IT'S TOO COMPLICATED: THE TECHNOLOGICAL IMPLICATIONS OF IP-BASED COMMUNICATIONS ON CONTENT/NON-CONTENT DISTINCTIONS AND THE THIRD PARTY DOCTRINE

Steven M. Bellovin,[1] *Matt Blaze,*[2] *Susan Landau,*[3] *and Stephanie K. Pell*[4]

For more than forty years, electronic surveillance law in the United States developed under constitutional and statutory regimes that, given the technology of the day, distinguished content from metadata with ease and certainty. The stability of these legal regimes and the distinctions they facilitated was enabled by the relative stability of these types of data in the traditional telephone network and their obviousness to users. But what happens to these legal frameworks when they confront the Internet? The Internet's complex architecture creates a communication environment where any given individual unit of data may change its status—from content to non-content or visa-versa—as it progresses Internet's layered network stack while traveling 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 IP-based communications environment, the once-stable legal distinction between content and non-content has steadily eroded to the point of collapse, destroying in its wake any meaningful application of the third party doctrine. Simply put, the world of *Katz* and *Smith* and 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

[1] 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.

[2] Associate Professor of Computer and Information Science, University of Pennsylvania.

[3] Professor of Cybersecurity Policy, Worcester Polytechnic Institute.

[4] Assistant Professor and Cyber Ethics Fellow, West Point, Army Cyber Institute & Department of English & Philosophy; Affiliate Scholar, Stanford 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 who provided useful comments on an earlier draft of this paper.

This is an unedited draft. The final version will appear in:
30 **Harvard Journal of Law and Technology** **(Fall 2016)**

communications environment. Building on a deep technical analysis of the Internet architecture, we define new terms, *communicative content*, *architectural content*, and *architectural metadata*, that better reflect the structure of the Internet, and use them to explain why and how we now find ourselves bereft of the once reliable support these foundational legal structures provided. Ultimately, we demonstrate the urgent need for development of new rules and principles capable of regulating law enforcement access to IP-based communications data.

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 *metadata* associated with it. The legal framework for surveillance law was developed largely in the context of the of the mid-twentieth century telephone system, which itself treated content and metadata as relatively 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 Internet'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 visa-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, 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 application of the third party doctrine. Simply put, the world of *Katz*[5] and *Smith*[6] and 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 development of new rules and principles capable of regulating law enforcement access to Internet communications data.

A dependence on the *physical* separation of metadata from message is recognized in *Ex parte Jackson.*[7] In 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.[8] The physical structure of the letter or package allowed for a clear constitutional rule that separates inside content from outside, publically exposed, address information.

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

[5] *Katz v. United States*, 389 U.S. 347 (1967).

[6] *Smith v. Maryland*, 442 U.S. 735 (1979).

[7] *Ex parte Jackson*, 96 U.S. 727 (1878).

[8] Ex Parte Jackson (cite)

collection was necessary.[9] 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*. What is the status of the dialed digits a caller discloses to a third party—the telephone company—when placing a call? In *Smith v. Maryland*, the Court found that government collection of dialed digits with a pen register device did not constitute a search. 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 *Katz*, dialed digits themselves did not comprise communications content.

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 the Wiretap Act, providing the strong protections for communications content that exist today, then followed with the Pen/Trap statute, providing more minimal 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, not very complex.[10] 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 long-distance service than that was provided by AT&T, which was the only network carrier at the time (and thus enjoyed a ubiquitous footprint grounded in a national monopoly[11]). Until the consent decree and subsequent breakup of AT&T,[12] 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. This dialing structure meant that *the dialed numbers were now the content of a call*. By the late 1980s, telephones began conveying not just dialing information, but content of various sorts (e.g., bank account and prescription numbers). The legal distinctions between content and non-content established by *Katz* and were beginning 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 high-quality voice transmission; this constrained the possible design space. Despite a century of high-quality

[9] *Id*.

[10] The Electronic Communications Privacy Act of 1986 (PL 99-508) did deal with wire transmissions, including pagers, and restrictions on access to stored electronic communications. Its sections on Pen/Trap, however, were exclusively focused on the telephony world.

[11] *See* Philip L. Cantelon, *History of MCI, 1968-1988 : The Early Years*, 1993, at 291.

[12] 552 F. Supp. 131 (D. D.C. 1982).

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.[13]

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.[14] Flexibility was inherent in the system design, with "the choice of any individual network technology … 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.'"[15] 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.[16] 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—a complexity that 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' job in 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*. Via 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. Others have questioned how to apply current legal definitions of content and non-content to information such as URLs.[17] This article looks at the same issues but through a very different lens. Our vantage point is 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 or construct new analogies to the Katz/Smith distinctions that are instead calibrated for an IP-based communications environment.

At the time of *Smith*, the phone network connected people around the world, but its user

[13] See Part II.B and III.A for more detail on this issue.

[14] Barry M. Leiner, Vincent G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," ACM SIGCOMM COMPUTER COMMUNICATION REVIEW, Vol. 39, No. 5 (October 2009), at 24.

[15] Ibid.

[16] 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): 277-288.

[17] *See supra* Part II.B.

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. We introduce the concept of *architectural content* to denote the *unexamined* transportation of a unit of data between two given points in the network.[18] 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. 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.[19] 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 and metadata have become untenable in an IP-based communications environment.[20]

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.[21] 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 it when collected in real-time or compelled as stored data. Content (what we call "communicative content", as defined in the Wiretap Act) can also be inferred indirectly, e.g., from ad networks. Finally, we examine the case of mapping services, which provides an example of how the information conveyed to the mapping provider is dependent on the architecture of the service and is 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" (per *Smith*) is, at best, a legal fiction.

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

[18] There is a complementary concept, *architectural metadata*, but we defer discussing it until we cover the necessary technical background.

[19] *See infra* Part III.C for a fuller discussion of these terms.

[20] We note that just because a particular piece of data may be architectural content does not, in and of itself, determine whether or not the data is afforded Fourth Amendment protections.

[21] This fact has been observed by others as well, e.g., "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." In Ross Anderson and Stephen Murdoch, "What's Next After Anonymity?," in *Sixteenth Annual Workshop on Security Protocols*, Cambridge UK, April 16-18, 2008, at 3.

communications environment:

1.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;

2. The application of traditional content/non-content distinctions leads to results that make no logical sense;

3. The concept of metadata as a category of communication information that is wholly distinguishable from communications content is outdated; and

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

These conclusions suggest that courts will find it more and more 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. In this all-encompassing networked environment, notification of a communication may be the entirety of the communication—the metadata and the message are one in 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.

Big Data collection and the ready availability of personal data — peoples' GPS locations, Facebook likes,[22] 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

[22] Social graphs, likes, etc., can be quite revelatory of individual's characteristics, even when these are not explicitly revealed; see, e.g., C. Jernigan and B. Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation," *First Monday*, vol. 14, no. 10, 2009.

effort to regulate law enforcement access to location data.[23]

Notwithstanding the fact that certain debates about law enforcement access standards for metadata have now 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. According to the Director of the FBI, these various new encryption tools are causing law enforcement to "Go Dark." More specifically, under certain circumstances, law enforcement will no longer enjoy the ready and easy access to the plain text of written text 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.[24]

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—are not the subject of this article. It is clear, however, that in this new 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,[25] will become even more important to law enforcement investigations. We do not argue for the prevention of law enforcement access to this and other rich, revelatory metadata. However, understanding the limitations and, in many cases, the inapplicability of the current legal framework (content/ non-content distinction and third party rule) 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 application of third party doctrine writ large. 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.[26]

[23] *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 the 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).

[24] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark, Susan Landau, "Going Bright: Wiretapping without Weakening Communications Infrastructure," IEEE SECURITY AND PRIVACY, Vol. 11, No. 1 (Jan./Feb. 2013), pp. 62-72, and Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY, Vol. 12, Issue 1 (2014). Also see Jennifer Lynch, "New FBI Documents Provide Details on Government's Surveillance Spyware," Electronic Frontier Foundation (April 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government, which describes an FBI software package that uses hacking tools for investigations.

[25] *See supra* Part IV E (cite to ambient noise example).

[26] 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, footnote 5 (2009*)* ("A list of every article or book that has criticized the doctrine would make . . . the world's longest law review footnote.").

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.[27] 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.[28,29] Finally, we do not evaluate[30] 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.

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, including 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.

II. Legal Background and Analysis

[27] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. § 1801 et seq (2008)).

[28] *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); 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 (2012) (proposing model legislation for law enforcement access to location data).

[29] Although this article does discuss mapping services, our focus is on the very different behaviors of very similar-appearing services. We do not address the more fundamental question of whether or not location services should always receive full Fourth Amendment protection.

[30] *See* e.g., Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech L. Rev. 3.

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. 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. Taken in its strongest expression, this rule affords no Fourth Amendment protection to information revealed to a third party. 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.[31]

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."[32] This interpretation suggests that the third party doctrine does not apply "where the third party is a mere conduit or bailee."[33] 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,*[34] 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*[35] and *Katz*[36]—established that the content

[31] *See* Matthew J. Tokson, *The Content/Envelop Distinction in Internet Law,* 50 William & Mary L. Rev. 2105, 2124-25 ("Determining whether different types of Internet communication information are content requires decoupling the question of content/ noncontent status from the question of whether the information is protected under *Smith*. . . . But conflating Smith's analysis of the content/noncontent 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.").

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

[33] *Id*. at 438.

[34] Smith v. Maryland, 442 U.S. 735 (1979).

[35] Berger v. New York, 388 U.S. 41 (1967).

[36] Katz v. United States, 389 U.S. 347 (1967). As Professor Stephen Henderson has observed, however, neither *Berger* or *Katz* involved law enforcement obtaining the content of the phone conversations from a third party telephone company. Henderson, *supra* note ** 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 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*)[37] and to the outside wall of a public telephone booth (*Katz*).[38] In response to the constitutional rule established in these cases, Congress, in 1968, passed Title III of the Omnibus Crime Control Act[39] (“Wiretap Act”), a statutory scheme intended to create uniform rules that would comply with the Fourth Amendment for government interception of “wire”[40] and “oral”[41] communications in criminal investigations.[42] 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.”[43]

Almost ten years after its enactment, the Supreme Court relied on Title III’s legislative history and statutory language to distinguish a Title III wiretap from a pen register device.[44] Specifically, in *New York Telephone Company,* the Court distinguished the Title III definition of an “intercept” (“the aural acquisition of the *contents* of any wire or oral communication through the use of any electronic, mechanical or other device”), from the operation of a pen register, which the Court characterized as “decoding 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 the information in a form to be interpreted by sight rather than by hearing.”[45] 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.” 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.” Simply put, “pen registers do not accomplish the ‘aural acquisition’ of anything” and there was “no congressional intent to subject pen registers to the requirements of Title III.”[46]

of telephone conversations is actually less certain than we assume it to be.” Henderson, *supra* note ** at 437, *citing* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 847–50 (2004).

[37] Berger v. New York, 388 U.S. 41 (1967).

[38] *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.

[39] Pub. L. No. 90-357, §§ 2510-2520, 82 Stat. 197, 211-225 (1968) (current version at 18 U.S.C. §§ 2510-2530 (2003)).

[40] *Id* at **

[41] *Id* at **

[42] *Id* at **

[43] 18 U.S.C. § 2510(8) (1964 & Supp. 1970) (amended 1986).

[44] United States v. New York Telephone Company, 434 U.S. 159 (1977).

[45] *Id*. at 167.

[46] *Id*. *Citing* S. Rep. No. 1097, 90th Cong., 2s Sess., 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.’”).

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.[47] 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 . . . .'"[48] 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") in 1986, when it passed the Electronic Communications Privacy Act ("ECPA").[49] What is now commonly known as the Pen/Trap statute[50] only applied,

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 instead of as DC pulses.

