THE NATURE OF THE REVOLUTION: RETHINKING *RENO* TO REFLECT THE REALITY THAT THE INTERNET IS PART OF THE PHYSICAL WORLD

William C. Snyder and Ryan D. White[1]

ABSTRACT

When the government regulates the Internet, it is not regulating speech but rather a transportation system. The United States Supreme Court erred—albeit reasonably and understandably—in the early days of the Internet when it viewed the Internet as if it were solely a medium for speech. A more accurate paradigm for evaluating government regulation of the Internet is that of the interstate highway system and trucks moving payloads. Those are highly regulated activities. With this more technologically-informed understanding of this network of networks, the Court should view the Internet through the lens of affirmative grants of power such as the Commerce Clause or national security powers. Much like trucks on a highway might carry caustic acid or political tracts, the presence of expressions of human thoughts in some packets will rarely outweigh legitimate government interests in public safety and security. Viewed in this way, government regulation of the Internet generally should be upheld.

[1] William C. Snyder is a Teaching Professor of Law at Syracuse University's College of Law and the Maxwell School of Citizenship and Public Affairs. Ryan D. White will graduate in May 2018 with a J.D. from Syracuse University College of Law and a M.P.A. from the Maxwell School of Citizenship and Public Affairs. Shelby E. Mann, law student and research assistant to Professor Snyder, ably contributed to this article.

I. INTRODUCTION

Since the early days of the Internet, the Supreme Court of the United States has assumed that cyberspace is different from the physical world and has treated what happens there as speech. The Court is mistaken in both aspects. It is not outside our physical world, and it is not speech. They are using the wrong paradigm. The Internet, in particular, is a channel and an instrumentality of interstate commerce that moves packets of data from one place to another. The Court has rushed in without understanding "the

nature of the revolution" that is the "Cyber Age."[2]

First, this article explores the misunderstandings of the Supreme Court's approach to Internet regulation in two cases twenty years apart, *Reno v. American Civil Liberties Union*[3] and *Packingham v. North Carolina*.[4] Second, the article explains, from a technical standpoint, how cyberspace works and why that activity is not automatically speech. Third, it addresses a number of constitutional authorities that could apply to regulating cyberspace. Fourth, it concludes that the most appropriate authority to regulate a packet-switched network such as the Internet is the Commerce Clause. Fifth, it looks at how the government can accomplish this regulation and why it might want to.

II. THE SUPREME COURT MISUNDERSTOOD THE NATURE OF THE INTERNET, AND THEREFORE ITS PRECEDENTS ARE FUNDAMENTALLY FLAWED.

A. The Supreme Court was unfamiliar with the Internet and cyberspace when it decided Reno v. American Civil Liberties Union.

It was a different time in 1997, so much so that the Supreme Court spent the first four pages of its opinion in *Reno v. American Civil Liberties Union* describing what the Internet was.[5] Justice Stevens wrote about the Internet's brief history, email communications, and browsing the World Wide Web.[6] While these terms are common in American society today, they were novel twenty years ago. Only 22% of adults in the United States used the Internet in 1997.[7] Both the *New York Times*[8] and the *Washington Post*[9] newspapers posted their first online editions in

---

[2] Packingham v. North Carolina, 137 S.Ct. 1730, 1736 (2017) ("While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be.")

[3] 521 U.S. 844 (1997) [hereinafter *Reno*].

[4] 137 S.Ct. 1730 (2017).

[5] *See Reno*, 521 U.S. at 849–53 (for the Court's description of the Internet).

[6] *Id.*

[7] ERIC C. NEWBURGER, COMPUTER USE IN THE UNITED STATES: OCTOBER 1997 (U.S. Census Bureau 1999).

[8] *Our History,* THE NEW YORK TIMES, https://www.nytco.com/who-we-are/culture/our-history/#2000-1971-timeline.

[9] *The Washington Post*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/The-Washington-Post; e-mail from Terence McArdle, Customer Care,

1996, just the year before the Supreme Court decided *Reno v. American Civil Liberties Union*.

Once the Court set the stage with its description of the Internet and cyberspace,[10] it addressed the statute at issue in the case, Title V of the Telecommunications Act of 1996,[11] which was known as the Communications Decency Act ("CDA" or "the Act"). The "undeniable purpose" of the CDA was to prevent minors from gaining access to indecent material on the Internet.[12] Immediately after the law was enacted, 47 plaintiffs filed suit in two different cases.[13] The cases were consolidated and heard by a three judge panel in the Eastern District of Pennsylvania.[14] Through a direct appeal provision of the CDA, the case then went directly to the Supreme Court.[15]

The question before the Court was whether certain provisions of the CDA violated the First Amendment's protection of free speech.[16] The first challenged provision prohibited the knowing transmission of obscene or indecent messages to any recipient under 18 years of age.[17] The second prohibited the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age.[18] The numerous

---

Washington Post, to William C. Snyder (Dec. 28, 2017) (on file with author) ("Washingtonpost.com was launched in 1996.").

[10] The Internet is different than cyberspace. The scope of this article is limited to the Internet. Cyberspace is larger, and while the concepts may apply in the same manner, that is not necessarily the case. Cyberspace may evolve in ways we can not foresee, while the Internet, on the other hand, is fixed by the protocol controlling its operation—TCP/IP. Uses and applications of it will evolve and are unpredictable, but the technical system, the Internet, cannot. If we start communicating by spooky action at a distance (as Einstein called quantum entanglement), then it might still be cyberspace, but it would not be the Internet. The European Telecommunications Standards Institute defines the Internet as "computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange." EUROPEAN TELECOMM. STANDARDS INST., ETSI EG 202 057-4 V1.2.1: SPEECH PROCESSING, TRANSMISSION AND QUALITY ASPECTS (STQ); USER RELATED QOS PARAMETER DEFINITIONS AND MEASUREMENTS; PART 4: INTERNET ACCESS 9 (2008).

