

somewhat straightforward. The Wiretap Act requires a Title III warrant for the collection of content defined as "the substance, purport or meaning of a communication" (what we call communicative content). There are no other significant legal questions for courts to consider when evaluating the appropriate standard for "real-time" law enforcement access to the path portion of the URL.

If law enforcement were to compel the disclosure of the stored path portion of the URL from a third party, however, there is no clear legal precedent on what access standard controls (e.g., a Rule 41 warrant or a lower standard available in the Stored Communications Act). While the path portion of the URL is communicative content, current law does not definitively bestow Fourth Amendment protections upon this stored content. The closest case may be *Warshak*, which held that the Fourth Amendment protects the contents of email held by an ISP.[331] As we discussed in detail in Part II, the court's reasoning turns on the analogy it draws between an ISP and a telephone company or post office — they are both intermediaries with respect to the content of communications.[332] While the "mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy," the court suggested that there might be some kind of interaction with data that could defeat the Fourth Amendment protections afforded to communicative content in the possession of a third party.[333] The court did not elaborate on what kind of third party interactions with, or use of, communicative content would defeat Fourth Amendment protections. We note that *Warshak*'s reasoning is consistent with Henderson's concept of a "limited third-party doctrine," where data loses Fourth Amendment protections through the third-party doctrine only when the data is provided to the third party for its use.[334]

> what is not, "content" in the context of web queries. Indeed, when it comes to differentiating content from non-content, . . . queried URLs [have been characterized] as "the most difficult and discussed case."

Orin Kerr, *Websurfing and the Wiretap Act Part 2 the Third Circuit's Ruling*, THE WASHINGTON POST (Nov. 19, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/19/websurfing-and-the-wiretap-act-part-2-the-third-circuits-ruling/ [https://perma.cc/4WPG-43KH] (quoting *In re* Google Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015)) (alteration in original).

331. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) ("We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails."). The court reached this conclusion despite the fact that the Stored Communications Act authorizes law enforcement to compel stored content from certain kinds of third parties under a relevance standard (via subpoena) or reasonable suspicion standard (via 18 U.S.C. § 2703(d) order). *See* 18 USC § 2703(b)(1)(B) (2009).

332. *Warshak*, 631 F.3d at 286–87.

333. *Id*. at 286.

334. *See supra* Section II.C.2.

The stored-path portion of the URL presents a more challenging analysis than stored email in the possession of a "mere intermediary" third party ISP. As previously noted, there are circumstances when a path consists of a number of subcomponents, such that the path component may be given to a third party. In the example we examine above, the user types the query "what is metadata" into the Google search engine. While the result returned appears to lead to a Wikipedia article about metadata, the user's browser interacts not with the Wikipedia web server with which she may expect to communicate, but rather with the Google web server. As our example demonstrates, the path component of the Wikipedia URL is given, wittingly or not, to a third party (Google) on the way to the Wikipedia server. If law enforcement compels the path component from Google (not a "mere intermediary" like the ISP in *Warshak*), does Google use the data in a way that would defeat application of the third-party doctrine? Even when the path portion of the URL is given to Google for its use, it is hard to argue that such a conveyance is voluntary under *Smith*. Indeed, what is given to a third party depends on the architecture of the particular service used — choices that the user has no control over and which remain largely invisible, even to the technically sophisticated user. If a court determined that the path portion was given to a third party for its use, the court would then need to determine if the disclosure was a voluntary conveyance under *Smith* and, if not, whether the user had a reasonable expectation of privacy in the data. In this case, we are still talking about communicative content, so without some additional authority, the prudent prosecutor should secure a warrant before compelling the stored path portion of the URL from a third party.

Thus far we have analyzed only the path portion of the URL. The authority portion of a URL, while generally non-content DRAS, can become architectural content in certain web hosting arrangements. If a single physical server hosts multiple web servers for different domains, the server uses the authority field that is sent to it as part of the HTTP request to determine which of its web servers should process the request. As we previously noted, in this hosting arrangement the authority acts both as non-content when it is translated to the server's IP address and used to establish network communication, and as architectural content when the original host name from the URL string is sent to the web server. When a single web server exclusively provides services to web sites owned by a single entity, there is no third party involved in serving the web page. In the case where a single web server is shared by different entities (as can be the case in commercial services), however, the operator of the server program must route the HTTP request to the appropriate web page. The particular hosting arrangement that determines whether a third party receives the

authority portion of the URL is a decision made and implemented by the hosting service operator. The user does not make a voluntary conveyance of information to a third party, as the user cannot control or know if or when a third party will receive the information. Accordingly, in a web hosting arrangement where a single server provides services to web sites owned by multiple entities, a court cannot rely upon the third-party doctrine to determine the appropriate access standard when law enforcement compels the authority portion of a URL from a third party. The court would need to conduct a reasonable expectation of privacy analysis without the benefit of the third-party doctrine.

As we noted at the beginning of this example, the DOJ instructs prosecutors that the use of a Pen/Trap order to collect URL information is prohibited without first consulting with the Computer Crimes and Intellectual Property Section at Main Justice.[335] This admonition is not, however, a blanket prohibition. The DOJ exempts from this policy the use of a trap and trace order "to . . . collect[], at a web server . . . tracing information indicating the source of requests to view a particular URL."[336] While the DOJ may be trying to prevent the collection of content with a Pen/Trap order, this exemption from the "phone home to Main Justice" policy may actually lead to the collection of content with a trap and trace device. Specifically, content may be improperly collected in the following example: Since some web servers host multiple web sites sharing a single IP address, the specific web site that is being accessed is not itself derivable solely from the server's IP address; thus, the server must inspect the authority field of the URL to determine what web page to serve. That information is transferred as part of the HTTP session. In that case, the authority field is architectural content, not metadata, to the network, although it may be metadata to a server run by a third party (i.e., one that is not the owner of the hosted web sites).

To summarize a complex analysis, the path and query sections of the URL are typically not DRAS information and should normally be considered content. The path can indicate, for example, what story on a newspaper site is sought, or what article on Wikipedia is being read or edited. The authority section of a URL is generally metadata, but the analysis is technically more subtle. In general, there are three common cases: (a) the IP address hosts only one site; (b) the IP address hosts multiple sites, but it's a hosting company; and (c) the IP address hosts multiple sites but they are all run by a single party. In case (a), the authority name is essentially equivalent to the IP address, and is DRAS information. In case (b), the authority name is third-party data. Case (c), however, is complicated; the authority field is not

335. *See* U.S. DEP'T OF JUSTICE, *supra* note 327.
336. *Id.*

third-party data and is not equivalent to the IP address. If it is determined not to be third party data, a reasonable expectation of privacy analysis should be performed. However, the determination of whether or not the authority is third-party data — and thus whether a reasonable expectation of privacy analysis applies — cannot occur until after the authority section has been collected and analyzed.

D. Blurred Boundaries

One issue that complicates distinguishing content from metadata on the Internet is the lack of clear boundaries between the two. On the phone network at the time of *Smith*, there was a structurally simple division: information was either a dialed number or a conversation, and there were no in-between categories.[337] While such boundaries sometimes exist on the Internet between the IP header and everything else, for example, other situations in IP-based communications are much less clear-cut.

The layered model of the Internet means that different abstractions might be exposed to different entities. Thus, we might expect that an examination of layering would yield definitive answers to questions of when and where a particular piece of data should be considered architectural content. When it works, layering can be a beautiful abstraction. Where legal and technical answers not only converge, but also make logical sense, using layering to answer questions about what constitutes content can be fruitful. Unfortunately, neither the layers nor their implementation are always as clear in practice as we might hope, in which case we must resort to a less philosophically pure analysis of the gory technical details before we can find reasonable answers.

A good example of this is email headers. As noted, there are some header lines, such as "Received:",[338] that are examined and generated by intermediate nodes. These lines were primarily intended for mail system operations: preventing forwarding loops,[339] debugging problems, tracing spam, etc. That said, they often contain more sensitive information. "Received:" lines often contain IP addresses, which in turn can hint at location.[340] They sometimes have the sender's actual

337. *See supra* Part I.

338. *See supra* Section IV.B.

339. In a forwarding loop, email is sent back to the same address, generally indirectly. For example, user ABC on computer host1.com might forward mail to abc@host2.com; on that machine, however, there could be an instruction to send the message back to abc@host1.com. *See* RFC 5321, *supra* note 251, at 71.