Prior to 1963, pen registers used by law enforcement monitored only the DC voltage on the target's phone line, and did not use or require access to the audio frequencies that carried call audio. But with the introduction of DTMF signaling, pen registers also had to monitor the same audio channel that carried call content in order to decode dialed digits. So it was not strictly technically correct to say in 1977 that "pen registers do not accomplish the 'aural acquisition' of anything," since in order to capture DTMF-encoded digits, the device must also have access to aural voice content.

For dialed digits sent to the telephone company for completing a call, this technical distinction may not be important in and of itself. However, there is another, more important difference between dial pulse signaling and DTMF that highlights the difficulty of distinguishing content from metadata. Dial pulse signaling can be used only to send dialed digits from the subscriber to the telephone company (this is because the DC current of a phone line is not conveyed past the telephone company's central office to the number called). It is thus never used to send call content another subscriber. But 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 (which are clearly "content") can be recorded by a pen register that is intended to collect only the digits sent to the telephone company.

[47] *Smith*, 442 U.S. at 738.

[48] *Id*. at 741.

[49] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). 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 (commonly referring to Title III ("Wiretapping and Electronic Surveillance") of the Omnibus Crime Control and

at that time, to “numbers dialed or otherwise transmitted” or “the originating number of an instrument or device.”[51] Although the Stored Communications Act (SCA), Title II of 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,[52] this Pen/Trap telephone-specific definition appears consistent with—indeed it carries forward—the legal content/non-content distinction suggested by the telephone network architecture in existence at the time of *Smith*.

With the passage of 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).[53] As David McPhie observes,, Congress “in an apparent effort to make clear the distinction between Title III and the pen register regulation schemes . . . modified Title III’s definition of ‘contents’ [by] eliminatin[g] the ‘identity of parties’ and mere ‘existence’ of communication” from its scope.[54] Indeed, the Senate Report appears to evince Congress’ intent to codify the Supreme Court’s analysis in *New York Telephone Company* and *Smith*[55]: “[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.’"[56] 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[57] includes “any

Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010))); Title II (“Stored Wire and Electronic Communications and Transactional Records Access”), commonly referred to as the Stored Communications Act (SCA), Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–1868 (codified as amended at 18 U.S.C. §§ 2701–2712 (2010)); and Title III (“Pen Registers and Trap and Trace Devices”), commonly referred to as the Pen/Trap Devices statute, Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–1873 (codified as amended at 18 U.S.C. §§ 3121–3127 (2010)).

[50] 18 U.S.C. §§ 3121–3127 (2010). 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 (2003) due to its incorporation of the probable cause standard, along with several other requirements that must be demonstrated to a judge (*see* U.S.C. §§ 2518 (1)-(4)(2010), the Pen/Trap statute permits law enforcement to acquire data under rather low, mere certification standard. Specifically law enforcement must only “certify” to a court the that information sought is “relevant to an ongoing criminal investigation.” 18 U.S.C. § 3121(b)(2) (2010).

[51] Title III of 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. . . .” 18 U.S.C. § 3127(3) (2000) (amended 2001). *See also* § 3127(4) (2000) (defining “trap and trace device” as that “which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted).

[52] Congress passed 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 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)).

[53] 18 U.S.C. § 2511 (2004).

[54] David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 Stan. Tech. L. Rev. 1, 10 (2005).

[55] *See id* at 10.

[56] *Id*. at 10, *quoting* S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3567.

[57] The data communications industry of 1986 was nothing like today’s Internet. The ARPAnet—the ancestor of

information concerning the substance, purport, or meaning of that communication."[58]

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.[59] 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."[60] As Beryl A. Howell, General Counsel for the Senate Judiciary 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."[61] 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

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 they 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. The presumption that mail left on a server for more than 180 days was abandoned was quite plausible; 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) (2010)).

[58] 18 U.S.C. § 2510(8) (2004). 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."

[59] 147 CONG. REC. S9402 (daily ed. Sept. 13, 2001)

[60] Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act,* 72 Geo. Wash. L. Rev, 1145, 1194 (2003-2004) *citing* the E-PRIVACY Act, S.2067, 105th Cong. (1998) ("propos[ing] changes in the pen register laws) and the Internet Security Act, S. 2403, 106th Cong. (2000) ("containing proposed changes to the pen register law). *Id*. at n. 327.

[61] Howell, *supra* note ** at 1194-95.

which device or process is attached or applied.'"[62]

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 type of information law enforcement was authorized to collect are, at best, less than clear. More specifically, the terms, "routing" and "addressing" were added, although the Administration refused to define them. This definitional vagueness raised concerns that those terms could be read to encompass content,,[63] which would require the government to obtain a Title III super warrant,[64] not a mere Pen/Trap order, to obtain these categories of information.[65] Recognizing potential situations where certain kinds of communications data might contain both content and non-content, DOJ "conceded that 'reasonable minds may differ as to whether, and at what stage, URL[66] information may be construed as content.'"[67]

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.[68] From DOJ's perspective, signaling information was broader than dialed numbers; it was to encompass "other kinds of non-content information used by a communication system to process communications."[69] But with respect to data related to cellular communications, the DOJ instructed 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."[70] Moreover, DOJ's 2005 Electronic Surveillance Manual notes

[62] Howell, *supra* note ** at 1197.

[63] After 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." Howell, *supra* note **, at 1198.

[64] *See supra* note **

[65] Howell, *supra* note ** at 1197.

[66] For an explanation of URLs—Uniform Resource Locators—*see infra* Part IIIIV.CB.

[67] Howell, *supra* note ** at 1197 *citing* Letter from Daniel A. Bryant, Assistant Attorney General, to Patrick J. Leahy, Chairman, Committee on the Judiciary (Nov. 29, 2001) (on file with The George Washington Law Review) (response to questions to Attorney General Ashcroft in letter dated Nov. 1, 2001) (answer to question number 5). 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.*

[68] *See* 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 instrument or facility from which a wire or electronic communication is transmitted"). "Signaling" is a well-recognized technical term in telephony; *see Engineering and Operations in the Bell System*, prepared by members of the technical staff and the Technical Publication Department, AT&T Bell Laboratories, R.F. Rey, technical editor, 2nd edition, 1983, Chapter 8. The term is not generally used on the Internet, except when describing telephony-like protocols. *See supra* discussion Part III (**)

[69] ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 46 (2005) [hereinafter 2005 ELECTRONIC SURVEILLANCE MANUAL], *available at* http://www.justice.gov/criminal/foia/docs/elec-surmanual.pdf (2005 ELECTRONIC SURVEILLANCE MANUAL.

[70] *Id.* (emphasis added). Similarly, the definition of "trap and trace" device, which originally included only "the originating number of an instrument or device" 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). 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

that the "scant legislative history" accompanying the PATRIOT Act indicates that the new definitions should apply to "all communications media."[71] Does 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.[72] Some of DOJ's guidance with respect to specific types of non-content information that can be collected under Pen/Trap authority is, we argue, incorrect—we will return to this issue *infra* Part III.

ECPA's amendments to the Wiretap Act's definition of content and the PATRIOT's Act's amendments to the Pen/Trap statute give us the most current legal definitions of content and non-content. These apply to IP-based communications of 2015. But Professor Orin Kerr, noting that the "Wiretap Act itself does not define 'contents' clearly,"[73] questions whether "there is a third category of information outside of 'contents' and 'dialing, routing, addressing, and signaling' information".[74] Kerr, who raises this question in the context of discussing whether "URLs that include search terms and other websurfing addresses can contain 'content,'"[75] 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 answered by the PATRIOT Act."[76] As we have previously, referenced, 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.

of unique identifying number], which identifies the source of a communication." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note ** at 46.

[71] 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note ** 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. at 47 *citing* H.R. 107-236 at 52-53.

"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*.

[72] In a different context, attorneys from DOJ's National Security Division and FBI's National Security Law Bureau told an Inspector General that "terms used to define metadata themselves lack standardized definitions and that applying them to rapidly changing technology can be difficult." 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, Office of the Inspector General, U.S. Department of Justice (May 2015) available at https://oig.justice.gov/reports/2015/o1505.pdf#page=1

[73] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Northwestern Univ. Law Rev. 607, 645 (2003).

[74] *Id*. at n. 186.

[75] *Id*. at 645-46. For a more in depth discussion of URLs, *see infra* Part IV.C.H

[76] *Id*. at 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. 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.”[77]

As limited, expansive or “unclear”[78] 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).”.[79]Are they even mutually exclusive terms?[80]

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.[81] 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.[82] 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 considered and treated legally as non-content rather than content?[83]

Kerr also recognizes the possibility that addressing or signaling information could be considered content in certain situations.[84] He argues that this “difficulty [is] latent in *Smith*:”[85]

> 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 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

[77] Tokson, *supra* note ** at 2126 *citing* 18 U.S.C. § 2510(8).

[78] Kerr, *supra* note ** at

[79] McPhie, *supra* note ** at 26.

[80] *Id*. at 26, *citing* Kerr *supra* note ** for the reference to “Senator Leahy’s criticism of the vagueness of the ‘addressing and signaling’ terms.” *Id*. at n. 55.

[81] *Id*. at 26. 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 Friewald 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.

[82] *Id*. at 26.

[83] *Id*. For a more indepth discussion of packet lengths and what they can reveal, *see* i*nfra* Part IV **.

[84] Kerr, *supra* note ** at 645-46.

[85] *Id*. at 646, n.190.

> 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.[86]

Both McPhie[87] and Kerr 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. Specifically, when a user types on his keyboard that results in his web surfing are these user commands: (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?[88]

To Distinguish and Categorize or Not?: That is the Question

Matthew Tokson also examines the complex legal and technical questions raised when applying the traditional content/non-content distinction to IP-based communications.[89] At the outset of Tokson's analysis, however, 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."[90] 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."[91] 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."[92] He believes that stronger

[86] *Id.*

[87] McPhie, *supra* note ** 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.").

[88] *Kerr*, supra note ** at 646; also *citing United States Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000) ("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'") *Id*. at n. 191.

[89] Tokson, *supra* note ** ("[W]e lack a robust conceptual framework for determining whether new forms of communications information, such as websurfing 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 would mean in terms of the Fourth Amendment and the ECPA—presents a complex legal and technical question.") *Id*. at 2124.

[90] *Id*. at 2112.

[91] *Id*. at 2105.

[92] *Id*. at 2105. In his examination of URLs, for example, Tokson cautions against trying to draw a legal

Internet privacy protections will come from recognizing the breadth of Internet communications data that should be classified as content under constitutional and statutory law.[93]

Recognizing the value of these and other[94] scholarly contributions to the effort of determining how to apply the content/non-content distinction to IP-based communications, 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 Stored Communications Act (SCA), Title II of ECPA, governs law enforcement access to data stored by specific kinds of third parties.[95] While the Wiretap Act requires the government to establish that there is "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense"[96] in order to collect the content communications in real-time, the SCA allows the government to compel disclosure of stored content communications under lower standards. Specifically law enforcement can compel stored content under what is often described as reasonable suspicion[97] standard or even a mere relevance showing.[98] The compelled disclosure of email content under standards lower than a Fourth Amendment "probable cause" showing has, however, been found unconstitutional under *United States v. Warshak*.[99] Specifically, *Warshak* holds that the Fourth Amendment protects the contents of email held by an ISP.[100] The court reasoned:

distinction between URLs that contain search terms, and therefore are easily identified as content, and those that do not. *Id* at 2135-2136. 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.

[93] *Id*. at 2124.

[94] *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 distinctions does not easily apply to location data).

[95] *See* 18 U.S.C. §§ 2101-2712(3) (2010).

[96] 18 U.S.C. § 2518(3)(a).

[97] *See* 18 U.S.C. § 2703(b)(B)(ii) (allowing law enforcement to compel communications content from ECPA-coverd third parties obtaining a Court Order finding that there are "specific and articulable facts" that the information sought is "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

[98] *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).