[11] Telecommunications Act of 1996, Pub. L. No. 104–104, § 501 et seq., 110 Stat. 56 (1996).

[12] *Reno*, 521 U.S. at 886 (O'Connor, J., concurring).

[13] *Id.* at 861.

[14] *Id*. at 861–62. *See generally* American Civil Liberties Union v Reno, 929 F. Supp. 824 (E.D. Pa. 1996) (for the consolidated action).

[15] *Reno*, 521 U.S. at 864.

[16] *Id.* at 849.

[17] *Id.* at 859. 47 U.S.C.A. § 223(a) (West, Westlaw through P.L. 115-140 approved 03/20/18).

[18] *Reno,* 521 U.S. at 859–60; 47 U.S.C.A. § 223(d).

individuals and organizations that challenged the law argued that through its attempt to protect children, the CDA criminalized what would otherwise be protected First Amendment speech for adults.[19]

Ultimately, the Court held that due to its vagueness and overbreadth, the CDA did, in fact, violate the First Amendment.[20] The opinion involved some limited analysis of the nature of the Internet but focused mainly on First Amendment law regarding obscene material and content-based speech protections.[21] At the conclusion of this case, the Court's stance was clear—activity on the Internet is, or at least can be, speech and must be afforded the pertinent constitutional protections.[22]

B. The Reno Court ruled on First Amendment speech grounds, but only because that is how the issue was framed in that case.

The only issue before the Court in *Reno* was the constitutionality of the CDA under the First and Fifth Amendments.[23] The specific facts of the case shaped that argument. At its very core, that statute and the case were about obscene content and minors.[24] The most obvious argument to be made, and perhaps the best one for the plaintiffs given the facts of that case, was First Amendment-based, because that was how courts had always handled obscene, "patently offensive," or "indecent" material.

During oral argument, Justice Scalia stated that "[t]his is a distinctive kind of first amendment statute."[25] The briefs at both the District Court and at the Supreme Court only raised those issues.[26] The First Amendment was the only issue that was

---

[19] Brief of Appellees, Reno v. ACLU, 521 U.S. 844 (1997) (No. 96-511), 1997 WL 74378, at *19; Plaintiff's Memorandum of Law in Support of a Motion for a Temporary Restraining Order and Preliminary Injunction, ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996) (No. 96-963), 1996 WL 33489551; Transcript of Oral Argument, Reno v. ACLU, 521 U.S. 844 (1997) (No. 96-511), 1997 WL 136253, at *34.

[20] *Reno*, 521 U.S. at 874 ("We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech.").

[21] *Id.* at 864. The Court affirmed the judgment "without reaching the Fifth Amendment issue."

[22] *Id.* at 870.

[23] *Id.* at 864.

[24] *See generally id.* at 849 (laying the framework for the Court's decision).

[25] Transcript of Oral Argument, *Reno*, 521 U.S. 844 (No. 96-511), 1997 WL 136253, at *50.

[26] *See*, *e.g.*, Brief for Appellees, *Reno*, 521 U.S. 844 (No. 96-511), 1997 WL 74378, at *21 (presenting arguments relating to speech).

discussed at oral argument.[27] And, ultimately, the Court decided the case on First Amendment grounds.[28]

That does not mean, however, that that was the only way the attorneys could have framed the issue or the only way that the Court could have reached a conclusion. Just because the Supreme Court viewed *that* Internet activity in *that* case as speech does not make it true in every other case, even if it was the correct analysis there. There is another way to address the regulation of activity on the Internet, one that is more comprehensive and accurate but that requires a more technical understanding of how the Internet functions. Neither the parties to the case nor the Supreme Court, perhaps naturally, had any understanding of that technical dynamic.

C. The Reno Court relied on stipulations of fact, and its analysis evinces a fundamental misunderstanding of the Internet.

The briefs in the case and the Court's opinion both demonstrate how new the Internet was in 1997. The descriptions provided indicate not just a lack of technical expertise but an even simpler misunderstanding of the impact the Internet would have. The opinion explained that "[t]he Internet is 'a unique and wholly new medium of worldwide human communication.'"[29] Moreover, the Court expressed the belief that "[t]aken together, these tools constitute a unique medium—known to its users as 'cyberspace'—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."[30] Finally, the Court concluded that: "No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web."[31]

The Supreme Court adopted most of these ideas from findings made by the District Court.[32] Those District Court findings were the result of a lengthy collection of stipulations made by the

---

[27] *See* Transcript of Oral Argument, *Reno*, 521 U.S. 844 (No. 96-511), 1997 WL 136253, at *33 (discussing the CDA's implications for freedom of speech).

[28] *Reno*, 521 U.S. at 849.

[29] *Id.* at 850 (citing ACLU v. Reno, 929 F. Supp. at 844).

[30] *Id*. at 851.

[31] *Id*. at 853 (quoting ACLU v. Reno, 929 F. Supp. at 838).

[32] *See id.* at 849 n.2 ("The Court made 410 findings, including 356 paragraphs of the parties' stipulation and 54 findings based on evidence received in open court).

parties.[33] These stipulations covered topics such as, "The Creation of the Internet and the Development of Cyberspace,"[34] "How Individuals Access the Internet,"[35] "Methods to Communicate Over the Internet,"[36] and "The World Wide Web."[37] In essence, the agreements made by the parties to the case before the District Court created the foundation on which the Justices of the Supreme Court relied in understanding the Internet.

There was little discussion of the technical nature of communication or data transfer on the Internet throughout the *Reno* litigation. All of the definitions agreed upon and explanations provided were generalizations about how the new phenomenon called the Internet worked.[38] The only limited discussion of a technical solution to the problems discussed in *Reno* concerned providers "tagging" their content or the feasibility of certain software programs to verify age before accessing pornographic websites.[39] As the next section of the article explains, there is now a more widespread understanding of the Internet—both from a technical standpoint as well as concerning its effects on society.