340. There are commercial services that map IP address to geographic location; they have varying degrees of accuracy. *See Geolocation: Don't Fence Web In*, ASSOCIATED PRESS (July 7, 2004), http://archive.wired.com/techbiz/it/news/2004/07/64178?currentPage=all [https://perma.cc/6ZUB-6SLL].

physical address, which is fair game for a Pen/Trap order; however, this metadata is embedded in what would otherwise clearly be considered communicative content per the Wiretap Act.[341] Nor is it simple to draw up lists of content versus metadata email headers; many mail systems have their own private header fields;[342] there is no way to know, *a priori*, how these fields behave. For that matter, different implementations of "Received:" have different formats; Google's Gmail service, for example, does not include the sender's IP address in the headers of outgoing messages from Gmail users.[343]

The technologies used by the government to implement the interception of many Internet services can blur the layering distinctions even further. Consider, for example, the problem of collecting (by monitoring of an actual physical network link) the email addresses of people sending mail to a target who uses a web-based mail service such as Google's Gmail or Microsoft's Outlook.com.[344] While the Pen/Trap statute permits email address collection,[345] the monitoring device must see, analyze, filter, and generally discard link layer, network layer, and transport layer headers before it even gets to the actual displayed web pages that contain the desired email addresses. The monitoring device must then parse the HTML text to ascertain precisely what is displayed, being careful to pick out only email addresses that appear to be metadata and not, say, the same strings in the "Subject:" line or body of a message. This process, known technically as "screen-scraping" or "web-scraping,"[346] can be difficult, fragile, and error-prone; [347] it is also highly dependent on the service provider and reliant on particular versions of the provider's software as well as

341. *See supra*, Section II.A.

342. *See* RFC 5322, *supra* note 295, at 30 ("Fields may appear in messages that are otherwise unspecified in this document.").

343. Presumably, this is done for privacy reasons, though to our knowledge Google has never said so explicitly. Technically, this is not standards-compliant behavior. *See* RFC 5321, *supra* note 251, at 60. In practice, this does not present operational problems, but does complicate the legal analysis of the status of "Received:" lines.

344. We are assuming for the purposes of this example that the government cannot obtain this information from the webmail provider's logs, e.g., because the provider is outside of its jurisdiction, or because the provider cannot readily provide the information itself.

345. The distinction between "envelope" and "header" is minimal or non-existent for web-based mail systems.

346. It is hard to find a definition of "screen-scraping" that matches the actual technical meaning. The best reference we have found is J.K. Hirschey, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*. 29 BERKELEY TECH. L.J. 897, 897 ("[S]craping typically collects data from screen outputs or extracts data from the HyperText Markup Language ('HTML') code that most websites display."); *but see infra* note 347.

347. Screen-scraping involves trying to intuit what a human will perceive from what is displayed on the screen. Changes that are trivial to a person, such as highlighting the current message via a font size change instead of, say, a color change, actually require a fair amount of HTML code that an intercepting program must process and decide to ignore.

the target user's configuration options.[348] Errors in interpretation here can result in both the unauthorized collection of information and the failure to capture information subject to authorized collection.[349] One state court, focusing specifically on the logic of *Smith*'s distinction between a pen register and a listening device, took the bold step of finding that law enforcement installation of a pen register device that also had audio wiretapping capabilities was unlawful, even when the voice collection capabilities were disabled.[350] Citing *Smith*, the court noted that:

> Central to the Court's analysis [in *Smith*] was the pen register's limited capabilities and the fact that unlike a listening device it does not "acquire the *contents* of communications." The Court, in making the distinction, quoted from its earlier decision in *United States v. New York Tel. Co.*: "These devices do not hear sound. They disclose only the telephone numbers that have been dialed . . . Neither the purport of any communication . . . nor whether the call was even completed is disclosed by pen registers."[351]

In a more recent opinion, the United States Foreign Intelligence Surveillance Court of Review ("FISCR") considered what might be characterized as a "blurred boundaries" question — whether the government could collect DRAS with a pen register if, in the course of

---

348. Even the intelligence community has found screen-scraping to be difficult. According to a spokesperson from the Office of the Director of National Intelligence, the NSA has experienced problems in exactly this situation. *See* Parker Higgins, *Intelligence Agency Attorney on How "Multi-Communication Transactions" Allowed for Domestic Surveillance*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS (Aug. 21, 2013), https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed [https://perma.cc/NFV5-8PTN] ("Those are all transmitted across the Internet as one communication, even though there are 15 separate emails mentioned in them. And for technological reasons, NSA was not capable of breaking those down into their — and still is not capable — of breaking those down into their individual components.").

349. Correct technical implementation and control of a wiretapping capability is not easy. In an FBI anti-terrorism investigation by the UBL — Usama bin Laden — Unit, the Carnivore wiretapping software malfunctioned and captured other emails that were not authorized by the FISA warrant. According to an FBI memo released via a FOIA request by EPIC, the FBI was required to cease collection until the matter could be "straightened out." *See FBI Memo on "FISA Mistakes"*, ELECTRONIC PRIVACY INFORMATION CENTER, https://www.epic.org/privacy/carnivore/fisa.html [https://perma.cc/6FND-CHYV] (last visited Oct. 19, 2016). Context is given in the EPIC press release. See *FBI's Carnivore System Disrupted Anti-Terror* Investigation, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/carnivore/5_02_release.html [https://perma.cc/QM3T-KYBF].

350. *See* People v. Bialostock, 610 N.E.2d 374, 378 (N.Y. 1993).

351. *Id*. at 377 (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979)) (internal citations omitted).

collecting DRAS, it also collected content.[352] As an initial matter, we note that the FISCR was addressing a question related to the collection of content via the Pen/Trap authority provided under the Foreign Intelligence Surveillance Act,[353] not the criminal Pen/Trap authority[354] that has been the focus of our inquiry throughout this Article. The constitutional determination made by the FISCR is an evaluation of national security equities, not law enforcement interests; [355] courts considering law enforcement equities under traditional Fourth Amendment considerations might reach a different result.[356] However, because FISA Pen/Trap authority incorporates definitions from the criminal Pen/Trap statute,[357] some of the FISCR's reasoning has implications for content/non-content distinctions on the Internet in criminal investigations.

Specifically, the FISCR considered whether an order issued under the FISA's Pen/Trap authority authorizes the government to obtain all post-cut-through digits ("PCDs"), when there is "no technology reasonably available to the Government" that could permit: (1) a Pen/Trap device to collect PCDs that are DRAS, while not acquiring PCDs that are "contents of a communication"; or (2) the government to discard the PCDs that are content information at the time the "non-content DRAS" is collected.[358] PCDs are numbers or characters entered by the user after the dialed call is connected or "cut through," such as credit card numbers, a password, social security number, or other telephone numbers entered after the use of a calling card.[359] As these examples illustrate, some PCD information — a phone number

---

352. *See In re* Certified Question of Law, No. FISCR 16-01, at 1–2 (FISA Ct. Rev. Apr. 14, 2016).

353. 50 U.S.C. § 1842(a) (2006).

354. *See* 18 U.S.C. §§ 3122–3127 (2012).

355. *In re* Certified Question of Law, *supra* note 352, at 26. The court stated:

> When law enforcement officials undertake a search to uncover evidence of criminal wrongdoing, the familiar requirement of a probable cause warrant generally achieves an acceptable balance between the investigative needs of government and the privacy interests of the people. *See*. But it has long been recognized that some searches occur in the service of "special needs, beyond the normal need for law enforcement," and that, when it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness.

Id. (quoting Vernonia Sch. Dist. 47J, 515 U.S. 646, 653 (1995)) (citations omitted).

356. Indeed, certain federal district courts and magistrate judges have held that the criminal Pen/Trap statute "does not authorize the collection of any post-cut-through digits." *See In re Certified Question of Law*, *supra* note 352, at 11 (collecting cases).

357. *See id*. at 10 ("The question whether title IV of FISA authorizes pen register orders to collect post-cut-through digits turns on the meaning of the definitional language in 18 U.S.C. § 3127(3). . . .").

358. *Id*. at 1–2. The question presented also included the caveat that the government could not make "affirmative investigative use" of any PCDs collected that were communications content. *Id*.

359. *See id*. at 4–5.

dialed after an original calling card connection — simultaneously exists as DRAS and architectural content (it is architectural content to the service provider). Some PCD information is communicative content — a credit card number, a password, or a social security number entered after the call is connected. We call this PCD quandary a "blurred boundary" because the government, at least under the current state of technology,[360] must collect content (architectural and communicative) in the course of collecting DRAS.