[99] 631 F.3d 266 (6th Cir. 2010).

[100] *Id*. at 282 ("We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his

> 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.[101] 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.[102]

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 office or a telephone company.[103] 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.”[104] 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.’"[105]

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.”[106] 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.

Put another way, what can a subscriber reasonably be excepted to discover or know about how various kind of third parties might be accessing and using that subscribers’ communications content? How might that discovery or knowledge affect the constitutional status of communications content? The fact that the ISP contractually reserved the right the access Warshak’s emails for certain purposes did not defeat Warshak’s reasonable expectation of

Internet Service Provider ("ISP") to turn over the contents of his emails.”).

[101] 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.

[102] *Id*. at 286 *citing* Jacobsen, 466 U.S. at 114; *Katz*, 389 U.S. at 353.

[103] *Id*.at 289 *citing* Patricia Bellia & Susan Freiwald, *Stored E-Mail,* 2008 U. Chi. Legal F. at 165 ("[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.").

[104] *Id*. at 286.

[105] *Id*. at 288.

[106] *Id*. at 287 *citing Warshak* I, 490 F.3d at 472-73 (*quoting* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

privacy.[107] 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 upon the content status of the communications data in question,[108] 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* and *Smith v. Maryland.*

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.[109]

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.").[110] 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*.[111] While the court asserted that one kind of content is more confidential and sensitive than another, it is equally important to note the *Warshak* court's focus on the documents in *Miller* as *voluntarily conveyed*

[107] *Id*. at 286. ("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. . . . [W]e 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.") (Internal citations omitted).

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

[109] *Miller*, 425 U.S at 443.

[110] *Warshak*, 631 F.3d at 287-88.

[111] *Id*. at 288.

for the bank's use.[112]

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*"[113]. In his examination of the reach and scope of the of the third party doctrine, 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."[114] 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*. As previously noted, the Sixth Circuit gave Fourth Amendment protection to email in the possession of an ISP, notwithstanding its use of algorithms to scan email content and its disclosure of that fact to subscribers.[115]

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."[116] In *Smith*, the phone numbers at issue were recorded by the phone company "for a variety of legitimate business purposes."[117] 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 telephone company."[118] 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

[112] *Id*. at 288.

[113] *Smith*, 442 U.S at 743-44 citing United States v. Miller*,* 425 U. S., at 442-444; Couch v. United States*,*409 U. S., at 335-336; United States v. White*,* 401 U. S., at 752 (plurality opinion); Hoffa v. United States*,* 385 U. S.293, 302 (1966); Lopez v. United States*,* 373 U. S. 427 (1963) (emphasis added).

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.

[114] Henderson, s*upra* note ** at 437.

[115] *Id*. at 438 *citing Warshak*, 631 F.ed at 286-87. Henderson cites a number cases where courts have recognized a reasonable expectation of privacy in something left with a bailee:

> 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). *Id*. at 437.

[116] *Miller,* 425 U.S. at 442.

[117] *Smith*, 442 U.S. at 743.

[118] *Warshak*, 631 F. 3d at 286. Henderson anticipated *Warshak's* holding and analogy to a pre-Internet age telephone company. Specifically, he argued 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).

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 such uses are *not*: the third party rule does not apply where the third party is a mere "intermediary."[119] 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. What if a third party converts, changes or manipulates the data entrusted to it in the "ordinary course of business[?]"[120] 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. Rather, he concludes, the scope of the doctrine is limited in its reach exclusively to data provided for a third party's *use*. 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*. 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).

For a conveyance to be made voluntarily, it must be done with intent or by design,[121] which, of course, presumes *knowledge* on the part of the consumer of that which is being conveyed. In both *Miller* and *Smith*, the Courts' discussion included facts showing that consumers knew that they were disclosing the information at issue to the respective third parties.[122] As we illustrate in Parts III and IV, however, the complexity of IP-mediated communications and services makes it difficult, if not impossible, for even the most technically

[119] *Id*. at 286-87.

[120] *Miller*, 425 U.S. at 442.

[121] *See* Webster's Dictionary definition of voluntary: "done by design or intention: intentional" available at http://www.merriam-webster.com/dictionary/voluntary.

[122] *Miller*, 425 U.S. at 442 (Respondent categorizes the check and deposit slips disclosed to the bank as "personal records") ; *Smith*, 442 U.S. at 743 ("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.").

sophisticated user to discover and comprehend the information she may be communicating[123] 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 (based on knowing, voluntary disclosures) continue to be a relevant, meaningful legal concept for regulating government access to data in an IP-based communications environment?[124]

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.

III. NETWORK ARCHITECTURES

Both the PSTN and the Internet are communications networks, but the Internet has a very different architecture than the Public Switched Telephone Network (PSTN), especially the PSTN that existed at the time *Smith* was decided. Despite basic similarities in purpose, the two networks have crucial differences in the way in which they operate and in the functions they are

[123] When considering whether a cell phone voluntarily shares cell phone location data, the Third Circuit reasoned:

> 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."

In the Matter of the Application of the United States of America for an Order Directing A Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317-18 (2010). But *see* United States v. Davis (No. 12-1928) --F.3d.—2015 (en banc) discussion, *infra* note **.

[124] Note: this discussion will be edited further with appropriate references to Graham (Fourth Circuit) when the court announces whether it will hear the case en banc and/or the Supreme Ct. grants or denies cert in Davis or some other cell site/ location data case. While the Third Circuit, *see supra* note **, notes a that cell phone user does not voluntarily share his location information with a cell phone provider (and thus does not apply the the third party doctrine to this non-voluntary disclosure), the Eleventh Circuit, in *Davis* (–F.3d—at **) when considering whether a user has a reasonable expectation of privacy in his location data holds "[t]he longstanding third-party doctrine plainly controls the disposition of the case." Specifically, in footnote 12, the court states that "[c]ell phone users voluntarily convey cell tower location information in the course of making and receiving calls on their cell phones." The court compares this situation to *Smith*, where "users could not complete their calls without necessarily exposing this information to the equipment of third party service providers." *Id.*at **. In it's reading of *Smith*, which is contrary to the reading and argument offered in this Article, the Eleventh Circuit incorrectly conflates the concept of information that is "necessarily" conveyed with the concept of a knowing, voluntary conveyance. Accordingly, Justice Jill Pryor, in her dissent, takes issue with several aspects of the majority's reading and application of *Smith* to the facts of the instant case. She opines that "[t]he extent of voluntariness of disclosure by a user is simply lower for cell site location data than for the telephone person dials. She concludes that Smith does not control that case and that "a comprehensive review of Supreme Court precedent reveals that the third-party doctrine may not be as all-encompassing as the majority seems to believer." *Id*. at **.

able to provide. These distinctions create a fundamental difference in kind. 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) 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 a data element. Indeed, the relevant facts and analysis can change in the course of data's transmission over the Internet. An analogue occurs with trains, where the front of a car becomes the back when the train changes direction.

As further illustrated in Part IV, whether a particular piece of information or data is content or non-content is often dependent on a number of different considerations. The architectural structure matters, but so does the location from which one looks. Note that by "location" we mean both which element—computer, router, network link—is monitored and at which "stack" layer the observation takes place.[125] There are other considerations as well, notably ownership of the observation point.[126] A router in someone'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

[125] The network stack is explained *infra*.

[126] 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 consideration of whether or not someone has a reasonable expectation of privacy in information *not* voluntarily given to a third party.

explain how DRAS (dialing, routing, addressing and signaling information) does not map well to the Internet and a rapidly innovating IP-based communications environment. Moreover, even in those circumstances where data can be fairly 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 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.[127]

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.[128]

In the phone network, all intelligence is *internal* to the network core. A phone switch receives signaling information such as tones or dial pulses to complete calls; the phone switches[129] are the only elements with any sophistication. 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, and rotary dial phones were almost completely electromechanical save for a few passive electronic components.[130] Rotary dial phones worked simply by interrupting the circuit at a rate of 10 pulses per second; it was even possible to dial phone calls by tapping the hook switch at

[127] For a detailed overview of how the PSTN worked back then, *see Rey,* fn XX, *supra.*

[128] The “protocol stack” refers to how different facets of a communication are accomplished. For more detail on the protocol stack see discussions in III. B, *infra*.

[129] Modern phone switches are special-purpose computers; in 1979, though, many electromechanical phone switches were still in use.

[130] *See* “An Improved Telephone Set”, A.H. Inglis and W.L. Tuffnell, *The Bell System Technical Journal* 30:2, April 1951, pp. 239-270, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6773313&filter%3DAND%28p_IS_Number%3A6773310%29. Phones of that design still worked in the 1979 phone network, and would likely still work today on classic twisted pair phone lines.

the proper rhythm.[131]

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-hook and listened for a dial tone. You then dialed the number and the phone system would then attempt to complete the call. This was the process understood by the justices in *Smith*.[132] Up to a point, it was correct.[133]

Given this design, most services had to be provided in the network as well, a requirement that happened to dovetail nicely with the business interests of the telephone companies. The only signaling mechanism a rotary dial phone had was one that 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, 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:[134]

> 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.*[135]

Indeed, on many phone switches, further circuit interruptions were perceived as requests for an operator to intervene in the call.[136]

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 *U.S. v. Dote*, for example, the court noted that:

[131] Personal experience by two of the authors of this paper. In 1980, one of us 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.

[132] For a description of how pen registers worked, *see* Victor S. Elgort, Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool, 60 Cornell L. Rev. 1028 (1975) Available at: http://scholarship.law.cornell.edu/clr/vol60/iss6/6, cited in *Smith* at 742. Elgort, quoting *United States v. Caplan*, 255 F. Supp. 805 (E.D. Mich. 1966), described a pen register’s function (fn 3) 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.” Though he 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.

[133] By 1979, a few more sophisticated services, such as 3-way calling, were being deployed in the PSTN.

[134] *See* Elgort, *id.,* at 1040.

[135] *Id* at **

[136] *Id at* **.

> 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.[137]

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.[138] These requests, and in particular the number to which a call is forwarded, are clearly the contents of a communication with the phone company.[139]

Another relevant feature was so-called "InWATS," an early form of today's 800 numbers.[140] 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 time of day.[141] In other words, even in 1979 the numbers dialed did not necessarily correspond to the number of the instrument that actually answered.[142]

The narrowness of the functionality provided by the telephone network guided the justices in *Smith.* 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 telephone network was designed to enable people to talk with one another. From the beginning, the Internet was based on a very different vision—a rather remarkable one. Begun in

[137] 371 F.2d 176, at **(need pin cite for quote) (7th Cir. 1966). (Emphasis in the original; internal citation omitted.)

[138] Personal experience of one of the authors; *also see* "Vertical Service Code", http://en.wikipedia.org/wiki/Vertical_service_code and *Rey,* FN xx, *supra*, at 57.

[139] In *In re Application of United States, supra* note **, *at 48*, the judge noted "Would 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".

[140] InWATS stood for "Inward Wide Area Telephone Service"; *see* US patent 4,191,680.

[141] *See Rey supra* note ** at **.

[142] Not all of these features were available on all phone switches--only the newer ESS (Electronic Switching Systems); *See* In the Matter of the Application of the United States of America for an Order Authorizing the Installation of a Pen Register, 610 F2d 1148, **(need pin cite) (1979). At that time, only a small percentage of phone switches were ESSs. *Id.* at **.

the late 1960s as a Defense Advanced Research Projects Administration (DARPA) project, the Internet was envisioned as a "globally interconnected set of computers through which everyone could quickly access data and programs from any site."[143]

Both networks are built upon the same physical infrastructures of semiconductors and fiber technology and often share the same physical infrastructure. The PSTN is a circuit-switched network in which each communication builds a circuit that it exclusively uses 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 an email, video, webpage, etc.