This observation is not a criticism of the brief writers in *Reno* or of the Supreme Court Justices. Their understanding and basic analysis were appropriate for attorneys of the era in which the case was litigated. Basic summaries of how people communicate and the implications of easily transferable information provided useful context. But that does not mean that those limited summaries are all we have to rely on in the present day, and today we have more. The Internet is not new or different from the physical world, and it is not ungovernable. While it is difficult for courts to do so, it is time for the Court to reconsider and overturn the erroneous precedent set in *Reno*. The technical understanding of the Internet is now widespread enough that we can have a proper tech-informed law regarding Internet regulation.

---

[33] *See ACLU v. Reno*, 929 F. Supp. at 830–49 ("Findings of fact are derived from the like-numbered paragraphs of a stipulation the parties filed with the court.").

[34] *Id.* at 830.

[35] *Id.* at 832.

[36] *Id.* at 834.

[37] *Id*. at 836.

[38] *See id.* at 830–49 (containing no citation to or acknowledgement of a well-known technologist or an Internet pioneer who participated in the preparation of the stipulations).

[39] *Reno*, 521 U.S. at 845, 847–48.

D. By Packingham v. North Carolina, the Supreme Court was more aware of what it did not "appreciate yet" about the Internet.

Twenty years after it decided *Reno*, the Supreme Court returned to the issue of regulating cyberspace in *Packingham v. North Carolina*.[40] Yet again, the facts of the case led to the Court relying on First Amendment speech protections to decide the case.[41] Indeed, the Petition for a Writ of Certiorari framed the only issue as "Whether, under this Court's First Amendment precedents . . . "[42] This time, however, the Justices acknowledged their own limitations in this highly technical subject.[43]

The question before the Court was whether a North Carolina statute prohibiting registered sex offenders from accessing certain websites, including major social media sites such as Facebook, violated the First Amendment.[44] The petitioner in the case, Lester Gerard Packingham, was a registered sex offender as a result of a 2002 incident with a minor for which he pleaded guilty.[45] In 2010, Packingham excitedly posted on Facebook after having a ticket dismissed in traffic court.[46] A local police officer was monitoring social media sites for violations of the state statute, and Packingham was ultimately convicted.[47]

The court relied heavily on *Reno* in deciding that the Internet is a crucial space in the marketplace of ideas.[48] Again, the Court decided that although the government interest was legitimate, the law was simply too broad.[49]

The Court was more informed than it was when it decided *Reno*. Or, at least, it was more self-aware about how limited its expertise

---

[40] *Packingham*, 137 S.Ct. at 1735.

[41] *Id*. at 1733.

[42] North Carolina v. Packingham, 368 N.C. 380 (N.C. 2015), *petition for cert. filed*, 2016 WL 1129388, at *1 (U.S. Mar. 21, 2016) (No. 15-1194).

[43] *See Packingham,* 137 S.Ct. at 1736 ("The forces and directions of the Inter net are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow.").

[44] *Id.* at 1733.

[45] *Id*. at 1734.

[46] *Id*.

[47] *Id*.

[48] *See id*. at 1736–37 (describing social media as a "means for access to the world of ideas").

[49] *See Packingham,* 137 S.Ct. at 1737 ("In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights.")

was. Justice Kennedy, writing for the majority, explained that "[t]his case is one of the first this Court has taken to address the relationship between the First Amendment and the modern Internet. As a result, the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium."[50]

Justice Alito wrote a lengthy concurrence in which he was joined by Chief Justice Roberts and Justice Thomas. The concurrence stated that:

> The Court is correct that we should be cautious in applying our free speech precedents to the Internet. Cyberspace is different from the physical world, and if it is true, as the Court believes, that "we cannot appreciate yet" the "full dimensions and vast potential" of "the Cyber Age," we should proceed circumspectly, taking one step at a time. It is regrettable that the Court has not heeded its own admonition of caution.[51]

The Court acknowledged the dangers of diving head first into Internet regulation but again relied on the logic set forth in *Reno* without obtaining any true technical understanding of how the Internet really works. Justice Alito's statement that "Cyberspace is different from the physical world"[52] is *dicta*, but it evinces a fundamental misunderstanding. The Internet is a part of the physical world, and most of what happens there is not speech.[53]

E. As late as 2010, justices did not understand that data travels over networks.

In *City of Ontario v. Quon*,[54] a 2010 case concerning a government employer's right to read text messages sent and received on a pager the employer owned, United States Supreme Court justices displayed no knowledge that digital information travels from one device to another through a network of computers.[55] The following exchange during oral argument illustrates their level of understanding.

---

[50] *Id.* at 1736.

[51] *Id.* at 1744 (Alito, J., concurring) (internal citations omitted).

[52] *Id.*

[53] *See infra* Part III for further discussion of the Internet.

[54] 560 U.S. 746 (2010).

[55] *Id.* at 750; Oral Argument, City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010) (No. 08-1332), 2010 WL 1540005, at *48–50 (demonstrating the Court's failure to recognize that there is more to the transmission of pager messages than a single transmission from sender to receiver).

CHIEF JUSTICE ROBERTS: Again, it depends upon their reasonable expectation. Do any of these other people know about Arch Wireless? Don't they just assume that once they send something to Quon, it's going to Quon?

[ATTORNEY][56]: That's—that is true. I mean, they expect --

CHIEF JUSTICE ROBERTS: Well, then they can't have a reasonable expectation of privacy based on the fact that their communication is routed through a communications company.

[ATTORNEY]: Well, they—they expect that some company, I'm sure, is going to have to be processing the delivery of this message. And -

CHIEF JUSTICE ROBERTS: Well, I didn't—I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing.