Of relevance to our discussion is the FISCR's response to certain arguments made by the amicus curiae in the case. The amicus curiae argued that all PCDs are "content with respect to the service provider" and that "the interception of post-cut-through digits should never be authorized."[361] The amicus curiae essentially made an architectural content argument without specifically using that terminology. In disagreeing with the amicus curiae, the court relied solely on the Wiretap Act's definition of content, what we have called communicative content, to conclude that PCD information that is dialing information is always just dialing information, "whether viewed from the perspective of the individual or the provider."[362] The court appeared to refuse to accept the idea that DRAS — in this case dialing information — can be non-content for one entity on the network, and content (in this case architectural content) for another. Without specifically parsing the differences between architectural and communicative content, however, several lower courts addressing the question of the collection of PCDs under criminal Pen/Trap authority have held that Pen/Trap does not authorize the collection of any PCDs.[363]

The amicus curiae further argued, more generally, that "if the government's argument were applied to Internet pen registers, the government could collect information generated by a wide variety of activities on the Internet, including searching, uploading documents, and drafting emails."[364] The court, not wishing to address the full implications of its reasoning as applied to the Internet, simply suggested that: (1) it would first "have to determine whether any technology is reasonably to excise content"; and (2) the consequences suggested by

360. *See id*. at 6 ("Because there is not now and has not previously been any known or reasonably available technology to segregate dialing information from content information in post-cut-through digits prior to the interception of those digits, the government has contended that it is entitled to obtain post-cut-through dialed digits even when the acquisition of such digits comes with some risk of intercepting content information.").

361. *Id*. at n.6.

362. *Id*. ("[T]he fact that the provider is not the one who uses that information for dialing purposes does not alter the fact that the information is dialing information.").

363. *See supra* note 356.

364. *See In re Certified Question of Law*, *supra* note 352, at n.7.

the amicus curiae "might call for a different Fourth Amendment balancing of interests."[365]

Even entirely with respect to dialed digits over voice telephone calls, the court's reasoning here leads to some counterintuitive — even perverse — outcomes when modest technological advances are considered. For example, most of today's automated systems that accept DMTF (tone) digits as input, including the "dial around" systems at play in this case, now also accept spoken digits, converting them to numbers using automated speech recognition technology. One could easily imagine a pen register system that records not only tone-dialed digits but also speech during the call, to ensure collection of any and all DRAS being sent by the target in the form of digits spoken to an automated system.[366] Of course, such a system would also record the entire spoken content of calls as well.

Would such a system be permissible under a pen register authority? What about a system that recorded only spoken digits during the call? Meaningful lines become very hard to draw here, even in the traditional telephony case.

In a paper written as a law student, Shane Huang has suggested that a simple "provider-conscious encryption test" can determine whether the material in a layer is content: if encrypting or scrambling that layer causes problems for a lower layer, it is metadata; if it does not cause any trouble, it is uninterpreted by that layer and hence must be content (what we have described as architectural content).[367] This

---

365. *See id*.

366. As far as the authors know, current telephone pen register collection technology used by the government does not do this, although there is no fundamental technical reason it could not.

367. Shane Huang, Distinguishing Content from Metadata: The Provider-Conscious Encryption Test (May 2, 2014) (unpublished student paper) (on file with authors).

Huang calls today's paradigm the "conceptual test": does the information sought "fit better into the conceptual categories of content or metadata?" The analysis noted that in a number of options, "the facts appear to involve only traditional telephone metadata held by traditional telephone companies, but the courts did not acknowledge any provider-specific reasoning when classifying information as less-protected metadata."

He instead proposes a "provider-conscious encryption test" to determine the boundary between metadata and content: see what would happen if part of the data were encrypted. If whatever mechanism — i.e., a lower layer of the network stack — that was transporting the encrypted content did not experience any problems, then the material was clearly content, at least to that layer. Conversely, if the system could not function properly under those circumstances, then the information being transmitted was material to the lower layer and could thus be considered metadata.

In fact, the provider-conscious encryption test is inadequate for two reasons. First, there are situations where the boundary is blurred, either inherently (e.g., in the case of mail headers) or in certain situations (e.g., for certain higher-layer protocols if Network Address Translators are present in the communications path). In these cases, if encryption is possible without causing difficulties, Huang's test properly concludes that as a syntactic matter, the encrypted data is content. A failure, though, does not always indicate that the data is non-content. It could be because of the boundary blurring; more seriously, as in several of our examples, users may be unaware of what is being sent.

test, however, does not function properly in all circumstances: email systems will misbehave if certain header lines in the message are encrypted (or are otherwise malformed or not effectively present), but an email message is always content,[368] probably both architectural and communicative content. Consistent, clear boundaries simply do not exist.[369]

In this paper, we've largely focused on examples where an uncritical application of the Pen/Trap statute to an IP-based communications environment may facilitate the acquisition of more information than law enforcement should be entitled to collect under Pen/Trap authority. But depending on configurations, sometimes law enforcement could end up with less. An instance of this problem occurs in domain fronting,[370] a technique in which domain names are manipulated in an HTTPS request so as to hide the authority within the encrypted portion of a path. The details are quite complex. Since to our knowledge the technique is currently used only to avoid censorship and not in US criminal contexts, we do not discuss it here save to note that the technological phenomenon exists.

There are other, similar boundary-blurring situations in the Internet today — notably, Network Address Translators[371] and certain firewalls. In the interests of minimizing the amount of technical arcana this Article covers, we have refrained from a detailed explanation. Nevertheless, they all have two critical properties: it is hard to draw a clean boundary between content and metadata, and Huang's test does not offer useful guidance. More precisely, a technical inability to encrypt some information without causing operational problems is a strong clue that intermediate systems need to access or modify that information; it does not, however, tell us anything about why there is a problem or how the problematic information is embedded in protectable information.

---

368. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) ("We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails.").

369. That headers could not be encrypted was known to the designers of S/MIME. *See* B. RAMSDELL & S. TURNER, SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME) VERSION 3.2 MESSAGE SPECIFICATION (RFC 5751) (2010), http://www.rfc-base.org/txt/rfc-5751.txt [https://perma.cc/AJ6U-8U7W]. RFCs are generally intended to document technical and organizational content not legal issues. *Request for Comments*, THE INTERNET ENGINEERING TASK FORCE, https://www.ietf.org/rfc.html [https://perma.cc/PS8S-EUK8].

370. *See generally* David Fifield et al., *Blocking-Resistant Communication Through Domain Fronting*, 2 PROC. ON PRIVACY ENHANCING TECH. 46 (2015).

371. *See* RFC 3022, *supra* note 262.

E. Discerning Content from Non-Content: Audio and Ambient Sound Processing

An emerging class of applications, on both mobile telephones and purpose-built specialized devices, process "ambient" sound from a local microphone. In some cases, these applications are always running, waiting for an audio signal to "wake up." For example, some Apple and Android phones will respond to spoken voice commands initiated by a special signal ("Hey Siri" and "Okay Google," respectively). The online retailer Amazon recently announced an appliance[372] built around a sophisticated always-on microphone array that responds to spoken queries (such as requests to add items to the user's online shopping cart). Other applications use always-on microphones to detect and respond to noise and non-verbal sounds in the local environment.

Because of computational limitations (and other factors that depend on the specific application), devices that process ambient audio often do so in conjunction with an online server provided by the application vendor or even with a third party vendor contracted by the application vendor. Sounds are continuously collected by the microphone and preprocessed locally to determine whether they are relevant or warrant further analysis. When a captured sound is determined to be of interest, it is sent to the server (which might have better computational capability and more context than the user's device). The server then processes the selected audio, for example, to convert speech to text, identify background music, count the number of people in the room, or whatever the application might require. That is, such applications follow the service-based architecture discussed earlier, with ambient audio processing as a centralized service.

Orwellian privacy implications of ubiquitous always-on microphones aside, such systems blur the distinction between content and metadata in a number of important ways. Clearly, the captured audio transmitted to the server is communicative content as defined under the Wiretap Act.[373] But what might seem at first to be innocuous metadata in the transmissions between the device and the server can,

---

372. *See*, *e.g.*, Sam Machkovech, *Amazon Announces Echo, a $199 Voice-Driven Home Assistant*, ARS TECHNICA (Nov. 6, 2014, 12:59 PM), http://arstechnica.com/gadgets/2014/11/amazon-announces-echo-a-199-voice-driven-home-assistant/ [https://perma.cc/WJ4F-9XL4].