The Internet's architecture is quite distinct from that of the phone network. 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." While there are many factors contributing to the change in design, one major reason 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.

Even so, running a large ISP is anything but simple. Its most basic functionality—moving packets from here to there with reasonable reliability—is quite challenging. Difficult issues include traffic engineering,[144] routing,[145] and interconnection with other ISPs.[146] These issues are interesting and important, but as they are not relevant to the topic of this article, we provide no details here.

In the conventional description, computer network technology is organized as a *stack*. Each *layer* in the stack offers services to the layer immediately above it and requests services from the layer below it. The Internet Protocol (IP),[147] which is the *network layer*,[148] is concerned with getting packets from a source computer to a destination computer. IP hands packets to and

[143] Leiner *supra* note **at 23.***

[144] Traffic engineering is not just having enough high-speed links but ensuring that the load is balanced across the different links, with enough backup links and spare capacity to handle failures.

[145] Routing is a set of complex mechanisms by which routers learn the appropriate next hop to reach a given destination. The best analogy is to a road map, but a road map that is updated continuously to reflect network outages or policy changes on the other side of the world.

[146] As its name implies, the Internet is a network of networks. Interconnections must not only satisfy traffic engineering and routing constraints, but also implement, on a technical level, the contractual relationship between the ISPs. For complex reasons, the tools to do this are inherently quite crude and hard to use.

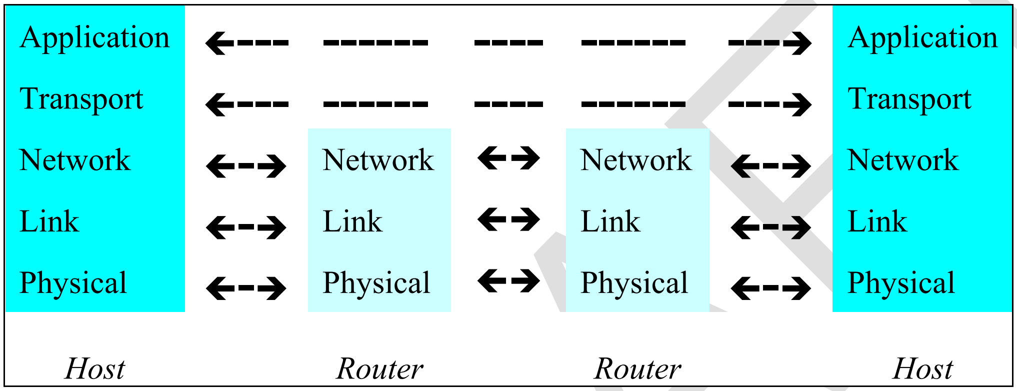
[147] *See* RFC 791 Internet Protocol. J. Postel. September 1981.

[148] The layer names come from the reference architecture of the Open Systems Interconnection standard (*see, e.g., Computer Networks, 5th Edition*, *Andrew S. Tanenbaum and David J. Wetherall*, Pearson, 2010, 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 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.

receives packets from the *link layer*. The transport layer—usually TCP (Transmission Control Protocol)[149]—turns the packets into a reliable stream for applications.[150]

Layers talk both "vertically" and "horizontally." As previously indicated, they communicate with the layers immediately above and below them in the stack. In addition, a layer on one device talks to the corresponding layer on some other device.[151] Knowing who owns the different devices is important for 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. [152]

A canonical depiction of the network stack as used on the Internet is shown below.[153]



Note that data in the application and transport layers are not processed by intermediate routers in the Internet.

All layers except the physical and application layers consist of a *header* and a *payload*.[154]

[149] *See* RFC 793 Transmission Control Protocol. J. Postel. September 1981.

[150] There are other, less frequently used transport protocols. The issues they present are largely similar, and we do not discuss them here.

[151] 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 is a property of the network layer—the request is routed through the adjacent layer, in this case transport.

[152] *See* discussion of architectural content *infra*. 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." "Websurfing and the Wiretap Act", *Volokh Conspiracy*, June 4, 2015, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/.

[153] The original stack model had seven layers; however, layers 5 and 6, the session and presentation layers, are not used in the Internet architecture.

[154] Arguably, there is a physical layer header for some media; this may be used to determine where a packet actually starts. On Ethernets, for example, there is a prologue of up to 64 bits. If the application layer has sublayers, there may be headers present there, too.

The header is the information processed by that layer; its payload is all of the higher layers. Consider an Ethernet packet (Ethernet is at the link layer). It has a 14-18 byte header; the remaining 1500 bytes of the packet are the network layer header, the transport layer header, and the application data.[155] We refer to the payload of a layer as its *architectural content*, explained *infra*.

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 differentWhile this part of the architecture seems innocuous enough, radio signals emitted from different sources at this layer are subtly different; this difference can be used to "fingerprint" and thus identify transmitters. [156] While there are potential statutory and Fourth Amendment issues raised by law enforcement collection of data at this layer, they 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 phones and the like. 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[157] that many computers make visible. (Note that "network" is used here in a narrow, technical sense to mean any network; the Internet derived its name from the fact that it is a network of networks.)

Many common networks can have multiple nodes connected to them. Accordingly, link layers frequently contain source and destination identifiers. As 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 MAC addresses (hardware address that uniquely identifies each node on a network) for these purposes is limited, since as noted they stay on-network. Under certain circumstances, e.g., 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, though under certain circumstances they may be sent elsewhere.[158] For Wi-Fi and Ethernet, the link layer identifiers are known as *MAC (Medium Access Control) addresses.*

Link layers are sometimes responsible for access control to and encryption of their networks;

[155] Strictly speaking, Ethernet packets also have a 4-byte trailer used for error detection.

[156] *See*, e.g., Cellular telephone anti-fraud system, U.S. patent 5448760 A, which describes how to prevent cellphone cloning by looking for the fingerprint of the authorized phone, or Bonne Rasmussen, Kasper; Capkun, S., "Implications of radio fingerprinting on the security of sensor networks," *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on* , vol., no., pp.331,340, 17-21 Sept. 2007.

[157] Technically, these are called SSIDs, service set identifiers.

[158] For a description of the problem, see RFC 4862, IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten, T. Jinmei. A solution is described in RFC 4941, Privacy Extensions for Stateless Address Autoconfiguration in IPv6. T. Narten, R. Draves, S. Krishnan. September 2007

the WPA2 encryption protocol for Wi-Fi is a well-known example. These mechanisms, too, may involve identifiers, 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.[159] Furthermore, under certain circumstances, Wi-Fi-connected nodes will broadcast the identifiers of networks they frequently connect to,[160] which can also identify a system.

IP, the network layer, is the lowest end-to-end layer.[161] The network layer and above are 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—that is, 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,[162] on the Internet—are set by the sender, examined by every router along the path,[163] and received by the ultimate destination. These routers are, in fact, parties to IP layer communications because they must examine these addresses. Furthermore, IP addresses were once effectively fixed:[164] a host received its IP address when it was first attached to its local network, and this address never changed.[165] 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.[166]

The transport layer, which is responsible for reliable delivery of data to applications, is strictly end-to-end. On the Internet, IP does not guarantee reliable delivery; TCP checks received

[159] Because the default MAC address of a WiFi interface is manufactured in to a device, the presence of a known MAC address on a network suggests that the device and hence its owner are present on a that network. This could, for example, be used to confirm that a suspect's phone was in a house, though only from quite near by; the range of WiFi is about 100 meters.

[160] *See* Dan Goodin, "Loose-lipped iPhones top the list of smartphones exploited by hacker", *Ars Technica*, March 16, 2012, http://arstechnica.com/apple/2012/03/loose-lipped-iphones-top-the-list-of-smartphones-exploited-by-hacker/ .

[161] "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 be no relation to the link-layer headers of the inbound packet.

[162] An IP address roughly corresponds to the street address of a building.

[163] 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. [[text here on routing protocols?]]

[164] IP addresses are reused and may not be unique across the Internet at any given time. *See* RFC 2101, IPv4 Address Behaviour Today, Rekhter, February (1997) B. Carpenter, J. Crowcroft, Y. *See* discussion of network address translators i*nfra*.

[165] This is slightly different for IPv6 (*see* RFC 2460, Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998); the differences are not relevant for our purposes.

[166] 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.

data for correctness, retransmits lost or damaged packets, etc. 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.[167] 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,[168] 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 system, these 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."[169] Fingerprinting can disclose how many computers are in a residence, what brands they are,[170] etc. 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.[171] From a law enforcement perspective, however, OS fingerprinting is an important part of the "reconnaissance" necessary before trying to penetrate a system.[172]

There are a number of deep architectural principles implicit in the Internet architecture. Most

[167] Well-known port numbers are assigned by IANA, the Internet Assigned Numbers Authority (http://www.iana.org), 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 from fn XX, *supra*, one can imagine that the mail room is always #25, the help desk is room #80, etc.

[168] *See* RFC 6335 Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number, M. Cotton, L. Eggert, J. Touch, M. Westerlund, S. Cheshire. August 2011.

[169] 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., "p0f v3: passive fingerprinter", Michael Zalewski, 2012, http://lcamtuf.coredump.cx/p0f3/README.

[170] There are other things, such as income level of the owners that can be learned (that stems from the fact that Macs are more expensive than Windows computers). This is not unrelated to the issues raised by *Kyllo v United States,* 533 U.S. 27 (2001), an issue we are not discussing in this paper.

[171] The IP layer also has such fields; however, since IP is not end-to-end, this information generally is given to third parties.

[172] The subject of lawfully authorized system penetrations is a very complex. Many aspects of it, including the need for a reconnaissance phase, are discussed in Bellovin et al., supra fn (**Part1, Lawful Hacking).

importantly, applications—the programs such as mailers, web browsers, remote disk connection and more that are most familiar to users—lie at the highest layer, and are the province of end hosts,[173] not of the network. The application layer is the one most familiar to users and of most interest to us.

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. As mentioned earlier, communications are always between peers at the same layer on different machines, or between adjacent layers on a single machine. An application talks only to another application, a transport layer talks only to another transport layer, etc. More specifically, the application layer on one computer never talks with, say, the network or link layers on another.

Application programs are provided by many sources. 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 differenceIf an ISP chooses to offer a mail service, the ISP's mail server behaves just like Google's or Yahoo's, running a full network stack with mail at the application level. ISP mail servers connect to the network in exactly the same way as any other mail server—the only salient[174] difference is that there may be a shorter path, i.e., one traversing fewer routers, to the captive offering than to a third party's offering. That is, the ISP's mail server behaves just like Google's or Yahoo's, running a full network stack with mail at the application level.is that there may be a shorter path, i.e., one traversing fewer routers, to the captive offering than to a third party's offering.[175] 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. Mail handling is discussed in more detail in Part IV, *infra*.

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.[176] Given the

[173] 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.

[174] 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 authentication; 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, though, users don't 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.

[175] The round-trip time affects the speed; effective bandwidth is related to the round trip packet time between the two machines. See the TCP bandwidth equation, given in Matthew Mathis, Jeffrey Semke, Jamshid Mahdavi, and Teunis Ott. "The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm". In: ACM SIGCOMM Computer Communication Review 27.3 (1997), pp. 67–82, http://dl.acm.org/citation.cfm?id=264023 at 68. "RTT' is the round trip time. As a result, the major independent mail providers use data centers all over the world, which in turn has given rise to some of the issues in *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir.).

[176] 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

state of the technology, two rules for interception, one for dialing and one for talking, made perfect sense. There were, apparently, no intermediate states to consider.[177] The interpretations and definitions, then, mimicked this understanding: "pen registers do not accomplish the 'aural acquisition' of anything."[178]

The same concepts can be expressed in modern computer science terminology. The phone network has a relatively simple "interface" or "service definition:"[179] 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.[180] Apart from the user-visible services such as email and Web browsing, there are complex network and programmatic interfaces.[181] A modern, 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."[182] We define its complement, *architectural metadata,* as information intended for the potential *use*[183] of a particular layer in the stack.[184] These two concepts are at the heart of our analysis.