[ATTORNEY]: Well --

JUSTICE SCALIA: You mean it doesn't go right to the other thing?

[ATTORNEY]: It's—I mean, it's like with e-mails. When we send an e-mail, that goes through some e-mail provider, whether it be AOL or Yahoo. . . . It's going through some service provider, just like when we send a letter or package, it's going through—some provider is going to move that for us, until it gets to the recipient. . . . And—and like, when I get a piece of mail from somebody, I could do that as well, but that doesn't mean that the government gets to go to the Post Office and get my mail before I get it. I think—I think that, you know, certainly adds a little bit to the correspondence that dealt with --

* * *

CHIEF JUSTICE ROBERTS: So we have to assume for your argument to succeed that they know that this goes somewhere else and then it is processed and then it goes to Quon.

[ATTORNEY]: Yes, but I think in today's—I think in today's society that's—that's a reasonable assumption to make. One --

JUSTICE SCALIA: Yes, I didn't know.[57]

In fact, as explained *infra* at Section III, the processing of the data occurs at both ends and the service provider in between simply transports the data in the form of energy from one place to another.

---

[56] Here and hereinafter, "ATTORNEY" refers to Dieter Dammeier, Esq., representing respondents.

[57] Oral Argument. Quon, *City of Ontario*, 560 U.S. 746 (No. 08-1332), 2010 WL 1540005, at *48–50.

III. HOW THE INTERNET WORKS

"For all the breathless talk of the supreme placelessness of our new digital age, when you pull back the curtain, the networks of the Internet are as fixed in real, physical places as any railroad or telephone system ever was."[58]

There is no single, authoritative definition for cyberspace,[59] but for our purposes it includes the Internet and is at least all hardware, software, and data that can store, process, or move digital information from one computer to another.[60] Digital information is the reduction of any information to a binary number consisting of only the digits, zero and one—for example, 0110111.[61]

What moves in cyberspace and the Internet is radiation at different wavelengths.[62] Whether itis electrical, light, or even sound, it is all electromagnetic radiation.[63] Information is data

---

[58] ANDREW BLUM, TUBES: A JOURNEY TO THE CENTER OF THE INTERNET 9 (HarperCollins 2012).

[59] *See, e.g.*, The White House, *National Security Presidential Directive/NS PD–54* (Jan. 8, 2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf ("'cyberspace' means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"); *ISO/IEC 27032:2012(en): Information Technology—Security Techniques—Guidelines for Cybersecurity*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en ("The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks."); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS (U) 3 (2006) ("A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures"); *Cyber Definitions*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/cyber-definitions.html.

[60] *See NSPD–54*, *supra* note 59, at 3 ("'cyberspace' means the independent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries").

[61] *See, e.g.*, *Digital*, TECHTERMS, https://techterms.com/definition/digital ("Dig ital information is stored using a series of ones and zeros. Computers are digital machines because they can only read information as on or off—1 or 0. This method of computation, also known as the binary system, may seem rather simplistic, but can be used to represent incredible amounts of data.")

[62] MICHAEL G. RAYMER, THE SILICON WEB: PHYSICS FOR THE INTERNET AGE 414 (Taylor & Francis 2009).

[63] *See* J. Clerk Maxwell, *A Dynamical Theory of the Electromagnetic Field*, 155 PHIL. TRANS. R. SOC. LOND. 459, 499 (1865) ("The agreement of the results seems to show that light and magnetism are affections of the same substance, and that light is an electromagnetic disturbance propagated through the field according to electromagnetic laws.")

plus meaning.[64] Thus, information is made of data.[65] Data is a lack of uniformity.[66] Thus, "information is a distinction that makes a difference."[67] At our best, we have been able to record states of either positive or negative, on or off, burned or not burned—that is, a binary lack of uniformity or digital data.[68] For example, on Compact Discs, there are only two states, zero or one.[69] Operating in a base two-number system then, you can select a number and assign it to something such as a letter in our alphabet.[70] We could say, for example, that the first 26 values in a binary system represent the letters in our alphabet or the 33 letters in the Russian Cyrillic alphabet, or that the next so many values represent the numbers in base 10 to which we are accustomed, or in base 16, known as hexadecimal, or the symbols on a keyboard. Then, that data moves down a wire or cable or as radio waves through the air to a destination where a computer reassembles it into a format we comprehend.[71] That is, a computer takes the numbers and assigns letters, pixels in a graphic, etc. to positions on a screen.

The Internet is a network of networks.[72] That is, computers, which are broadly defined as things that can run software or store or move digital information,[73] are connected or "networked" together and those networks are connected. The Internet itself is a collection of many, many interconnected networks.[74] "The networks that compose the Internet share a common architecture

---

[64] LUCIANO FLORIDI, INFORMATION: A VERY SHORT INTRODUCTION 20 (Oxford Univ. Press 2010). ("Over the past decades, it has become common to adopt a General Definition of Information (GDI) in terms of data + meaning.").

[65] *Id.*; *Data, Data Everywhere*, THE ECONOMIST (Feb. 25, 2010), https://www.economist.com/node/15557443.

[66] FLORIDI, *supra* note 64, at 23.

[67] *Id. See also* UNDERSTANDING INFORMATION: FROM THE BIG BANG TO BIG DATA 12 (Alfons J. Schuster ed., 2017) ("[T]his lack of uniformity actually is what we call data.").

[68] UNDERSTANDING INFORMATION, *supra* note 67, at 12.

[69] *Digital*, *supra* note 61.

[70] *See id.* (explaining the capabilities of such a system).

[71] *See* RAYMER, *supra* note 62, at 16 (discussing the "delicate, tenuous, inter connected" information network).

[72] NAT'L RESEARCH COUNCIL ET AL., THE INTERNET'S COMING OF AGE 3 (National Academies Press 2001) [hereinafter INTERNET'S COMING OF AGE].