373. While such audio collected in real time would clearly be covered by "super warrant" Wiretap Act standards, what legal standard would control law enforcement access to the audio if stored by the server? Although the audio is content, the company that owns the server is not a mere intermediary as the ISP was in *Warshak*. In some instances, the consumer has installed equipment in her home and purchased or consented to a service that delivers ads to her TV based on the ambient noise picked up in the room (see discussion below). Could this be the kind of content disclosed to and used by a third party that does not receive Fourth Amendment protection under *Warshak*? *See supra* Section II.C.

by itself, allow quite a bit to be inferred about the room audio, including what is being said in the room.

Researchers have developed practical techniques that infer content from digitally encoded and transmitted audio entirely from metadata about the audio signal.[374] Digital data is compressed to require less bandwidth,[375] and the pattern of the lengths of strings of packets can be revealing. Under certain circumstances, it is possible to recover significant portions of a conversation by identifying and recovering individual phonemes.[376] Other researchers have found that even if the communication is encrypted, it is possible to identify who is speaking.[377] More subtly, the patterns of packet sizes generated by different spoken languages are distinctive enough to identify which language a user is speaking, without any direct access to the audio bitstream itself.[378] When speakers switch languages during a conversation, the act of doing so reveals a situational change (e.g., a change in "governing norms"), which is also revealing of content.[379]

Moreover, because applications on the end-user's device generally select and pre-process relevant audio sent to the server, the mere fact that a client-server communication has occurred reveals, by its nature, that a sound-triggered event has been detected. The specific conditions under which this will happen will vary from application to application. At a minimum, it reveals that there is activity in proximity to the microphone. But, depending on the application and other metadata, communications metadata can reveal far more. In one patent application for a TV set-top-box ambient noise processing system, different ads are served depending on the type of activity

---

374. *See generally* Andrew M. White, et al., *Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on fon-iks*, 32 IEEE SYMP. ON SECURITY AND PRIVACY 3 (2011).

375. Voice, like text, is redundant. Much as "zipped" files are much smaller than the originals, voice can be compressed to less than one-fourth of its normal size. Typical voice compression algorithms use "variable bit-rate" encoders; this means that the output is only as long as is necessary to identify a particular sound. The different lengths, and hence the different sounds, can show through the encryption. This notion goes back to the earliest days of computer science; *see generally* Claude Shannon, *A Mathematical Theory of Communication,* 27 BELL SYS. TECH. J. 379, 379–423, 623–56 (1948).

376. A phoneme is the smallest unit of speech that can be used to make one word different from another. *Phoneme | Definition of Phoneme by Merriam-Webster*, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/phoneme [https://perma.cc/AG3E-AD8V]; *see also* White, *supra* note 374, at 3.

377. *See* Michael Backes, et al., *Speaker Recognition In Encrypted Voice Streams*, 15 ESORICS 508, 508–23 (2010).

378. *See* Charles Wright, et al., *Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?*, 16 PROC. USENIX SECURITY SYMPOSIUM 52 (2007).

379. *See generally* Jan-Petter Blom & John J. Gumperz, *Social Meaning in Linguistic Structure: Code Switching in Norway*, *in* DIRECTIONS IN SOCIOLINGUISTICS: THE ETHNOGRAPHY OF COMMUNICATION, 407, 407–34 (John J. Gumperz & Dell H. Hymes eds., 2014).

detected in the room.[380] If, for example, sounds associated with intimate romantic activity are detected, ads for appropriate products (getaway vacations, or perhaps contraceptives) will be displayed.[381] The fact that the server is delivering an ad from a particular source in response to an audio segment being sent reveals quite a bit about what might be occurring near the microphone. Such information is derivable without directly collecting the room audio itself.

Again, much of what we might think of as purely metadata here is strongly reflective of the underlying content. Seemingly innocuous information, such as packet sizes, connection lengths, and web sites contacted are, at least statistically, revelatory of the communicative content itself. In some situations, it is already possible to invert the relationship and derive the actual content that caused those ads to be shown.[382]

In circumstances where law enforcement may be unable to place a listening device in a room (either due to an operational challenge or the inability to satisfy the Wiretap Act's stringent legal standards), installing a Pen/Trap at the locus of the fiber or cable TV that targets the residence would allow law enforcement to collect DRAS information. As discussed above, this information could enable law enforcement to infer what was occurring inside the home. How might a court apply *Kyllo*[383] to this situation? In *Kyllo*, law enforcement used a thermal imaging device to scan Kyllo's home in an effort to detect whether marijuana was being grown inside the residence.[384] The Court held that the use of the sense enhancing technology to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search — at least where (as here) the technology in question is not in general public use."[385]

In *Kyllo*, law enforcement, positioned across the street from the home, used an uncommon technology to determine what was occurring inside a constitutionally protected space. In our example, installation of a Pen/Trap to pick up DRAS information sent between a home and third party provider — a party that has arguably been "invited" into the home — may not be perfectly analogous to *Kyllo*. Given the extremely revelatory and private information about goings-on inside the home that can be inferred from DRAS information, a court should at least be given the opportunity to determine if the Pen/Trap rele-

380. U.S. Patent Application Publication No. 2012/0304206 (November 29, 2012).

381. *Id.* at ¶ 0048.

382. *See* Mathias Lécuyer et al., *XRay: Enhancing the Web's Transparency with Differential Correlation*, 23 PROC. USENIX SECURITY SYMPOSIUM 49 (2014).

383. *See* Kyllo v. United States, 533 U.S. 27 (2001).

384. *See id*. at 29–30.

385. *Id*. at 34 (citations omitted).

vance standard would be constitutionally sufficient for the collection of DRAS information, or whether a higher standard is required. Moreover, if law enforcement's intent is to collect DRAS information for the purpose of determining what is occurring inside a home, it is unlikely that a court would be aware of this fact given that all law enforcement must do under the Pen/Trap statute is to certify to a judge that the information sought is relevant to an ongoing criminal investigation.[386]

F. Service Location Ambiguity

While the PSTN can accommodate modems, faxes, and 800 numbers, it is not an architecture that facilitates finding a Moroccan restaurant near your destination, calculating the time needed to reach it based on current traffic, and then arranging a dinner reservation. IP-mediated communications can provide such services and more. These various services can be executed in many different ways, with different degrees of involvement — including none at all — by third parties.

In earlier Parts, we observed that at times it is essentially impossible for the user to determine whether information is shared with a third party. In this Part, we illustrate this issue in a different situation: that of determining whether a service is provided locally or remotely, or somewhere in between. Consider the issue of making that dinner reservation. From the user's vantage point, she uses her phone to look up restaurants near her destination, to calculate the time she will arrive, and to make a reservation. The user rarely thinks about how such capabilities are achieved. Even if she does, it is hard to determine exactly where the information of her location, her destination, and her estimated time of arrival is stored and computed. It could be done entirely on her phone, as it is on many standalone Global Positioning System ("GPS") devices, it could be done on cloud servers, or it could be done jointly. Many users accessing cloud services do not understand where data resides.[387] Knowing where this information is stored is important for determining whether or not the third-party doctrine applies.

We discuss a practical example of a system that might reasonably be designed to occupy any of a number of places on the architectural spectrum from purely local to fully cloud-based: a mapping application that allows the user to see their location on maps of the local area and plot routes to different places. This example, which shows how the same service can be implemented in three different ways, illus-

386. *See* 18 U.S.C. § 3122(b)(2) (2012).
387. *See infra* Section IV.F.2.

trates that it is impossible for most users to know or discover whether they are disclosing information to a third party.

Mapping applications that perform these functions exist for standalone GPS devices as well as general-purpose computers and smartphones. While all functionally similar, these applications make very different uses of network-based services depending on their architecture. As a consequence, they can emit very different information and metadata to third party service providers and external eavesdroppers.

A mapping application can determine its own location in a variety of ways. For the purposes of our discussion, we assume that in each case the computer is equipped with a sensor that receives signals from the US government's constellation of GPS satellites. As long as the receiver is within the line of sight of sufficiently many GPS satellites, the receiver can calculate its position on Earth to within several meters.[388]

The use of GPS does not, by itself, emit any information to any third party. GPS receivers used by consumers (and now built into almost all current mobile phone handsets) are passive devices that do not transmit any signals.[389] A user's location (latitude, longitude, and altitude) is calculated entirely within the receiver based on the received signals.[390]

However, most modern mapping applications that use GPS do not simply display position as numeric latitude and longitude. Rather, they display the location on a map, in the context of surrounding streets and landmarks. Many GPS applications can also provide turn-by-turn driving directions to a destination, and can display real-time traffic conditions to help the user avoid or anticipate delays. Such features are now common to virtually all currently distributed mapping applications.