Content as defined by structure or architecture—as opposed to substance or meaning—is not, however, an entirely new concept. Recall that 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 the umbra of these

simple: "Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy." *Smith* at 744. 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 was needed with MCI's early offerings, had not yet been raised; *see supra, note **.*

[177] Law enforcement had little, if any, need to know if or when a call was answered without knowing what the calling number was; if it did need to know, a simple device based on phone line voltages could have made the determination quite easily. A trap-and-trace device could have provided that information; in 1979, however, trap-and-trace was often a laborious, imperfect process; *see* 610 F2d 1148, *In the Matter of the Application of the United States of America for an Order Authorizing the Installation of a Pen Register* (1979) at 1152.

[178] United States v. New York Telephone, fn XX, *supra.*

[179] An *interface* is the definition of how two components communicate. Frequently, it specifies the *inputs*—what one component can send to another—and the *outputs*: what is returned in response to given inputs. In this case, of course, one of the "components" is the user of the telephone.

[180] This difference is a major reason why the Internet has so many more security problems. *See* William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994, at xi.

[181] The conceptual interface to TCP is given in RFC 793, fn XX, *supra*, starting at 44.

[182] 18 U.S.C. § 2510(8) (2004).

[183] The ordinary meaning of the word "use" is adequate. The technical meaning is that the protocol specification dictates what should be done with that information, i.e. how it should be processed, set, etc.

[184] Note that architectural metadata often include information not directly useful for identifying an endpoint, as described in the definition of a trap and trace device (pull cite).

protections.[185] 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 occurs in the processing of a TCP/IP packet in a router, per the discussion in III.B. The TCP payload, i.e. data being transmitted from application to application like the contents of an email message or web page, is content even per the current statutory definition of "substance, purport, or meaning." But in addition, the TCP header and payload are both *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. 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 its 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 payload are thus architectural content to IP; the application layer is architectural content to TCP.

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

D. Defining DRAS

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."[186] In the 2005 ELECTRONIC SURVEILLANCE manual, DOJ argued that the new terms added to the Pen/Trap statute extended the statute's reach to essentially all technologies.[187] The rationale for this interpretation is based on the scant legislative history found in a House Report[188] and does not appear to reflect deep technical analysis or understanding of the technical meaning of these terms. Accordingly, in this section we look to technical definitions used in academic and engineering literature describing the phone network and the Internet. These technical definitions illustrate how the terms dialing, routing, addressing, and signaling information do not map well to the Internet.

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."[189] It goes on to define "customer-line signaling" as "the interaction between

[185] Ex Parte Jackson, fn XX, *supra*.

[186] 18 U.S.C. § 3127(3) (2012).

[187] *See* discussion *supra* Part II A.

[188] *Id*.

[189] *See Engineering and Operations in the Bell System*, prepared by members of the technical staff and the

the customer and the switching system that serves the customer."[190] 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 (hopefully one hopes that someone will answer), etc."[191]

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.[192] The signaling messages include both the called number[193] and the "Calling Party Number."[194] Access to these messages is therefore 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.

"Addressing" is also straightforward. It is "the task of specifying to the network the destination of a call;"[195] an "address" is "a unique 10-digit number assigned to a main station,"[196] i.e., a phone number.

"Routing" is rather more complex in the phone network. The word "routing" is used in many different places in Signaling System 7. Many of these references, though, refer to the general networking concept of routing and have nothing to do with identifying the endpoints of a given call.[197] The use of interest has to do with determining which phone *actually* receives a call, as opposed to the number dialed.[198] Which phone receives the call and which number was dialed could differ for a number of reasons, including dialing an 800 number,[199] number busy or unanswered,[200] local number portability,[201] and call forwarding.[202]

We see, then, that for the phone network, the phrase "dialing, routing, addressing, and signaling" was intended to preserve traditional surveillance abilities (i.e. which phone receives the call), but in a more convenient form despite changes in technology.

Technical Publication Department, AT&T Bell Laboratories, R.F. Rey, technical editor, 2nd edition, 1983, Chapter 8.

[190] *Id.*

[191] *See Newton's Telecom Dictionary*, Harry Newton, with Steve Schoen, contributing editor, 27th Edition, 2013, Flatiron Books, 2013.

[192] *See Engineering and Operations*, fn XX, *supra*.

[193] Newton*,* fn XX, *supra*, definition of "Signaling System 7".

[194] *Id.*, definition of "signaling information fields".

[195] *See Engineering and Operations*, fn XX, *supra*, at 85.

[196] *Id.* at 115.

[197] See 18 USC § 3127 (4) (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, *infra.* The definition of pen register, found in 18 USC § 3127 (3), however, does not contain a purpose statement.

[198] Purpose as stated in 3127 4.

[199] *Tutorial on Signaling System 7 (SS7)*, Performance Technologies, 2003, at 4, available at http://www.eurecom.fr/~dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf

[200] *Id.*

[201] "How LNP Works", Number Portability Administration Center, available at https://www.npac.com/number-portability/how-lnp-works. 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.

[202] *Tutorial on Signaling System 7 (SS7)*,, fn XX, *supra*.

Most of these terms neither translate nor map well to the Internet domain. Dialing is an obvious mismatch. Signaling and routing are not a good match for the purpose of identifying endpoints to a communication under the Pen/Trap statute.[203] And addressing is far more complicated than it would appear at first glance.

Signaling has the same meaning as in the PSTN: the messages involved in setting up or tearing down a connection. Crucially though, on the Internet network routers are *not* involved in setting up a TCP connection. Per the discussion in part B of this section, *supra*, TCP connections are end-to-end, from client host to server host.[204] Indeed, the lack of involvement of the network in individual connections is a fundamental aspect of Internet architecture, and arguably the most important single decision in its design. (There are in fact some complexities, discussed *infra*, that make the end-to-end statement not always strictly correct.) 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.[205] As part of TCP, signaling information is architectural content to the IP layer. As discussed in Part II, *supra*, application of the Pen/Trap statute and its incorporated mere relevance standard to compel third parties to disclose information to law enforcement is based on the third party rule, which depends on the existence of a third party—but there are no third parties involved in Internet signaling.

"Routing" is problematic for a different reason. As noted, the term is used in several different ways in the telephone network; for law enforcement's purposes, the interesting one concerns the actual, as opposed to putative, destination of a particular call. In the sense that it has to calculate the path through the network to a given destination, the Internet also does such routing.[206] However, 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 connection.[207] There are routing messages, but they do not concern particular connections. This is a necessary consequence of the fundamental design principle stated earlier: 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 network policies of every ISP along the path.[208] While law enforcement investigators might be interested in

[203] *See supra* note **.

[204] TCP connections are established by the so-called "3-way handshake"; *see* RFC 793, *supra*.

[205] Strictly speaking, on the phone network "dialing" is a sequence of signaling messages. It is called out separately in the statute because it is user-visible. That is, *people* originate the dial message. The closest analog on the Internet, typing the name of another computer (perhaps in a URL or in an email address) does not generate any message traffic.

[206] "The path that transmitted information takes from the sending end system is known as a **route** or a **path** through the network" [emphasis in the original]. *Computer Networking: A Top-Down Approach*, Kurose and Ross, Addison-Wesley-Longman, 2001, at 3.

[207] 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* Bellovin, "Security problems in the TCP/IP protocol suite", *Computer Communication Review* 19:2 (1989) at 35) and network performance issues.

[208] How routing protocols work and how they interact with each other is probably the single most complex feature of the Internet.

collecting IP routing data[209] (e.g., for investigations regarding IP hijacking— routing IP packets to incorrect destinations by corrupting IP routing tables) collecting such information was not the identified purpose of the Pen/Trap statute.[210]

It would seem that "addressing" is very simply defined: in the Internet, it should mean an IP address. IP addresses are in the IP header of every packet, and are used by every router along the path from its source to its destination. The actual destination of a packet, though, is determined not just by its IP address but also by the port number. The port number, though, 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.

To a network engineer—and therefore to the rest of us—it is far from obvious that "service requested"—that is, the port number—is not part of the "address."[211] 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. Furthermore, although ISPs are not "given" TCP port numbers, they have in effect "taken" them. For example, some of the earliest dedicated IP routers[212] had the ability to filter—firewall—based in part on port numbers.[213] More strikingly, many ISPs use the NetFlow protocol to monitor load on their networks.[214] NetFlow records include not just port numbers but also the TCP header bits that are used in signaling messages.[215] It is not obvious why ISPs, whose primary concern is monitoring traffic levels for purposes of determining the levels of bandwidth needed, should care about what services are used by their customers.[216] Some ISPs do, however, monitor this data, which means that a third party is examining architectural content.

Furthermore, in some situations network providers do handle signaling information when they provide Network Address Translators (NAT).[217] NATs are used because the Internet has effectively run out of IP addresses.[218] Thus, most public Wi-Fi hotspots provide customers with

[209] *See, e.g.,* Vervier, Pierre-Antoine, Olivier Thonnard, and Marc Dacier. "Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks." *Proceedings of the Network and Distributed Systems Security Symposium* (2015).

[210] *See supra* note **,

[211] Indeed, one of the authors of this article explicitly advocated making the service part of the IP address; *see* RFC 1681, On Many Addresses per Host. S. Bellovin. August 1994.

[212] Before dedicated routers existed, ordinary computers with extra network interface cards were used instead.

[213] *See, e.g., Gateway System Manual*, cisco Systems, Inc., July 1988, http://archive.computerhistory.org/resources/access/text/2013/04/102721279-05-01-acc.pdf, at 10-5.

[214] *NetFlow Services Solutions Guide*, cisco, 2001, available at http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/netflow/nfwhite.html.

[215] *Id.*, 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; *see* RFC 793, *supra*, at 12 and 16.

[216] Recall that port numbers often indicate which services are being used. See discussion *infra*.

[217] RFC 3022, Traditional IP Network Address Translator (Traditional NAT). P. Srisuresh, K. Egevang. January 2001.

[218] Because it was clear in the early 1990s that the Internet would run out of IP addresses, 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.

"private IP addresses;"[219] 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 NAT box operation necessarily includes examination of and modification to various TCP header fields, including the port numbers and the TCP flags field.[220] 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.

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 Part IV, the disclosure to or possession of this information by third parties (i.e. those parties which are not the peer endpoints) is hardly known to most Internet users. This situation highlights the problem of applying the third party doctrine on the Internet when conveyances will *not* be knowing and voluntary for most users. 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.[221]

From this description of Internet functionality, it is clear that some elements of the Pen/Trap statute are difficult to apply. There are more network elements, with more complex service definitions. 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. Not only is it unclear which parties are involved in a communication and whether or not ordinary citizens are aware of the disclosure of information to third parties, in some cases metadata is intermingled with end-to-end data, making it hard to use our notion of architectural content as a guideline. In fact, some applications are sufficiently complex that their network behavior implies the content of communications or private data that is resident on a user's device.

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

[219] RFC 1918, Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. February 1996.

[220] In fact, in some circumstances a NAT box must examine and modify information that is indisputably content per the statutory definition.

[221] As is discussed in Part IV.XXB, email is usually—but not always—relayed via third parties.

distinctions erode or collapse entirely.

We start by considering email. In Subpart B, we will see that the addressing information in the protocol—the "From" in the email "envelope"—may be different from the "From" that the user sees within the message header, meaning the latter is architectural content, not address information. Next, in Subpart C, we examine URLs, "addresses" for web pages. URLs include a set of instructions of sites to visit. Determining which parts of URLs are content and which are non-content DRAS has proven to be a challenging endeavor for courts and scholars. In Subpart D, we look more deeply into what we are calling *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 Subpart E, we discuss a less direct, but quite revelatory, phenomenon: *DRAS from ad networks* that enables significant inferences about the user's activities.