[73] 18 U.S.C.A. § 1030(e)(1) (West, Westlaw through P.L. 115-140 approved 03/20/18).

[74] *See, e.g.*, Code.org, *What is the Internet?* YOUTUBE (June 27, 2016), https://www.youtube.com/watch?time_continue=124&v=Dxcc6ycZ73M ("The Internet is made up of an incredibly large number of independently operated networks.").

(how the components of the networks interrelate) and protocols (standards governing the interchange of data) that enable communication within and among the constituent networks."[75]

Critical to this article is how that information is moved across networks and devices. Data traveling from one computer to another is broken into smaller units called packets.[76] Each of these packets might travel very different routes before ultimately arriving at its destination to be reassembled into the same form in which you sent it.[77] This communication of information from the sender to the receiver is not a constant connection or a circuit—like an old telephone call or even a lightbulb.[78] There is no constant connection from your computer to your friend's computer if you send her an email, you view a website that she created, or if you are doing an instant chat.[79] Even if you send a picture, the information you send to her is broken up into little groups originally called "datagrams" but now called "packets."[80] The packets are then sent from one machine to the other where they are reassembled, traveling by the best available route at the time as determined by complicated routing algorithms, not the end user.[81] In such a packet-switched network of networks, "the data to be transmitted (be it a webpage, images, sound files, or a video) is broken down into chunks known as packets, each of which is sent off individually to its destination."[82]

"Data travel along the Internet's communication links in packets adhering to the standard Internet Protocol (IP) that defines the packets' format and header information."[83] "An

---

[75] DAVID CLARK ET AL., AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC CONCEPTS AND ISSUES 21 (National Academies Press 2014).

[76] *Id.*

[77] *Id.*

[78] INFO. SCI. INST., UNIV. OF S. CAL., DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION 2 (1981) [hereinafter DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION].

[79] *See id.* ("The internet protocol treats each internet datagram as an independent entity unrelated to any other internet datagram. There are no connections or logical circuits (virtual or otherwise).").

[80] *Id.* at 1.

[81] INTERNET'S COMING OF AGE, *supra* note 72, at 32.

[82] Aaron L. Jones et al., Joint Comments of Internet Engineers, Pioneers, and Technologists on the Technical Flaws in the FCC's Notice of Proposed Rule-making and the Need for the Light-Touch, Bright-Line Rules from the Open Internet Order 5, https://assets.documentcloud.org/documents/3899283/Comments-of-Internet-Engineersfcc-Nn.pdf [hereinafter Joint Comments].

[83] CLARK ET AL., *supra* note 75, at 21.

Internet packet contains several important pieces of information: the numerical address of the device which sent the packet, known as an Internet Protocol address (or IP address); the IP address of the intended recipient; the type of data the packet contains; and the actual data, often referred to as the 'payload.'"[84] Thus, even when a packet's payload contains a message from one human to another, much of the data in a packet is not an assertion by any human; it is software and machine generated addressing, routing, and header information.[85]

> "The analogy often used to describe a packet is an envelope, with an address on the outside and data on the inside," but "[a] better analogy might be a postcard, since unless the data is encrypted it too is visible as the packet is moved across the Internet."[86]

[A] packet is similar to a postcard—anyone who is part of the delivery chain can read whom it is intended for, who sent it, and what it says. (Note that this does not hold true if the content of the packet is encrypted—then the packet is more like a postcard where the message is written in code only the sender and receiver can understand, but anyone reading the postcard can still see who the sender and receiver are.)[87]

"The origins and destinations of data transiting the Internet are computers (or other digital devices), which are typically connected to the Internet through an Internet service provider (ISP) that handles the necessary technical and administrative arrangements."[88] "[T]he user specifies the endpoints that they would like to communicate with, and the network is only responsible for transferring packets back and forth between the two."[89] "Information in the packets' headers enables the message to be restored to its proper order at its destination."[90] The ability of the receiving machine to properly reassemble the data into information is achieved by adherence to a protocol known as TCP/IP, an acronym for "Transmission Control Protocol

---

[84] Joint Comments, *supra* note 82, at 5.

[85] CLARK ET AL., *supra* note 75, at 21.

[86] David D. Clark & Susan Landau, *Untangling Attribution*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 25, 26–27 (National Academies Press 2010) [hereinafter Clark & Landau].

[87] Joint Comments, *supra* note 82, at 5.

[88] CLARK ET AL., *supra* note 75, at 21.

[89] Joint Comments, *supra* note 82, at 28.

[90] CLARK, et al., *supra* note 75, at 21.

(TCP)/Internet Protocol."[91] Indeed, some define the Internet by reference to TCP/IP.[92]

"Every device connected to the Internet has a unique identifying number known as its IP address. An IP address may take the form 144.171.1.22 (for IP Version 4) or 2001:db8:0:1234:0:567:1:1 (for IP Version 6)."[93] Networked computers "use the addresses carried in the internet header to transmit internet datagrams toward their destinations. The selection of a path for transmission is called routing."[94]

A 1994 National Academy of Sciences report explained:

> The core technical concept of the Internet is packet switching, which was proposed about 30 years ago as a very efficient way of sharing very expensive long-distance telecommunications circuits. A packet (a small amount of data with a destination address on the front) can be put in line with packets from other hosts and sent in turn down a link. . . .
>
> Internally, the Internet is composed of networks . . . A network is a logical entity that may in turn be composed of a number of physical network elements called subnetworks. . . . Each network has a unique network number that is part of the address of the end nodes, or computers, attached to each net. Addresses are organized in a nested manner and are represented by four elements, which are written as four numbers separated by dots. . . .
>
> The device that connects networks together and passes packets among them is called a router.[95]

So, once you have that number, an address for your destination computer, the information you want to send is broken up into

---

[91] *See* Joint Comments, *supra* note 82, at 7; DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, *supra* note 78, at 1; VINTON CERF ET AL., SPECIFICATION OF INTERNET TRANSMISSION CONTROL PROGRAM 2 (1974); J. POSTEL, INTERNET CONTROL MESSAGE PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFIC ATION 1 (1981) (describing the function of TCP).