---

388. There are currently approximately thirty-two actively operational GPS satellites in low-earth orbit around the globe. To calculate latitude and longitude a user must be within line of sight to at least three, and to calculate latitude, longitude, and altitude, the user must be within line of sight of at least four. In practice, a GPS receiver must simply be outdoors with a reasonably clear view of the sky. *See generally Official U.S. Government Information About the Global Positioning System (GPS) and Related Topics*, GPS.GOV, http://www.gps.gov [https://perma.cc/NEN5-EFLR] [hereinafter *Government Information about GPS*].

389. *See id.* In addition to their internal GPS receivers, most modern smartphones can use the presence of nearby Wi-Fi networks and cell towers to determine approximate location. Unlike a GPS system, though, these other schemes do not directly produce longitude and latitude information. Instead, they are used in conjunction with large server-resident databases, and can thus be considered "location as a service." *See, e.g.*, Fred Zahradnik, *WiFi Positioning System*, ABOUT TECH, http://gps.about.com/od/glossary/g/wifi_position.htm [https://perma.cc/T9Z9-RBQB]. However, this does not alter our basic analysis. In fact, it is yet another example of how the same function can be done in different ways with different privacy implications.

390. *Government Information about GPS*, *supra* note 388.

Whether a mapping application reveals information about the user's current position, destination, or travel history to a third party depends on the architectural choices made by the designer. Whether a mapping application relies on — and reveals information to — a service provider depends on its design rather than anything inherent in the functionality. We will discuss a range of possible architectures, each of which reveals a different amount of metadata to third parties.

1. Standalone, Entirely Local Architecture

Some GPS applications and devices are designed for autonomous offline operation and do not depend on a live Internet connection for their operation. Here, all mapping data for the areas to which the user travels are pre-loaded on the user's computer, so the appropriate map segments can be displayed for the currently calculated position. This mapping data may include both graphical representation of landmarks as well as information about streets and traffic rules. This allows the application to not only display the current position on a map, but also to calculate driving directions to a selected destination.

Real-time information on road conditions (such as traffic congestion) can also be displayed (and taken into account in calculating directions) if the application has a source for this information. Obtaining traffic data does not always require the use of an Internet connection. Local traffic data is digitally broadcast over a special subcarrier channel on many FM radio stations. If the computer is equipped with a suitable receiver, this data may be available to the mapping application. However, simply because the mapping application is receiving real-time FM radio generated information does not mean that the user is disclosing information to any third party.

This kind of "stand-alone" architecture[391] is commonly used in purpose-built GPS receivers,[392] and can also be implemented on applications for smartphones and general-purpose computers.[393] Under this architecture, the mapping application does not reveal any information about its location, or even the fact that it is being used, to anyone. Because all data (map graphics, GPS position, and real-time

391. Stand-alone maps are often used when there is no connectivity, for example, a GPS system built into a car; when connectivity would be prohibitively expensive, for example, when traveling in a foreign country; or when traveling in remote areas where there is no cellular coverage.

392. For example, Garmin, a manufacturer of stand-alone GPS devices, offers models with real-time traffic data from both receive-only FM radio as well as two-way 3G/4G/LTE Internet service. Whether the service is receive-only or Internet-based may not be functionally apparent to the end user. *See Garmin Traffic*, GARMIN, http://www8.garmin.com/traffic/ [https://perma.cc/UH3P-37FM].

393. Mapping smartphone applications that can operate offline with pre-loaded maps are available from, for example, OpenStreetMap. *See* OPENSTREETMAP, http://openstreetmap.org/about [https://perma.cc/U497-RPFE].

traffic) are either stored or calculated locally, with no network-based capability depended upon, no location data ever leaves the user's device.[394]

2. Fully Connected Architecture

Other mapping applications occupy the opposite architectural extreme, using "mapping as a service," with the user running software that provides little more than a user interface to a remote mapping server. This is the approach used by many (but not all) mapping programs that run in web browsers or on smartphones, such as Google Maps, Apple Maps, etc.

In this architecture, the user's software periodically reports its current location (as calculated from a GPS sensor or other techniques)[395] to a mapping server operated by the application provider. The server then returns the current map segment, centered on the user's location, for display. As the user moves around, the updated location is sent to the server so appropriate map segments can be retrieved. Current mobile networks have sufficient bandwidth to allow maps to be sent and updated effectively in real time as the user moves around an area. Maps can typically be annotated with real-time traffic information and similar information, which is also obtained from the server.

Routes from one place to another are usually calculated on the provider's server rather than on the user's device. The software typically sends the starting and ending points to the server, where a route is calculated and returned to the user's device for display.

In this type of architecture, there is quite a bit of communication between the user's device and the application provider's servers. This communication is typically over a mobile wireless network, such as 3G or LTE services provided by cellular carriers. Depending on the particular implementation, such applications may stop working altogether if communication is interrupted, or they may operate with more limited functionality. For example, they may rely on the integrated GPS to update the displayed position but not provide updated road condition information or display map context when moving out of the last downloaded segment.

Thus, even in the case of a pure mapping-as-a-service architecture, where there is a substantial amount of communication between

394. Whether content or metadata, if law enforcement wants to access information on a user's device, a warrant will generally be required. *See* Riley v. California, 134 S.Ct. 2473, 2493 (2014) (holding that "a warrant is generally required before . . . a search, even when a cell phone is seized incident to arrest").

395. The location might be calculated purely locally by GPS or by the WiFi technique described previously. *See* Zahradnik, *supra* note 389.

the user's device and the application provider's server, the information displayed to the user is not always a result of the communication of the user's location to the third party application. The user doesn't know when she is actually sharing her location with the third party server. In the context of application of the third-party doctrine, should a user be expected to know that she is always or sometimes sharing her location with the mapping application? In *Smith*, the Court references phone books and long-distance listings on bills as the type of information that puts consumers on notice that the numbers they dial will not remain secret.[396] Are there analogous real-world cues to put the user on such notice in the context of mapping applications?

What content is sent to a third party in the fully connected, mapping-as-a-service architecture? This determination is partly a question of position and perspective on the network. The mobile network carries the traffic between the user's device and the application provider's servers but does not process it. To the carrier, everything except the existence of the communication is architectural and communicative content. From the perspective of the application provider — that is, the mapping service — the user's locations are delivered to it as communicative content, but, unlike the carrier, it is a recipient of the communication containing that content and which it has explicitly requested. However, one form of location determination uses carrier-provided information.[397] From a technical perspective, this can be understood as another illustration of the use of architectural content and architectural metadata: the carrier has provided location information as metadata, but it is sent to the mapping service as content. In this case, some of the location information may have actually originated from a cellular provider,[398] thus blurring the boundary even further.

3. Middle-Ground Architectures

Some applications employ a hybrid architecture that is neither entirely offline nor entirely service based. This hybrid is partly a matter of trading off frequent communication (in a more service-based application) for increased storage and computation (in a more offline application). A mapping application can occupy a middle ground between the two extremes by employing essentially a service-based design, but using map segments that cover a large enough geographic area such that the current precise location need not be reported as frequently as in a purely service-based architecture. That is, a single re-

396. Smith v. Maryland, 442 U.S. 735, 742–43, 748–49 (1979).

397. For example, the positions of nearby cell towers can be used to determine location. *See* Zahradnik, *supra* note 389.

398. *See id.*

quest from the user's device to an online mapping service can download considerably more data than is immediately necessary. The additional data could include the surrounding area, the immediate area zoomed in or out, etc. There are a number of reasons for this, including the considerable expense of calculating the area and initiating a transaction; the actual data transfer is a comparatively small part of the cost of the operation. This middle ground is thus primarily a technical engineering decision, depending on the business model of the provider, the capabilities of the users' devices, and the expected reliability of the communications infrastructure. Most phone-based mapping software, including Google Maps, operates this way.

From our point of view, what is notable is that an application's position on this spectrum between online and offline operation is essentially opaque to the end user. Whether a mapping application is sending its location to the application provider frequently, occasionally, or never need not manifest itself in the behavior of the software. Identical functionality can be provided from any place on the spectrum. In fact, the behavior of even a single application can change over time as the application provider adjusts parameters to manage performance; these changes are entirely invisible to the user. Particularly in the context of the fluidity of middle-ground architectures, it will be difficult, if not impossible, for a user to know or discover when she is sharing data with a third party. Such variable, essentially unknowable conveyances can hardly be seen as voluntary. This challenge is equally problematic for courts. How are they to discern, in middle-ground architectures, when a user makes a voluntary conveyance under *Miller* and *Smith*?