In Subpart F, we examine the case of mapping services, which illustrates that whether information is conveyed to the mapping provider varies and is dependent on the architecture of the service—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're 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 interests of space and clarity, we do not present full-fledged analyses of any others; still, a brief look at a few is useful. A deeper analysis of them will appear in a Columbia University Computer Science Technical Report.[222]

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 the statutory definitions of content nor non-content;

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

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

[222] *See* CUCS-2016-XX.

statutory law.[223]

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) In the context of IP-based communications, 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) In the context of IP-based communications, application of the third party doctrine will turn on where in the network law enforcement compels access to the information.

We begin in Subpart 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 third-party rule.

A. Services and Architecture

Can we draw bright lines that distinguish between content and metadata in modern systems? The distinction is both legal and technical. Legal frameworks that rely on pre-Internet technological interpretations have become increasingly difficult to apply to many of today's applications.

Moreover, 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.

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. What is architectural metadata—the complement of architectural content—at one layer will be architectural content at another. 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 on the system—what may require legal process under a

[223] Location data, discussed briefly in Parts I and IV, a form of particularly revelatory metadata that is neither content nor non-content, is causing Congress and the courts to consider appropriate new statutory and constitutional privacy protections.

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 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.

An example is useful. Consider the different ways that an Internet-resident teleconferencing system used for internal corporate communications might work. No matter how it's 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.[224]

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 communication. Many other applications, such as those used for photography, mapping, and games, might, however, communicate with some entity on the network. Indeed, these may do so at unexpected times and in ways that are effectively invisible to—or even deliberately hidden from—their users.

Whether and how an application communicates over the network, and the extent to which it depends (if at all) 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

[224] 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.

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 are stored locally—that is, on media such as flash memory or magnetic disc drives that are directly connected to the local computer. Using the data on another computer[225] requires physically copying or transferring the media from one device to the other.

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. 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.[226]

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 users' data are 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,[227] and these may be implicitly or deliberately hidden from the user.[228]

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

[225] In this section, 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-screen tablet, or a mobile phone. For our purposes, all are computers, and we will not distinguish between them except when necessary.

[226] 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, 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.

[227] *See* the discussion of "actors", III.xx, *supra*.

[228] 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.

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 users disclosure of information to myriad third parties.[229] This fact undermines a meaningful application of the third party doctrine.

Moreover whether an application's data is properly considered content or metadata (and, indeed, whether that distinction is even meaningful technically) in modern applications has become a complex question, dictated partly by architectural choices, partly by arbitrary-seeming decisions made by implementers and system administrators,[230] 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.[231]

B. Email Headers and Envelopes

Despite the travails of snow, rain, heat, and gloom of night,[232] 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 (such as a change of address), the address to which the item is to be delivered.

Like physical mail and unlike phone calls, email is *asynchronous*; someone sends an email and sometime later, the recipient receives it. What is peculiar or, more accurately, invaluable about email delivery is that although the email may be sent to Alice@work, she may read it anywhere in the world through Internet access.

Delivery of email is a complicated technical process. We start with a simple explanation

[229] *See*, for example, Christopher Slogobin, "Transaction Surveillance by the Government," *Mississippi Law Journal*, Vol. 139, No. 75 (2005), at 193.

[230] 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.

[231] In the past, misunderstandings of the technology led to faulty judgments; see, e.g., *In re Application of United States*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

[232] Despite popular belief, "Neither 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.

followed by a legal analysis.

Briefly, mail to Alice@work goes to her employer's *inbound mail server*.[233] The simplest analogy is to general delivery at a post office. With it, 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 (e.g., her laptop, smart phone, etc.). Alice's address as it appears to the sender is simply Alice@work; 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,[234] and the multimedia extensions.[235] Mail transport uses SMTP, the Simple Mail Transfer Protocol[236] and a mail retrieval protocol.[237]

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
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
```

[233] 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*.

[234] *See* RFC 5322, Internet Message Format. P. Resnick, Ed. October 2008.

[235] 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.

[236] *See* RFC 5321, Simple Mail Transfer Protocol, J. Klensin. October 2008. The ancestor of this protocol goes back to at least 1980 and probably earlier; *see* RFC 772, Mail Transfer Protocol. S. Sluizer, J. Postel. September 1980.

[237] These include IMAP and POP.

```
221 yyy.com closing connection
```

Notice that the greyed-in part, the message, includes a "From" line. From: email addresses appear in two places, the SMTP envelope and the email message itself.[238] These two addresses need not be the same. We will discuss the consequences of that distinction in the legal analysis that follows this technical discussion.

The second important issue is that the "From:" in the email is not required to be the same as the SMTP "MAIL FROM." That is, the SMTP protocol does not put any requirements on the message's communicative content.[239] 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
```

Having different values in the envelope and header From: lines is by no means unusual.[240] 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 this scenario to occur. The email is sent via the house's local ISP mail server, but the From: line would refer to the business. The envelope line—typically ignored by almost all recipients—would be her residential account; the From:

[238] *See* Part III.C, *supra*.

[239] SMTP does impose certain requirements on the *syntax* of the message, as discussed in Part IV XX D *supra*.

[240] As noted *supra*, the envelope of a letter might say "Mr. President" while the inside is addressed to "Ike".

line in the header would show the work account.[241] *Thus the "From" in the header line is (architectural) content, not seen by any entity other than the sender and receiver.*[242]

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, such as Google and Yahoo, but there are 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 their *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.

Legal Analysis: 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.

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 that transfers mail, the email header line is architectural (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) 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—i.e. from which entity law enforcement seeks to compel the information. While the

[241] 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, available at http://www.slate.com/articles/technology/webhead/2002/03/email_impersonators.html.

[242] 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.

SMTP "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. 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; it is not based on the communication's meaning.* We therefore conclude that the SMTP "Mail From:" is addressing information under the Pen/Trap statute, but the email message "From:" is content per 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.[243] The two addresses would look the same to SMTP but not to the recipient.

Given the dual appearance of FROM, it is not surprising that DOJ overlooked the difference between "From:" in the SMTP protocol. 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."[244] Consistent with the inside/outside distinction recognized by the Court's structural analysis of a package in *Ex Parte Jackson*, the email message "From" is architectural content (like the inside of the package).

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.[245]

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

[243] *See* RFC 5322, fn XX, *supra*, at 11.
[244] 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* fn ***, at 39.
[245] *See In re Application of United States*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

collection of this information was lawful under a Pen/Trap order.[246] 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 mere "relevance" standard. 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.

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 their *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 dDetermineing 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. From a statutory perspective it is, at best, 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.[247] 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/Traps "relevance" standard.

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 that distinction has been done for a single, albeit extremely common email protocol.

If there is any truism about IP-mediated communications, it is that change is rapid and frequent. 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 III and use in the current analysis.

[246] The fact that the judge's conclusion is consistent with the information provided in the 2005 ELECTRONIC SURVEILLANCE does not mean, however, that the judge made the correct decision.

[247] At least with respect to cell phone location information, DOJ has taken the position that scant language in the PATRIOT Act House Report permits its direct collection (i.e. not from a third party) under Pen/Trap authority. See 2005 ELECTRONIC SURVEILLANCE MANUAL, supra note ** at 47-48. ("[T]he statutory text and legislative history strongly suggest that the pen/trap statute governs the collection of cell phone location information directly by law enforcement authorities.") Id. at 48. Whether DOJ believes that the Pen/Trap statute authorizes collection of other kinds of DRAS from entities that are not third parties is unclear..

C. The World Wide Web and URLs

URLs (Uniform Resource Locators)[248] are familiar to anyone who has ever used a web browser. Informally, they serve as the "addresses" of web pages. 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 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.[249] Accordingly, real-time collection of the path portion of the URL by law enforcement is *always* 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. The "http://" heading identifies it as a standard web URL that can be obtained via the HTTP protocol. Everything up to the next "/" – "en.wikipedia.org" – specifies the web server's host name. It is called the *authority* in URL parlance. The rest of the URL – "wiki/Metadata" – specifies the particular web page or service being requested from the server, and is called the *path*, in this case a Wikipedia article discussing the concept of metadata.

From a technical standpoint, the authority component appears simple at first blush appears simple. 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

[248] *See* RFC 3986 Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, R. Fielding, L. Masinter. January 2005.

[249] *See e.g.* In Re: Google Inc. Cookie Placement Consumer Privacy Litigation, _F.3d_ (Slip Opinion) (No. 13-4300) (3rd Cir. 2015). The court noted that:

> To 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 23 (internal citations omitted).

DRAS, squarely on the “non-content” end of the spectrum. (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).

The rest of the URL—the path—is where most of our trouble begins. In our example above, it 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 the HTTP protocol, 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.

It might appear, then, 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, e.g..:

```
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. Clearly, this is a communication from the user to the receiving web server, and we are still in “clearly content” territory (this is true from both architectural and communicative content perspective). But when we look at what happens next, things become 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. Appears to, but not quite.

In fact, the supposed Wikipedia URL returned by Google leads in reality to *another* Google web page, with a Google server in the authority component and a far more complex (and opaque) 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%2Fe
n.wikipedia.org%2Fwiki%2FMetadata&usg=AFQjCNE3JFDxIJ647wzHKykLvY
bekf5C0w
```

When the user clicks on this URL, her browser initially interacts not with the Wikipedia web server with which she expect 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. Observe that 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 (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.[250]

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

In the most straightforward case, a user browser communicates directly with a website. But connections are often far less straightforward. Sometimes users do not connect directly to a website, but instead use a *proxy server*; this is frequently the case, for example, when users are on a corporate network or behind certain kinds of network firewalls.

In any case, proxy or not, URLs are communicated to web servers via a communication protocol, called HTTP, the Hyper-Text Transfer Protocol.[251] (A related protocol, HTTPS, defines HTTP over encrypted communication sessions, and, for our set of concerns, is essentially similar.) 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.

HTTP sessions are complex; they not only convey the URL authority and path, but also consist of a *method*,[252] a version number, a 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, the header lines in a GET command include the query information; the header lines in a POST command do not (they are, instead, part of content). What this means is that query information in a GET command might not only be logged by the receiving web server,[253] but will be to be

[250] 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, 16 (1st Cir. 2003) at 15.

[251] RFC 7230, RFC 7231.

[252] *See* RFC 7231, fn XX, *supra*, at 24.

[253] For this reason, web developers are generally taught to avoid putting sensitive information, such as social security numbers or passwords, into query fields. *See* RFC 2616, Hypertext Transfer Protocol—HTTP/1.1. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. June 1999, at 152.

visible to, and *thus processed by*, any proxy servers used to create the connection. On the other hand, the query lines in a POST request are invisible to any proxy servers 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, 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 is appears to be a domain name, to be converted (either by the user's web browser or a proxy server) into an IP address via the DNS 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 that 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, there may be no new third parties involved with the authority component,[254] 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 service 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, they 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, then, depends on technical and economic decisions made by an outside party—*and even the site owner may not know these details.*

Proxy severs muddy the distinction between content and non-content even further. If a proxy server is used, the user's browser generally does not itself convert the domain name in the authority field into an IP address with DNS. Instead, it simply sends the entire URL to the proxy server, which performs the authority name resolution there. In other words, while in our simplest (non-proxy) cases the authority field is entirely non-content, in other configurations it is treated entirely as content. And none of this can be determined simply by examining the URL itself.

Legal analysis: It is a telling fact that 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.[255] While DOJ asserts that the PATRIOT Act gives

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

[255] *See* DOJ USA Book at 9-7.500 available at http://www.justice.gov/usam/usam-9-7000-electronic-surveillance.

law enforcement authority to collect non-content information associated with Internet communications, it DOJ acknowledges that the use of Pen/Trap to collect URLs raises "privacy and other concerns."[256] The Department is right to be cautious, as trying to assign a single rule, or even set of rules, to apply *all* portions of the URL could, among other things, 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, i.e. what the user is requesting from a website.[257] The path portion is also *architectural* content, in that it is a request from the user to another system for a resource. The authority—the hostname—is the recipient of the message; the path is itself the message.