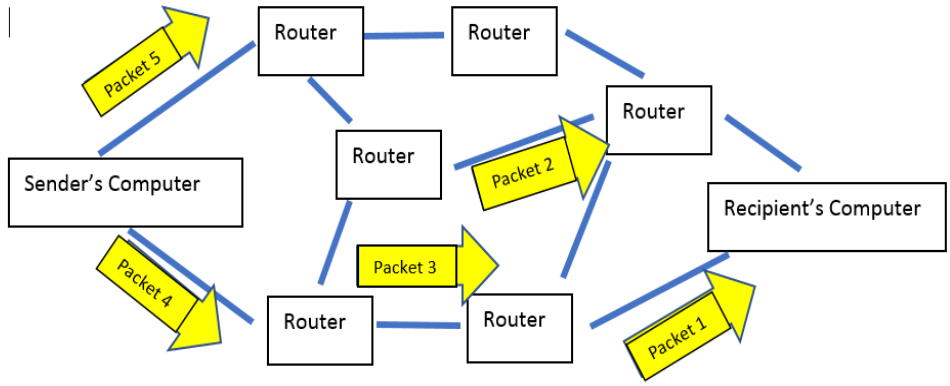
[92] *See, e.g.*, John Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, 1(1) J. CYBER POL'Y 5, 5 (2016) ("The Internet that we use today—i.e. the network of computer networks based on the Transmission Control Protocol (TCP)/Internet Protocol (IP) suite of protocols . . . ").

[93] NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 100 n.20 (William A. Owens et al. eds., 2009).

[94] DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, *supra* note 78, at 2.

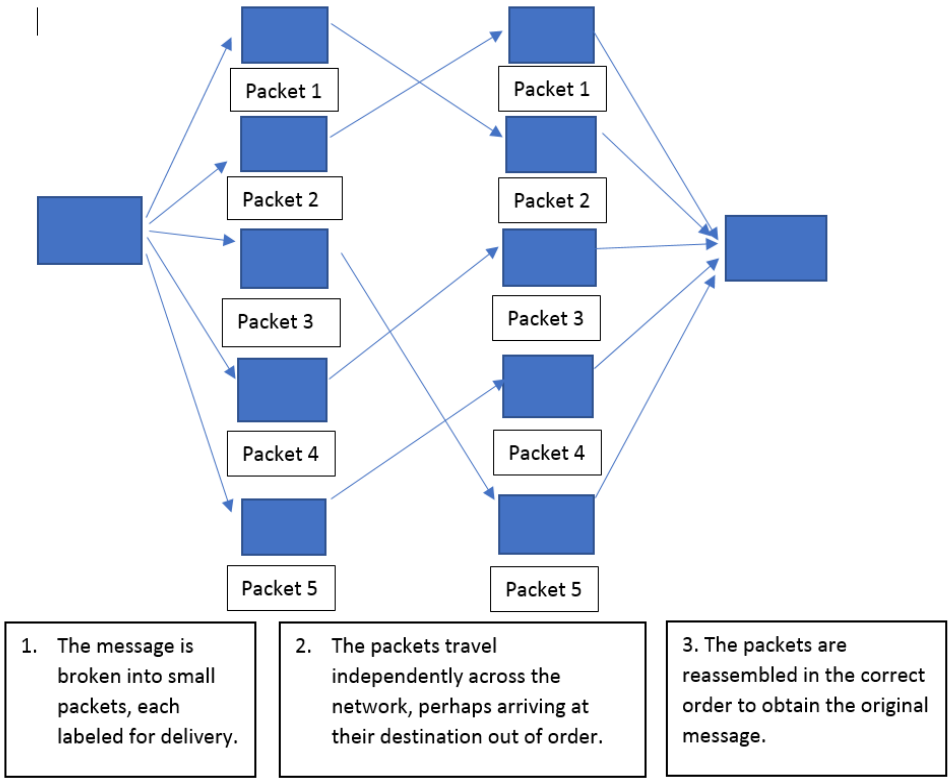
[95] NAT'L RESEARCH COUNCIL, REALIZING THE INFORMATION FUTURE: THE INTERNET AND BEYOND 246–47 (National Academies Press 1994).

packets, and that address is attached to each packet.[96] Then, when the packets leave a computer, they go to a router.[97] The router tries to decide how to get each packet on to its destination.[98] One of the interesting concepts behind much of cyberspace and particularly the Internet is that the router makes that decision separately for each packet. Every time a packet arrives at an IP router, an individual decision is made about where to send it next.[99] There is no concept of a session with a preselected path for all traffic. How does the router make a decision between routes? There is no single correct answer. More sophisticated routing measures traffic patterns and sends data through the least busy link.[100] Thus, given the web nature of this network, there are many different paths available for a packet to travel from one point, or computer, on the Internet to another point—as you can see from this simple diagram.



How a Message is Transmitted Over the Internet

[96] DAVID REED, A BALANCED INTRODUCTION TO COMPUTER SCIENCE (Prentice Hall 2004).
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*



The neutrality of the design of the Internet made it generative, in the words of Jonathan Zittrain, whose book, "The Future of the Internet, And How to Stop It" notes that: "Both [the personal computer and the Internet] were . . . designed to accept any contribution that followed a basic set of rules (either coded for a particular operating system, or respecting the protocols of the Internet)."[101] In other words, the transport system itself that known as the Internet is indifferent to what the payload of a packet is; as long as it follows the TCP/IP protocol, the payload might be a photograph, music, a communication, or any other digital data.[102]

---

[101] JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 3 (Yale Univ. Press 2008).