We note that mapping software is but one example of this phenomenon. Indeed, virtually any application can be built along a similar continuum from entirely local to entirely service-based, with the degree to which data moves from client to server effectively invisible to the user. The actual information transmitted and the destination of whatever information is sent is not only unknown to most people but can also vary over time, even for the same service.

G. Other Examples

There are many other important Internet applications that demonstrate the difficulty of drawing the line between content and metadata. Here we present a brief analysis of three such examples.

1. The Domain Name System

The Domain Name System ("DNS") is the Internet service that converts host names such as "www.supremecourt.gov" into IP ad-

dresses. Because of the way in which DNS functions, law enforcement needs access to DNS message payloads — which are architectural content and arguably communicative content — in order to obtain metadata that is available in the phone network.

The problem is more complex because of the many different computers that are involved in DNS name resolution. In common (but not mandatory) configurations, the metadata alone generally does not indicate which party has made a request nor what hostname the request is for. That is, a Pen/Trap on a consumer's link to the Internet would show the existence of a DNS query but not which site is being requested; a similar Pen/Trap on a DNS name server would show the ISP from which the query came but not the actual consumer.

2. Ad Networks

Many "free" online services are supported by advertising supplied by ad networks. These create complex communications patterns that are not always directly triggered by the users' intentional interactions with the applications that incorporate them. They involve third parties largely hidden from the user without notice to the user.

The ads themselves and the data sent by the user to fetch the ads should be considered communicative content. However, the patterns of communication between an application and its interacting ad networks are quite revealing. For example, not only can they indicate which applications are on a user's device, but they can also indicate when they are used.[399] These communications are transmitted silently, without the user explicitly initiating them. In no way can they be said to be voluntary.

While such a traffic pattern may technically be DRAS information falling under the Pen/Trap statute, its collection under Pen/Trap is not consistent with an application of the third-party doctrine requiring a voluntary conveyance of information under *Smith*. A Pen/Trap placed at the locus of an ad network would be collecting DRAS between the ad network and the application. This highlights a conflict between: (1) what the Pen/Trap statute authorizes for collection under a relevance standard and; (2) the collection of DRAS information which may not be subject to the third-party doctrine. Furthermore, this monitoring can be used to infer what applications are on the phone. In *Riley*, the Supreme Court held that if law enforcement wants to access information on a user's device, a warrant would generally be required.[400]

---

399. There is a vast literature on "application protocol identification." *See, e.g.*, Charles Wright et al., *On Inferring Application Protocol Behaviors in Encrypted Network Traffic*, 7 J. MACHINE LEARNING RES. 2745 (2006).

400. Riley v. California, 134 S.Ct 2473, 2493 (2014).

3. Metadata as Messages

An extreme example of how meaningless the distinction between content and metadata can be is the application Yo. Originally designed as an April Fool's joke but quickly enjoying considerable commercial success, the initial Yo application was a messaging service that transmitted the message "Yo" — nothing more.[401] In this instance the metadata — the notification that the user has a message — is the message/content.[402] That said, in many countries, Yo has become a serious application employed for serious uses. For example, in Israel, Yo has provided users with a notification of an inbound missile though not whether it will hit nearby.[403]

4. Middle Boxes

Although the basic Internet architecture favors end-to-end services, in recent years there has been a proliferation of "middle boxes," components residing within the network that provide useful and/or profitable services.[404] There are many types of middleware; one particularly important form is the web proxy.[405]

For our purposes, middle boxes have three salient features. First, they are privy to (and sometimes modify) a great deal of information that is in fact architectural content. For example, some web proxies filter content considered inappropriate by the box operator.[406] Second, they are often run by third parties, which may raise some third-party doctrine issues we have identified in this Article.[407] Third, middle boxes are often invisible to users. Regardless of whether or not a necessary function should be considered voluntary,[408] it is harder to argue

401. Alyssa Bereznak, *Developers Have Hit a Yo Point with This Terrible New App*, YAHOO! TECH (June 19, 2014), https://www.yahoo.com/tech/developers-have-hit-a-yo-point-with-this-terrible-new-89277145724.html [https://perma.cc/9K95-D8BK].

402. *See also* Elgort, *supra* note 188, at 1040 (discussing phone ringing as a signal).

403. *Yo App Warns Israeli Citizens of Missile Strike*, BBC NEWS (July 10, 2014), http://www.bbc.com/news/technology-28247504 [https://perma.cc/4P4S-TNDC]. This application has middling value: the user is informed that there is an incoming missile, but is not alerted as to whether that missile is targeted nearby.

404. *See, e.g.*, B. AIKEN ET AL., NETWORK POLICY AND SERVICES: A REPORT OF A WORKSHOP ON MIDDLEWARE (RFC 2768) (2000), https://www.ietf.org/rfc/rfc2768.txt?number=2768 [https://perma.cc/TW4W-QWMK]; J. KEMPF & R. AUSTEIN, THE RISE OF THE MIDDLE AND THE FUTURE OF END-TO-END: REFLECTIONS ON THE EVOLUTION OF THE INTERNET ARCHITECTURE (RFC 3724) (2004), https://www.ietf.org/rfc/rfc3724.txt [https://perma.cc/D58M-9ZNB].

405. *See generally* BALACHANDER KRISHNAMURTHY & JENNIFER REXFORD, WEB PROTOCOLS AND PRACTICE 59–80 (2001) (explaining the function of web proxies).

406. *Id.* at 68–69.

407. *See generally* discussion *supra*, Part IV. Not all middle boxes are run by third parties. *See, e.g.,* KRISHNAMURTHY & REXFORD, *supra* note 405, at 17 (discussing load balancers); *id.* at 438 (discussing content distribution networks).

408. *See supra* Section II.C.2.

that information taken by an optional, invisible feature deployed by, say, an ISP has been voluntarily conveyed. That said, any concrete analysis of the legitimacy of Pen/Trap access via a middle box operator is very dependent on exactly which type of box is used and how it is operated.

H. Concluding Remarks

The various examples discussed in this Part illustrate how, in an IP-mediated communications environment, the distinction between content and non-content steadily erodes to the point of collapse. Moreover, the examples demonstrate that it is practically impossible for a user to know or even discover when she discloses information to myriad third parties. The concept of voluntary conveyance contemplated in *Smith* is little more than a fictitious discussion in an IP-mediated communications environment. Accordingly, the content/non-content distinction and the third-party doctrine are no longer workable rules for courts to apply.

In the next Part of this Article, we discuss some general conclusions and effects stemming from the breakdown of the content/non-content distinction and the third-party doctrine. Understanding that appropriate legislative action will take time, we offer some interim guidance to both the DOJ and courts with respect to use and authorization of the Pen/Trap statute.

V. RECOMMENDATIONS

Four conclusions follow from the predicament we describe:

(1) The concept of metadata as a category of communication information that is wholly distinguishable from communications content is outdated.

(2) The current rules are too difficult to apply — *Katz*, *Smith*, and the definitions of content and non-content found in the Wiretap Act and Pen/Trap statute are no longer viable rules for regulating law enforcement access to data in an IP-based communications environment.

(3) When these older rules are applied to the Internet, they lead to inconsistent and anomalous results.

(4) The general notion that a user voluntarily conveys information — as contemplated in *Smith* — in the context of a complex, IP-mediated communications environment is an unsustainable legal fiction.

We discuss each of these conclusions in turn:

(1) *The Concept of "Metadata" is Outdated.*

In the telephony era, dividing communications data into "content" and "dialing information" made sense. That technology enabled distinctive, workable legal definitions and corresponding privacy protections. Today, however, there are many more categories of information, and metadata provides much more and often much richer information than DRAS information did in the context of the PSTN. Because the content of a communication can sometimes be inferred from its corresponding metadata, however, it is not clear that distinct, meaningful legal lines can be drawn between these two categories of information in the way it could be done during the telephony era. The concept of metadata as a category of information that is entirely distinguishable from communications content and thus deserving of lower privacy protection is no longer tenable.

(2) *The Current Rules Distinguishing Content and Non-Content are Too Difficult to Apply.*

Understanding where the boundary is between metadata and content is specific to the situation and the communications protocol used. Simple guidelines such as "email addresses are metadata" are often misleading. A detailed understanding of the technical minutiae of Internet protocols is therefore required to begin the analysis. As we have seen in many cases (for example, URLs and service location ambiguity), it is necessary to do a deep analysis of the specific fact pattern of each desired interception to determine where the boundary may lie.

(3) *On the Internet, Older Rules Lead to Inconsistent and Anomalous Results.*

Internet architecture is sufficiently different from the PSTN that the analogies simply do not make sense. The flexibility of IP communications complicates the situation further, since often there are multiple ways of accomplishing a task. For example, blurred boundaries show how even a structural rule cannot distinguish between content and non-content.