The fact that the path portion of the URL is *always* communicative content,[258] however, makes at least a portion of the legal analysis 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,[259] however, there is not clear legal precedent on what access standard controls (e.g., 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.[260] As we

[256] *Id*.

[257] *See In re Goggle Cookie Placement Consumer Privacy Litigation*, __F.3d __(Nov. 10, 2015) 3rd Cir. at 26 ("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. path] are designed to communicate to the visited website which webpage content to send the user.").

[258] As Orin Kerr notes, the recent Third Circuit opinion *In re Google Cookie Placement Consumer Privacy Litigation* suggests that everything after the domain name in a URL is content. *See supra* note ** (currently footnote above this one). 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 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 Circuits Ruling (Nov. 19, 2015) available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/19/websurfing-and-the-wiretap-act-part-2-the-third-circuits-ruling/

[259] Web proxy servers generally log all transactions, including URLs retrieved.

[260] 631 F.3d at 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.") *Id*. 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 (subpoena) or reasonable suspicion

discuss 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. 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 possession a third party.[261] 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 only loses Fourth Amendment protections via the third party doctrine when it is provided to the third party for its *use*.[262]

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 sub-components, 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, back 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, it 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 only analyzed 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 the web servers that it hosts 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

standard (2703(d) order). *See* 18 USC § 2703(b)(B).

[261] *Id*. at 286.

[262] *See* discussion *supra* Part II.

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 will be 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.

Proxy severs further complicate the determination of what is content and what is metadata in a URL. As previously discussed, the path portion of the URL is always communicative content. The authority field, on the other hand, is not as stable. In simple cases where no proxy is used and where the web server serves only a single domain, the authority field is non-content, as the user's browser converts the domain name to an IP address. But if, for example, a proxy server is used, the user's browser generally does not itself convert the domain name in the authority field into an IP address with DNS. Instead, it sends the entire URL to the proxy server, which performs the authority name resolution. In this configuration, because the URL is transmitted in its entirety to the proxy server without being visible to lower levels of the protocol stack, the authority field is architectural content. Whether a URL is sent to a proxy server is not something that can be determined simply by examining the URL itself. Note that the proxy server itself may be a third party. Web servers that host multiple web domains are another example where the authority field is content, as discussed earlier.

As we noted at the beginning of this example, DOJ instructs prosecutors that the use of a Pen/Trap to collect URL information is prohibited without consulting with the Computer Crimes and Intellectual Property Section at Main Justice first. This admonition is not, however, a blanket prohibition. DOJ exempts from this policy the use of a trap and trace order "to . . . collec[t], at a web server . . . tracing information indicating the source of requests to view a particular URL."[263] While DOJ may be trying to prevent the collection of content with a Pen/Trap, 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, as we noted above, some web servers host multiple web sites sharing a single IP address. Which specific web site is being accessed is not itself derivable solely from the server's IP address; that information is transferred as part of the HTTP session. In that case, the authority field is *not* metadata to the network; 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.

[263] *See* DOJ USA Book at 9-7.500 available at http://www.justice.gov/usam/usam-9-7000-electronic-surveillance.

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, there was a structurally simple division when *Smith* was handed down: information was either a dialed number or a conversation, and there were no in-between categories. While such boundaries sometimes exist on the Internet, e.g., between the IP header and everything else, other situations in IP-based communications are much less clear-cut.

The layered model of the Internet means that different abstractions are 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 "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 is 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 Received:,[264] that are examined and generated by intermediate nodes. These lines were primarily intended for mail system operations: preventing forwarding loops, 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.[265] They sometimes have the sender's actual—envelope—address, which is fair game for a Pen/Trap order; however, this information is embedded in what would otherwise clearly be considered (communicative) content per the Wiretap Act. Nor is it simple to draw up lists of content versus metadata email headers; many mail systems have their own, private header fields; there is no way to know, a priori, how these 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.[266]

The technologies used by the government to implement interception of many Internet services can blur the layering distinctions even further.

Consider, for example, the problem of collecting (by interception of the network connection) 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*.[267] While the pen/trap statute might permit email

[264] *See* Part III.***IV B, *supra.*

[265] There are commercial services that map IP address to geographic location; they have varying degrees of accuracy.

[266] 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, Simple Mail Transfer Protocol. J. Klensin. October 2008, at 60); in practice, this does not present operational problems, but does complicate the legal analysis of the status of Received: lines

[267] We are assuming for the purposes of this example that the government cannot obtain this information from

address collection,[268] to actually extract the addresses 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. The monitoring device must then parse the HTML text to ascertain precisely what is being 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", can be difficult, fragile, and error-prone; it is also highly service provider-dependent and reliant on particular versions of the provider's software as well as the target user's configuration options.[269] Errors in interpretation here can result in both the unauthorized collection of information and the failure to capture information subject to authorized collection.[270] 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.[271] 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' (at 741 [emphasis in original]). The Court, in making the distinction, quoted from its earlier decision in *United States v New York Tel. Co.* (434 US 159, 167): " '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' " *(Smith v Maryland, supra,* at 741).[272]

S. Huang has suggested that a simple 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

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.

[268] The distinction between "envelope" and "header" is minimal or non-existent for Web-based mail systems.

[269] Even the intelligence community has found screen-scraping to be difficult technically. According to a spokesperson from the Office of the Director of National Intelligence, the NSA has experienced problems in exactly this situation; see https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed.

[270] 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* https://www.epic.org/privacy/carnivore/fisa.html; Context is given in the EPIC press release at https://www.epic.org/privacy/carnivore/5_02_release.html.

[271] People v. Bialostock, 80 N.Y.2d 738; 610 N.E.2d 374; 594 N.Y.S.2d 701 (1993).

[272] *Id*. at 744.

we have described as architectural content).[273] .This test, however, does not function properly results in all circumstances: email systems will misbehave if certain header lines are encrypted (or are otherwise malformed or not effectively present), but a mail message is content,[274] probably both architectural content and communicative content. Consistent, clear boundaries simply do not exist.[275]

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,[276] 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[277] 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

[273] In a student paper, Huang proposes a "provider-conscious encryption test."[273] Huang suggests that one way to determine if something is content or metadata is to see what would happen if it were encrypted, scrambled, or otherwise made unintelligible. If whatever mechanism—i.e., a lower layer of the network stack[273]—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.

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." Shane Huang, "Distinguishing Content from Metadata: The Provider-Conscious Encryption Test," student paper, 2014. On file with the authors.

In fact, the 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.

[274] *See Warshak*, 631 F.3d 266 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.").

[275] That headers could not be encrypted was known to the designers of S/MIME (*see* RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. B. Ramsdell, S. Turner. January 2010. Part III.C, *supra*). Their concern was mail system behavior, not legal issues.

[276] *See* David Fifield, Chang Lan, Ron Hynes, Percy Wegmann, and Vern Paxson, "Blocking-resistant communication through domain fronting," Proceedings on Privacy Enhancing Technologies, 2015, pp. 1-19.

[277] *See* RFC 3022, fn xx, *supra*.

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.

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 ("Siri" and "Okay Google", respectively). The online retailer Amazon recently announced an appliance[278] 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 pre-processed 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 to, for example, 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 itself (communicative) content as defined under the Wiretap Act.[279] But what might seem at first to be innocuous metadata in the transmissions between the device and the server, can, by itself, allow quite a bit to be inferred about the room

[278] "Amazon Echo", currently marketed at http://www.amazon.com/oc/echo/

[279] 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 *infra*). 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* discussion *supra* Part II.C.

audio and even what is being said *in the room*.

Researchers have developed practical techniques[280] that infer content from digitally encoded and transmitted audio entirely from metadata about the audio signal. Digital data is “compressed” to require less bandwidth,[281] 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.[282] Furthermore, other researchers have found that the communication encrypted, it is possible to identify who is speaking.[283] 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.[284] When speakers switch languages during a conversation, the act of doing so reveals a situational change (e.g., a change in "governing norms"),[285] which is also revealing of content.

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 application[286] proposed for a TV set-top-box ambient noise processing system, different ads are served depending on the type of activity detected in the room. If, for example, sounds associated with intimate romantic activity are detected, ads for appropriate products (getaway vacations, or perhaps contraceptives) will be displayed. 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

[280] *See* White, Andrew M., Austin R. Matthews, Kevin Z. Snow, and Fabian Monrose. "Phonotactic reconstruction of encrypted VoIP conversations: Hookt on fon-iks." In *Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 3-18. IEEE, 2011.

[281] 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.

[282] A phoneme is the smallest unit of speech that can be used to make one word different from another. http://www.merriam-webster.com/dictionary/phoneme. *See* White, *supra*.

[283] *See* Backes, Michael, Goran Doychev, Markus Dürmuth, and Boris Köpf. "Speaker recognition in encrypted voice streams." In *Computer Security–ESORICS 2010*, pp. 508-523. Springer Berlin Heidelberg, 2010.

[284] *See* Charles Wright, Lucas Ballard, Fabian Monrose, and Gerald Masson. Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob? In Proceedings of the 16th USENIX Security Symposium, Boston, August, 2007.

[285] Jan-Petter Blom and John J. Gumperz, “Social Meaning in Linguistic Structure: Code Switching in Norway,” in John Joseph Gumperz, and Dell H. Hymes (eds), Directions in Sociolinguistics: The Ethnography of Communication, Oxford: Basil Blackwell, 1986, at 407-434.

[286] US Patent Application 20120304206, November 29, 2012.

underlying content. Seemingly innocuous information, such as packet sizes, connection lengths, and web sites contacted are, at least statistically, revelatory of the 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.[287]

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. Per above, this information could enable law enforcement to infer what was occurring inside the home. How might a court apply *Kyllo*[288] 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.[289] 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."[290]

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 synonymous with *Kyllo*. Given the extremely revelatory, private information about goings-on inside the home, which can be inferred from DRAS information, however, a court should at least be given the opportunity to determine if the Pen/Trap relevance standard would be constitutionally sufficient for the collection of DRAS information. 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.[291]

F. Service Location Ambiguity

While the PSTN can accommodate modems, faxes, and 800 numbers, it is not an architecture

[287] *See* Lécuyer, Mathias, Guillaume Ducoffe, Francis Lan, Andrei Papancea, Theofilos Petsios, Riley Spahn, Augustin Chaintreau, and Roxana Geambasu. "XRay: Enhancing the Web's Transparency with Differential Correlation." Usenix Security 2014.

[288] Kyllo v. United States, 522 U.S. 27 (2001).

[289] *Id*. at 29-30.

[290] *Id*. at 34. (Internal citations omitted).

[291] Cite to Pen/Trap statute.

that facilitates such applications as 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 Subparts, we observed that at times it is essentially impossible for the user to determine whether information is shared with a third party. In this Subpart, 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 the estimated time of arrival is stored and computed. It could be done entirely on her phone, as it is on many stand-alone GPS devices, it could be done on cloud servers, or it could be done jointly. Users accessing cloud services do not understand where data resides. 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 between purely local and service-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, illustrates 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, depending on their architecture, these applications make very different uses of network-based services. 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 will 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 line of sight to sufficiently many[292] GPS satellites, the receiver can calculate its position on Earth to within several meters.

The use of GPS does not, by itself, emit any information to any third party. GPS receivers used by consumers (and now built in to almost all current mobile phone handsets) are passive

[292] There are currently approximately 32 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 http://www.gps.gov .

devices that do not themselves transmit any signals. A user's location (latitude, longitude and altitude) is calculated entirely in the receiver itself based on the received signals.[293]

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.