(4) *The General Notion that a User Voluntarily Conveys Information is an Unsustainable Legal Fiction.*

The concept of voluntary conveyance, as recognized in *Smith*, depended upon a knowing and voluntary disclosure of information by an

individual to third party. In an IP-based communications environment, it will become increasing difficult for a user to know or discover when and what kind of information she is disclosing to myriad third parties.

In summary, the Internet is far more complex than the phone network was in 1979. Electronic surveillance laws and policies must accommodate this complexity. Relying on the courts to perform the kind of broad reform that is needed is an unlikely path to success; the complexity of the analysis is too great and the results are likely to be too confusing for easy application by law enforcement. Legislative action would provide an opportunity for a statute that could draw the kind of nuanced distinctions required for an appropriate balancing of law enforcement and privacy equities in the context of an IP-based communications world. We have not attempted to map out new legislation, but we have below provided principles to guide its direction.

Meanwhile there is an immediate problem. The consequences of the current mismatch between law and communications technologies likely play out daily in investigations and court authorization of Pen/Trap applications. We present a set of recommendations to help guide decisions in the interim before new legislation alleviates the divergence between old electronic surveillance law and new communications technologies.

A. Recommendation for the Department of Justice

As we have observed in our discussion on email headers, the DOJ's 2005 Electronic Surveillance Manual and 2009 Search Manual contain an incorrect conclusion regarding email headers.[409] The SMTP address is addressing information within the context of the Pen/Trap statute; the email header "From:" is not. This error, which has likely propagated throughout law enforcement,[410] should be corrected immediately. The 2005 Electronic Surveillance Manual discussion of Pen/Trap orders currently reads as follows:

> Pen register and trap and trace devices may obtain any non-content information — all "dialing, routing, addressing, and signaling information" — utilized in the processing and transmitting of wire and electronic communications. Such information includes IP

409. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91; 2009 SEARCH MANUAL, *supra* note 95. *See also,* discussion of email headers, *supra* Section IV.B and note 307.

410. *See* U.S. MARSHALS SERVICE, POLICY DIRECTIVES 15.1, NON-CONTENT INTERCEPT UNDER THE PEN/TRAP STATUTE 22, http://www.usmarshals.gov/foia/directives/technical_operations.pdf [https://perma.cc/838F-349Q] (including the same language as in the DOJ manual regarding email headers "To" and "From").

> addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail.[411]

The second and third sentences of the Electronic Surveillance Manual's language should be replaced with the following:

> Such information includes IP addresses and possibly port numbers.[412] While pen/trap orders can obtain the sender and recipient email addresses, they cannot authorize the interception of the content of a communication. This content includes the information in the "To" and "From" email headers, words in the "subject line," and the body of an e-mail.

The 2009 Search Manual should also be amended to correct the same error. Judges should be informed of these changes.[413]

B. Recommendations for Judges

Throughout this Article, we have argued that the content/non-content distinction and the third-party doctrine, as codified in the Wiretap Act and the Pen/Trap statutes, are no longer workable rules in an IP-based communications environment. New statutory rules (or at a minimum, new statutory definitions) that account for these realities in an IP-based communications environment will take time to develop, but the specific observations below, more precise than the general principles above, should be useful to the courts.

(1) Some IP-based data is neither DRAS information nor content.

(2) With respect to the technical design of the Internet, the intent was that certain information was to be transmitted between the sender's computer and the receiver's without examination or use by intermediate parties. This is analogous to the way the phone company carries voice but does not use it. Today's Internet is considerably more complex

411. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 91, at 39.

412. Per the discussion in Section III.D, the content/non-content status of port numbers is unclear.

413. *See supra* note 307.

than its architectural specifications might suggest, and under certain circumstances, some of this transmitted information may be accessed and used by intermediaries. Because of such complexity, the content/non-content status of some data cannot be addressed in the abstract, but must be examined on a case-by-case basis.

(3) IP-based data that may technically be DRAS information but may otherwise reveal information that is more content-like in nature may be protected under separate, existing Fourth Amendment doctrine.

(4) The concept of a knowing, voluntary conveyance of information to a third party, as contemplated in *Smith* is, at best, a legal fiction in an IP-based communications environment.

We also offer some interim guidance to assist courts with evaluating Pen/Trap applications for IP-based communications under current statutory regimes. These recommendations are by no means all-encompassing rules for analysis. The first part is a series of questions and determinations for courts to make when evaluating Pen/Trap applications in an IP-based communications environment. The second part concerns specific categories of IP-based data. We caution, however, that the IP-data guidelines are "95% rules." That is, our analysis would apply to most, but not all situations, or may address only particular elements of the overall analysis.

As we have noted, this Article has examined only whether or not a third party actually participates in a given Internet transaction or whether or not the user is aware of transactions with such third parties. We have not proceeded further to conduct reasonable expectation of privacy analyses.

Overall, we suggest the following procedure for judges evaluating Pen/Trap applications for IP-based communications before the collection occurs.

(1) Inquire about the functionality and form of the information that will be collected with each application.

(2) Determine whether it is entirely third-party DRAS information.

(3) If it is not third party DRAS information, ask the government if technology is available to collect only the DRAS information.[414]

414. *See* 18 U.S.C. § 3121(c) (2012).

(4) If not, order briefing (perhaps inviting amici) to determine whether the over-collection involves content or non-DRAS non-content information and ultimately whether a Title III order or Rule 41 search warrant would be required for collection by law enforcement.

Again, these are general principles. They do not address claims asserting that even if the information is third party DRAS, there may not have been a voluntary conveyance by the user, as contemplated in *Smith*. These kinds of challenges will likely arise at the district court level by defendants in the context of a motion to suppress. We have argued that, in an IP-based communications environment, voluntary conveyances will be the exception rather than the rule. In these circumstances, courts will need to conduct a "reasonable expectation of privacy" analysis without the benefit of the third-party doctrine.

Below are several recommendations specific to IP data:

(1) Collection of email headers: Whether an email address is DRAS information or content depends on which protocol element it appears in: the SMTP dialog or the mail message itself. Email Pen/Trap orders should require that collection be of the envelope addresses in the SMTP dialog, and not from the headers in email messages. Headers in email messages are clearly content.

(2) A special situation arises if the target of the order is using a web-based mail service such as gmail.com. In that case, there is no SMTP dialog between the user and a server; there is just web browsing. Picking out just the Pen/Trap content — the "To:" and "From:" addresses — from a web page requires a technology known as "screen-scraping." Screen-scraping is very challenging to implement correctly and can easily collect unrelated communications.[415] Moreover, since connections to the three major web mail providers (Google, Microsoft, and Yahoo) are normally encrypted,[416] a simple wiretap or Pen/Trap will not pick up

415. As noted, even the NSA has found this difficult. *See* Higgins, *supra* note 348.

416. All three have made statements about encryption. *See Staying at the Forefront of Email Security and Reliability: HTTPS-Only and 99.978 Percent Availability,* GOOGLE OFFICIAL BLOG, http://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html [https://perma.cc/HT5Q-7LDW]; *Explained: How 'TLS' Keeps Your Email Secure*, YAHOO! TECH, https://www.yahoo.com/tech/explained-how-tls-keeps-your-email-secure-88310223169.html [https://perma.cc/4N7X-8CB9]; *Advancing Our Encryption and Transparency Efforts*, MICROSOFT CORPORATE BLOGS, https://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/ [https://perma.cc/4N7X-8CB9]. Google also supplies statistics on interprovider email en-

anything that is useful to law enforcement. For these reasons, law enforcement will need to serve a subpoena or a Section 2703(d) order on the provider who will, in most cases, have access to an unencrypted version of the email address.[417] This process, while perhaps not real-time Pen/Trap collection, provides law enforcement with the information it seeks without the over-collection risk of screen-scraping and similar methods.[418]

(3) Collection of IP headers: The IP header, including source and destination IP addresses, is intended for use by intermediate routers, and thus will generally be third party information. Accordingly, it should be obtainable legally using a Pen/Trap order.[419] However, parts of the IP header are not DRAS information, and thus not covered by the Pen/Trap statute.[420] This includes, as explained in Section III.C, packet length. If information is not DRAS, courts should determine whether the information being collected falls under a different statute or whether the collection of the non-DRAS information implicates Fourth Amendment concerns.

(4) Collection of port numbers: The TCP header is normally end-to-end, and thus should not be subject to the third-party doctrine. Note that this includes the port numbers. That said, it is unclear if there is a reasonable expectation of privacy in port numbers. As explained in Section III.C, ISPs often examine and use port numbers even though they theoretically do not need to do so. There is other information in the TCP header that is neither content, as defined in the

---

cryption. *Email Encryption in Transit*, GOOGLE TRANSPARENCY REPORT, https://www.google.com/transparencyreport/saferemail/ [https://perma.cc/CWQ7-XZHE].

417. 18 U.S.C. § 2703(d). A Section 2703(d) order, provided for by the Stored Communications Act (SCA), does not authorize prospective collection. It compels the disclosure of stored data. Depending on the facts of the specific investigation, law enforcement may therefore need to serve a series of Section 2703(d) orders on a provider.

418. According to a press conference statement by a spokesperson from the Office of the Director of National Intelligence, the NSA has experienced problems in exactly this situation. *See Intelligence Agency Attorney on How "Multi-Communication Transactions" Allowed for Domestic Surveillance*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Aug. 21, 2013), https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed [https://perma.cc/J96P-ZQT4].

419. *See infra* for a discussion on advanced analytics.

420. Note that the definition of content in 18 U.S.C. § 2510 no longer includes "any information concerning the identity of the parties to such communication or the existence." Wiretap Act, *supra* note 55. Per the discussion in Part III, information about the existence of an Internet communication is contained in the TCP header.

Wiretap Act, nor information given to third parties.[421] Whether law enforcement can collect this information requires further analysis.

(5) Collection of URLs: The path and query sections of the URL are typically not DRAS information and should normally be considered content. The path can indicate, for example, what story on a newspaper site is sought, or what article on Wikipedia is being read or edited. The authority section of a URL is generally third-party metadata, but the analysis is complex. Per Section IV.C.1, *supra*, when it is determined that the authority section is not third-party data, a reasonable expectation of privacy analysis is needed to evaluate whether a search has occurred. It is also possible for the authority portion of the URL to be content, but again, the analysis is complex (see *supra* Section IV.C.1).

As previously indicated, there are certainly more complex scenarios. In some situations, for example, collecting DRAS information or other forms of non-content can reveal content. Such scenarios include advanced analytics: for example, using IP address patterns to learn which apps are on a cell phone, or using packet sizes to ascertain which language is being spoken during a voice over IP call. These kinds of situations will likely be matters of first impression for a court and may be more appropriately analyzed and addressed after the collection has occurred. Therefore, a defendant may be successful in a motion to suppress at the district court level if she can show that law enforcement actions amount to an unreasonable search under existing Fourth Amendment doctrine.

C. Guidance to Policymakers

The only real way out of the morass of the currently overcomplicated situation is through new legislation. Unlike the specific suggestions proposed for the DOJ and judges handling current cases, we have provided several philosophical points for policymakers for consider. Though we make no specific legislative proposals, here are a few guiding principles:

(1) We have employed the terms "architectural content" and "communicative content" to illustrate how content on the

421. Examples include the Acknowledgement Number, Window Size, and Urgent Pointer. *See* RFC 793, *supra* note 205, at 15.

Internet can be a function of either structure or semantic meaning. Sometimes, a given unit of data may appropriately be classified as both architectural and communicative content. Legislators must understand how these dual concepts of content operate in an IP-based communications environment and resist the temptation to focus solely on whether any specific unit of data is DRAS information. DRAS information may be architectural content depending on where in the network law enforcement seeks to compel the data. Moreover, DRAS information may reveal communicative content.

(2) The law should be solidly grounded in today's technical realities. Simply trying to extend the concept of a "dialed phone number" to the Internet does not work. At the same time, it is crucial that the law not focus too closely on current technological paradigms. In the brief time in which this paper was written, notifications as communications went from an April Fool's example — Yo — to a set of serious products.

(3) The consideration of the appropriate level of privacy protections that should be afforded to various kinds of communications information must account for the existence of "big data" analysis. Indeed, the momentum and analytical capacities driven by big data is changing even faster than technology in general.[422] While the law does not generally regulate how information is analyzed once lawfully collected, the revelatory insights afforded by big data should give rise to new and stronger privacy considerations for non-content.

VI. CONCLUSION

In *Ex Parte Jackson*, the Court performed a structural analysis of a package and provided Fourth Amendment protections to the inside "layer" of the package but did not extend protection to the outer, publicly exposed layer of the package. In this scenario, the Court had only to account for a two-layer, stable architecture and was able to construct a constitutional rule that remains viable today. At the time of

422. *See, e.g.*, EXEC. OFFICE OF THE WHITE HOUSE, PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, at 27 (2014) ("Social-media data can be used as an input source for scene extraction techniques. When these data are posted, however, users are unlikely to know that their data would be used in these aggregated ways and that their social media information (although public) might appear synthesized in new forms.").

Smith, the PSTN's physical separation of voice from the dialing and routing elements of a communications facilitated a simple distinction between content and metadata, which is reflected in the Wiretap Act and the first iteration of the Pen/Trap statute. But the PSTN structure that enabled this content/non-content distinction was already beginning to change at the time of *Smith.* Specifically, when Sprint and MCI filed to offer residential long distance services in 1979,[423] they lacked direct access to phone switches.[424] As a result, their customers first needed to dial their carriers, and — after those calls were connected — enter their account numbers and then the actual phone numbers desired. In other words, in the year *Smith* was decided, dialed numbers — metadata — were about to be transmitted as content.

The Internet disrupts the content/non-content distinction even further, arguably to the point of collapse, as it ceases to remain a workable rule for courts to apply in the context of an IP-based communications environment. Specifically, the multi-layered nature of the Internet requires an analysis of content that is based on structure — architectural content — in addition to "meaning" as used in the Wiretap Act — communicative content. Unlike the simple, two-layered structure of a package, the determination of what constitutes architectural content on the Internet, which is a function how the Internet was designed to transport data, requires a technological analysis that most courts are not capable of doing on a daily basis. Content determinations — both communicative and architectural — are further complicated by the fact that the answer could change depending on where in the network law enforcement seeks to compel the data and that, at times, data may appropriately be defined as architectural and communicative content.

---

423. *See* CANTELON, *supra* note 13, at 291, 293.

424. *See United States v. Am. Tel. and Tel. Co.*, 552 F. Supp. 131, 195 (D.D.C. 1982) ("One of the government's principal contentions in the AT&T case was that the Operating Companies provided interconnections to AT&T's intercity competitors which were inferior in many respects to those granted to AT&T's own Long Lines Department . . . [A] substantial AT&T bias has been designed into the integrated telecommunications network, and the network, of course, remains in that condition. It is imperative that any disparities in interconnection be eliminated so that all interexchange and information service providers will be able to compete on an equal basis.") The bias was that consumers automatically were connected to the AT&T network but had to work harder to reach Sprint or MCI: "Long distance calls may presently be placed over the AT&T network by dialing ten or eleven digits while twenty-two or twenty-three digits are necessary to use the facilities of the other interexchange carriers." *Id.* at 197. "This conclusion is buttressed by the requirement in the proposed decree that the divested Operating Companies provide a service which will permit a subscriber to route his calls automatically to a single interexchange carrier other than AT&T." *Id.* at 198. Consequently, the court ordered that "[t]he governing principle established by the proposed decree is that by September 1, 1986, the Operating Companies must provide access services to interexchange carriers and information service providers which are 'equal in type, quality, and price' to the access services provided to AT&T and its affiliates." *Id.* at 196.

Similarly, application of the third-party doctrine becomes unworkable due to the fact that the architecture of the Internet and choices made by application developers determine when an entity on the network is given data for its use (what we have called "architectural metadata"). Even when architectural metadata is identified, the question of whether the user made a knowing, voluntary conveyance of the information to myriad third parties remains.

In this Article, we have assiduously avoided discussing how the reasonable expectation of privacy should be calibrated and interpreted in an IP-based communications environment. But this issue is very much front and center for both the public and the judiciary. Indeed, in her concurrence in *Jones*,[425] Justice Sotomayor wrote:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., *Smith* [and] *Miller*. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[426]

The arguments made in this Article — namely that the architecture of the technology itself both collapses the content/non-content distinction and renders application of the third-party doctrine unworkable — nevertheless provide an evidentiary technical foundation that supports the privacy-based concerns raised by Justice Sotomayor. Whether or not courts and legislatures choose to engage with the privacy questions inevitably raised by the complexities of IP-based communications, the shaping influence of the factual technical terrain we have described upon surveillance law and policy cannot be avoided.

425. United States v. Jones, 132 S.Ct. 945 (2012).
426. *Id*. at 957 (citations omitted).