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[294] is commonly used in purpose-built GPS

[293] In addition to their internal GPS receivers, most modern smart phones can use the presence of nearby WiFi 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, *available at* http://gps.about.com/od/glossary/g/wifi_position.htm.. 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.

[294] Stand-alone maps are often used when there is no connectivity, e.g., a GPS system built into a car; when connectivity would be prohibitively expensive, e.g., when traveling in a foreign country; or when traveling in remote

receivers,[295] and can also be implemented on applications for smartphones and general-purpose computers.[296] 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 traffic) are either stored or calculated locally, with no network-based capability depended upon, no location data ever leaves the user's device.[297]

2. Fully connected architecture

Other mapping applications occupy the opposite architectural extreme, using "mapping as a service,"[298] 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)[299] 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 endpoints 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 (e.g., relying on the integrated GPS to update the displayed position, but not displaying map context when moving out of the last downloaded segment and not providing updated road condition information).

areas where there is no cellular coverage.

[295] For example, Garmin, a manufacturer of stand-alone GPS devices, offers models with real-time traffic data from both receive-only FM radio ("HD Digital Traffic") as well as two-way 3G/4G/LTE Internet service ("Live Traffic"). Whether the service is receive only or Internet based may not be functionally apparent to the end user. See http://www8.garmin.com/traffic/

[296] Mapping smartphone applications that can operate offline with pre-loaded maps are available from, e.g., OpenMaps.

[297] 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. 2437, 2493 (2014) (A "warrant is generally required before . . . a search, even when a cell phone is seized incident to arrest.").

[298] This is sometimes known as a "service-based architecture."

[299].The location might be calculated purely locally by GPS or by the WiFi technique described in fn XX, *supra*.

Thus even in the case of a pure mapping-as-a-service architecture, where there is a substantial amount of communication between 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 listing on bills as the type of information that puts consumers on notice that the numbers they dial will not remain secret.[300] Are there analogous real-world cues exist 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 itself. To the carrier, everything except the existence of the communication is clearly 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.

From a technical perspective, this can be understood as another illustration of the use of architectural content and architectural. In this case, some of the location information may have actually originated from a provider, thus blurring the boundary even further.[301]

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 larger 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 request 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

[300] *Smith*, 442 U.S. at 742-43, 748-49.
[301] *See* fn XX, *supra.*

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.

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 it 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 addresses. Because of the way it functions, law enforcement needs access to message payloads—which are architectural content and arguably communicative content—in order to obtain information that is available in the phone network via subpoenas or 2703(d) orders.

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 what 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 of the "free" services on the network 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 and fourth parties largely hidden from the user and 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 themselves quite revealing. For example, not only can they indicate which applications are on a user's device, but also when they are used.[302] These communications are transmitted silently, without the user explicitly initiating them. In no way can they be said to be voluntary.

While such pattern traffic 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 mere 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 Court held that if law enforcement wants to access information on a user's device, a warrant would generally be required.[303]

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.[304] In this instance the metadata—you have a message—is the message/content.[305] 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.[306] This application has middling value: the user is informed that there is an incoming missile, but not is alerted as to whether that missile is targeted nearby.

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

[302] There is a vast literature on "application protocol identification", *See, e.g.,* Charles Wright, Fabian Monrose, and Gerald Masson. On Inferring Application Protocol Behaviors in Encrypted Network Traffic. In Journal of Machine Learning Research (JMLR): Special issue on Machine Learning for Computer Security, volume 7, 2745-2769, 2006.

[303] *Riley*, 134 S.Ct at 2493,

[304] Alyssa Bereznak, "Developers Have a Yo Point with This Terrible New App," YAHOO! TECH, June 19, 2014.

[305] *See also* the discussion of phone ringing as a signal, *supra*.

[306] BBC News, "Yo app warns Israeli citizens of missile strike," July 1-, 2014.

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 fictional 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 final Part of this article, we discuss some general conclusions and effects stemming from the break down 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 DOJ and the courts with respect to use and authorization of the Pen/Trap statute.

V. Conclusions

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 the umbra of these protections to the outside, publically exposed layer of the package. In this scenario, the Court only had to account for a two-layer, stable architecture and was able to construct a constitutional rule that remains viable today. At the time of *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, as Sprint and MCI began to offer long distance services in 1979[307] (prior to the breakup of AT&T), they lacked direct access to phone switches;[308] as a result, their customers first needed to dial their account numbers and then enter the actual phone numbers desired. In other words, in the year *Smith* was decided, dialed numbers—metadata—were already being 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 (what we have called *architectural content*) in addition to the traditional form of content that is based on semantic meaning (what we have called *communicative content*), per the Wiretap Act. 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 is not the kind of thing most courts are capable of making on a daily basis (at least without a technologist on staff). 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.

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

[307] *See* Philip L. Cantelon, *History of MCI, 1968-1988: The Early Years*, 1993, at 270. [[check page]]

[308] *See* MFJ, fn XX, *supra*.

when architectural metadata is identified, the question of whether the user made a knowing, voluntary conveyance of the information to myriad third parties remains.

There are three inescapable conclusions that follow from the predicament we describe:

1. 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.

2. On the Internet, older rules lead to inconsistent, anomalous results.

3. The concept of metadata as a category of information that is wholly distinguishable from communications content and thus deserving of lower privacy protection is no longer tenable.

We discuss each of these in turn.

The rules are too difficult to apply.

Understanding where the boundary is between metadata and content is protocol and situation-specific. Simple guidelines such as "email addresses are metadata" are often false. A detailed understanding of the technical minutiae of Internet protocols is therefore required to begin the analysis. As we have seen in many cases (e.g., 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.

On the Internet, older rules lead to inconsistent, anomalous results.

Too often, the result of the situation-specific analysis described above is dependent on arbitrary actions of parties unrelated to a suspect or target of an investigation. Blurred boundaries show how even a structural rule cannot distinguish between content and non-content. Nevertheless, from a technical perspective a strict application of the principles and analysis of *Smith* leads to that conclusion. Law enforcement needs more stable, consistent results from its investigative processes and authorities.

The concept of "metadata" is outdated.

In the telephony era, dividing communications data into "content" and "dialing information" made sense. The 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 the former DRAS categories.

Similarly, there is information in the network- and link-layer headers that is given to third parties but is not DRAS data and thus not authorized for collection via a simple pen/trap order.[309] Before we can even start discussing what law enforcement access standards should apply to these categories of information, we must, at a minimum, define them. 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. 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.

Our final conclusion is simple. 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 plays out daily in our courts. 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 department's 2005 Electronic Surveillance Manual has an incorrect conclusion regarding email headers.[310] The SMTP address is addressing information within the context of the Pen/Trap statute; the email header FROM is not. The error, which has undoubtedly propagated to numerous law-enforcement agencies[311] and throughout the judicial system, will need to be corrected immediately. The new language should replace the second and third sentences in:

> 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 addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header.

[309] It is also unclear if *Smith* would apply, since conveyance of this information is almost always unknowing.

[310] 2005 ELECTRONIC MANUAL, *supra* fn **.

[311] *See*, for example, United States Marshals Service, *Policy Directives 15.1*, Non-Content Intercept under the Pen/Trap Statute, http://www.usmarshals.gov/foia/directives/technical_operations.pdf, at 1, where the same language as in the DOJ manual appears regarding email headers TO and FROM.

> 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.

with:

> Such information includes IP addresses and possibly port numbers.[312] While pen/trap orders can obtain the sender and recipient email addresses, they cannot authorize the interception of the content of a communication. This includes the information in the “To” and “From” of the email headers, words in the “subject line,” or the body of an e-mail.

It is important that judges also be informed of this change.

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 approaches for 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 arise, 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 nor content;

(2) As a matter of 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 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, this issue cannot be addressed in the abstract, but must be examined on a case-by-case basis.

(3) IP-based data that may technically fall under Pen/Trap DRAS 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

[312] Per the discussion in Part XX.Y, the status of port numbers is unclear.

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 only address particular elements of the overall analysis.

As we have already explained, because this article has only examined whether or not a third party actually participates in given Internet transaction or whether or not the user is aware of transactions with such third parties, we have *not* conducted a reasonable expectation of privacy analysis.

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

(1) Inquire about the type of information that will be collected with each application;

(2) Determine whether it is third-party DRAS;[313]

(3) If not third-party DRAS, ask the government if technology is available to collect only the DRAS;[314]

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

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.

IP-data Specific Recommendations:

1. <u>Collection of email headers:</u> Whether an email address is DRAS 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

[313] It is unclear whether or not port numbers are subject to third party collection.
[314] *See*18 U.S.C. 1321 C.

dialog, and not from the headers in email messages. Headers in email messages are clearly content.

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/From addresses—from a Web page requires a technology known as "screen-scraping". Screen-scraping is technically very challenging to implement correctly and can easily collect unrelated communications.[315] Moreover, since connections to the three major Web mail providers (Google, Microsoft, and Yahoo) are normally encrypted,[316] a simple wiretap or pen/trap tap will not pick up anything that is useful to law enforcement. For these reasons, law enforcement will need to serve a subpoena or 2703(d) Order on the provider who will, in most cases, have access to an unencrypted version of the email address.[317] This process, while perhaps not real-time Pen/Trap collection, both provides law enforcement with the information it seeks while avoiding the overcollection risk of, e.g., screen-scraping.[318]

2. 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, a Pen/Trap order should be legally sufficient (but see the discussion, *infra*, on advanced analyses). However, parts of the IP header are not DRAS, and thus not covered by the Pen/Trap statute.[319] This includes, per part 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.
3. Collection of port numbers: The TCP header is normally end-to-end, and thus not 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

[315] As noted, even the NSA has found this difficult; see fn XX, *supra*.

[316] All three have made statements about encryption: Google (http://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html), Yahoo (https://www.yahoo.com/tech/explained-how-tls-keeps-your-email-secure-88310223169.html), and Microsoft (https://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/). Google also supplies statistics on interprovider email encryption: https://www.google.com/transparencyreport/saferemail/.

[317] 18 USC § 2703 (d). A 2703(d) Order, a provision of 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 2703(d) orders on a provider.

[318] 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 https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed.

[319] 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." Per the discussion in Part III, information about the existence of an Internet communication is contained in the TCP header.

Section III.D, *supra*, ISPs often examine and use port numbers, the nominal Internet architecture notwithstanding. There is other information in the TCP header that is neither content, as defined in the Wiretap Act, nor information *given* to third parties. Law enforcement collection of this information would require further analysis.

4. Collection of URLs: The authority section of a URL is generally metadata. It will be translated into an IP address, which per our second guideline should be treated as third party DRAS. If the Web site is hosted by a service, many sites may have the same IP address; in such cases, though, the actual site desired will be given to a different third party: the hosting service itself.

   However the rest of the URL (the path and query sections) is typically not DRAS and should normally be considered content. The path can indicate, for example, what story on a newspaper site is being sought, or what article on Wikipedia is being read or edited.

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, *e.g.*, using IP address patterns to learn what apps are on a cell phone, or using packet sizes to ascertain 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. That is, 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

Clearly the only real way out of the current morass of "it's too complicated" is through new legislation. Unlike the specific suggestions we have for DOJ and judges handling current law, we have provided several philosophical points for policymakers, but we make no specific legislative proposals. Here are a few guiding principles:

1. The law should be solidly grounded in today's technical realities. Simply trying to extend the concept of "dialed phone number" to the Internet doesn't 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 serious set of products.
2. 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" analyses. Indeed, the momentum and analytical capacities

> driven by big data is changing even faster than technology in general.[320] 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.

In her concurrence in *Jones*,[321] 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,* 442 U. S., at 742; *United States v. Miller*, 425 U. S. 435, 443 (1976). 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.[322]

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. 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. In other words, 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.

[320] We note that the Web as a consumer phenomenon is more than 20 years old.

[321] *United States v. Jones*, 132 US 945 (2012).

[322] *Id*. at XX.