[102] *See generally History of the Web*, WORLD WIDE WEB FOUND., https://webfoundation.org/about/vision/history-of-the-web/. The World Wide Web is a subset of the Internet that consists pages that are linked together and links that you click. The World Wide Web was released to the public mostly in 1993, although

Thus, "[t]o the designers of the network, **the term 'Internet' is reserved for the general platform that transports data from source to destination**, in contrast to the various applications (email, the Web, games, voice, etc.), which are described as operating 'on' or 'over' the Internet."[103]

IV. THE FIRST AMENDMENT PROTECTS SPEECH, WHICH THE INTERNET IS NOT.

The First Amendment to the Constitution states that "Congress shall make no law . . . abridging the freedom of speech."[104] Speech by citizens on matters of public concern lies at the heart of the First Amendment, which "was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[105] The main theory behind this is the marketplace of ideas, which suggests that without government intervention, ideas will succeed or fail on their own merits.[106] The truth will eventually emerge as people decide for themselves what works and what does not. In the present day, as the Supreme Court has recognized in *Reno* and *Packingham*, the Internet plays a significant role in this marketplace. Courts have shown significant respect for the First Amendment protection and only allow speech to be limited in a few narrow situations with varying standards for doing so.

The first step in any First Amendment analysis is to determine whether the relevant activity falls within the law's protections.[107] In this context, that means assessing whether the activity is actually speech.[108] What would seemingly be a straightforward

---

the very first web page went public years earlier from the CERN laboratory in Europe. *Id.*

[103] Clark & Landau, *supra* note 86, at 26.

[104] U.S. CONST. amend. I.

[105] Roth v. United States, 354 U.S. 476, 484 (1957).

[106] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (indicating that "the best test of truth is the power of the thought to get itself accepted in the competition of the market").

[107] *See* Katlyn E. DeBoer, *Clash of the First and Second Amendments: Proposed Regulation of Armed Protests*, 45 HASTINGS CONST. L.Q. 333, 341 (2018) (explaining that the first step in the First Amendment analysis to determine whether the expressive nature of the conduct is equivalent to speech for First Amendment purposes).

[108] Claire A. Noonan, *Art Expressed on a Living Canvas: Proposing a Balance Between the Protection of Free Expression and the Governmental Interest in Regulating the Tattoo Industry*, 60 LOY. L. REV. 137, 142 (2014) ("The first step in a First Amendment analysis is to discern whether the disputed activity constitutes pure expression, symbolic conduct, or non-expressive conduct.").

analysis can actually be much more cumbersome. In fact, that analysis is very judge- and fact-specific.

The Supreme Court's opinion in *Clark v. Community for Creative Non-Violence*[109] demonstrates this first step. The issue in that case was whether sleeping in tents in a public park as part of a demonstration was speech for the purposes of the First Amendment.[110] The majority assumed without deciding "that overnight sleeping in connection with the demonstration is expressive conduct protected to some extent by the First Amendment,"[111] but noted "it is the obligation of the person desiring to engage in assertedly expressive conduct to demonstrate that the First Amendment even applies."[112] "To hold otherwise," the Court noted, "would be to create a rule that all conduct is presumptively expressive,"[113] which it declined to do. In short, conduct is not necessarily expressive, if not expressive then is not speech, and if not speech is not protected by the First Amendment. Moreover, that assumption was only the beginning of the Court's analysis. "Expression, whether oral or written or symbolized by conduct, is subject to reasonable time, place, or manner restrictions," which, in turn, "are valid provided that they are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information."[114] Ultimately, the Court ruled that the challenged regulation was an acceptable incidental burden on speech.[115] Indeed, Justice Burger, in a strong concurrence, would not even accept the assumption that there was any speech to protect, stating: "The actions here claimed as speech . . . simply are not speech; rather, they constitute conduct."[116] He went so far as to call the case "frivolous" and a waste of time for "1 District Judge, an en banc court of 11 Court of Appeals Judges,

---

[109] 468 U.S. 288 (1984).
[110] *Id.* at 289.
[111] *Id.* at 293.
[112] *Id.* at 293 n.5.
[113] *Id.*
[114] *Id.* at 293 (citing City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789 (1984); United States v. Grace, 461 U.S. 171 (1983); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45–46 (1983); Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 647–48 (1981); Va. Pharm. Board v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976); Consolidated Edison Co. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 530, 535 (1980)).
[115] *Clark*, 468 U.S. at 298.
[116] *Id.* at 300 (Burger, J., concurring).

and 9 Justices of this Court."[117]

The *Community for Creative Non-Violence* court cited the seminal 1968 case of *United States v. O'Brien*,[118] a 7 to 1 opinion in which the Supreme Court stated:

> We cannot accept the view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaging in the conduct intends thereby to express an idea. However, even on the assumption that the alleged communicative element in O'Brien's conduct is sufficient to bring into play the First Amendment, it does not necessarily follow that the destruction of a registration certificate is constitutionally protected activity. This Court has held that when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms. . . . [W]e think it clear that a government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[119]

We have already shown that much of the data moved by the Internet is not intended by any human to express an idea. Also, even packets of data that do contain an expressive payload (speech) always mix in nonspeech elements. We submit that many possible government regulations of the Internet would satisfy this *O'Brien* test.

Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests.[120] This commonsense meaning of the phrase "content-based" requires a court to consider whether a regulation of speech on its face draws distinctions based on the message a speaker conveys.[121] Any sort

---

[117] *Id*. at 301 (Burger, J., concurring).
[118] 391 U.S. 367 (1968).
[119] *Id.* at 376–77.
[120] Ashcroft v. ACLU, 542 U.S. 656, 660, 677 (2004).
[121] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S.

of content-based regulation is only valid if it can withstand strict scrutiny.[122]

One prominent example of a content-based speech restriction can be found in *Brandenburg v. Ohio*.[123] In *Brandenburg*, the Court held that the government could not prohibit inflammatory speech unless that speech was directed to inciting or producing imminent lawless action and was actually likely to incite or produce such action.[124] Another example of a content-based restriction is evident with false statements of fact, with varying standards depending on who the subject of the statement is. In *New York Times v. Sullivan*,[125] the Court held that the burden to prove libel against a public official requires the showing of actual malice.[126] For speech about private individuals that are not involved in public debate, that individual states must establish their own standard that falls somewhere below actual malice.[127]

Commercial speech receives limited deference under the First Amendment and review of a government regulation of commercial speech only must withstand intermediate scrutiny.[128] Thus, it is evident that whether data traversing the Internet are considered to be speech or commerce and, if speech, whether commercial or non-commercial, will make a great deal of difference in the protections afforded that speech. "Strict scrutiny" requires the government to prove that a law is necessary to achieve a compelling governmental interest, unrelated to the suppression of ideas, usually in least restrictive means available.[129] "Intermediate scrutiny" requires only that the law or regulation furthers an important or substantial governmental interest and, in this context, that the governmental interest is unrelated to the suppression of free expression.[130]

Of course, there is some speech that has no value to society and is not protected at all. Additionally, commercial speech that is false or misleading is not entitled to any protection under the First

557, 564 n.6 (1980) (discussing regulations based on the content of the speech).

[122] Sable Commc'n of California, Inc., v. F.C.C., 492 U.S. 115, 126 (1989).

[123] 395 U.S. 444 (1969).

[124] *Id.* at 447.

[125] 376 U.S. 254 (1964).

[126] *Id.* at 279–80.

[127] Gertz v. Welsh, 418 U.S. 323, 347 (1974).

[128] United States v. Edge Broad. Co., 509 U.S. 418, 426 (1993).

[129] United States v. Alvarez, 567 U.S. 709, 725 (2012).

[130] *See* Craig v. Boren, 429 U.S. 190, 219 (1976) (discussing the elevated level of scrutiny).

Amendment and, therefore, can be prohibited entirely.[131] Unprotected speech includes advocacy of illegal action, seditious libel and disclosure of private facts, owned speech, obscenity, and fighting words.[132] Laws restricting unregulated speech need only satisfy minimal scrutiny—that is, a rational connection to a legitimate state objective.[133]

The First Amendment also includes protections regarding religion and assembly. Taken as whole, these protections create an implied right to freedom of association. This premise was established in *NAACP v. Alabama*,[134] when the Court wrote that both the First and Fourteenth Amendments made it necessary to allow for the freedom of association.[135] The Supreme Court has also recognized a right to anonymity in speech, something that is more common and more easily executed on the Internet. In *McIntyre v. Ohio Election Commission*,[136] the Court held that anonymous speech is an integral part of First Amendment protections. Anonymity has a long and highly valued role throughout history.[137] It allows people to be more persuasive, to be safe from retaliation, and to create a more complete marketplace of ideas.[138] Yet, the fact that some content on the Internet might be protected speech, that the Internet provides a means by which people can associate with each other through communication, and that anonymity is relevant to Internet regulation freely does not mean that the First Amendment is dispositive or the primary means by which the Internet should be regulated.

Even if the Internet were to be considered as a medium for speech, "[e]ach medium of expression, of course, must be assessed for First Amendment purposes by standards suited to it, for each

---

131 *See* Friedman v. Rogers, 440 U.S. 1, 9 (1979) ("Equally permissible are restrictions on false, deceptive, and misleading commercial speech.").

132 *See, e.g.*, *Roth*, 354 U.S. at 483 ("libelous utterances are not within the area of constitutionally protected speech . . . obscenity, too, was outside the protection intended for speech and press"); Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.").

133 F.C.C. v. Beach Commc'n, Inc., 508 U.S. 307, 314 (1993).

134 357 U.S. 449 (1958).

135 *Id*. at 460.

136 514 U.S. 334 (1995).

137 *See id*. at 357 (for further discussion of anonymity in speech).

138 *Id*. at 341–42.

may present its own problems."[139] As delineated in Section II, *supra*, the Court did not well understand the problems of the Internet when it issued its early rulings of the cyber age. The Court has noted: "Each method of communicating ideas is 'a law unto itself' and that law must reflect the 'differing natures, values, abuses and dangers' of each method."[140] The abuses and dangers of the Internet are far different from those of a book, paper, or even television signal, because the Internet can carry computer code that actually makes things happen—such as causing an electrical generator to fail.[141]

V. THE INTERNET IS A PHYSICAL NETWORK THAT MOVES ENERGY—AND THEREBY DATA—FROM ONE LOCATION TO ANOTHER.

Now we synthesize how the Internet works with First Amendment law and assert: The Internet is a transportation system and no more speech than is a train on a railroad or a truck on an interstate highway. In the words of a National Academy of Sciences report: "The links and routers of the Internet provide the critical connectivity among source and destination computers, but nothing else."[142] A group of Internet Engineers, Pioneers, and Technologists—including Vint Cerf, a father of the Internet[143]—put it this way in 2017: "[T]he user specifies the endpoints that they would like to communicate with, and the network is only responsible for transferring packets back and forth between the two."[144]

"The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks,"[145] according to the 1981 Defense Advanced Research Projects Agency's original Internet program protocol specification.

"In light of the prominence of the Web today, Web-based

---

139 Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975).

140 Metromedia, Inc. v. City of San Diego, 453 U.S. 490, 501 (1981) (quoting Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Jackson, J., concurring)).

141 *See, e.g.*, Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vuln erability in Power Grid*, CNN (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk/.

142 CLARK ET AL., *supra* note 75, at 21.

143 Max Senges et al., *Vinton G. Cerf*, RESEARCH AT GOOGLE, https://research.google.com/pubs/author32412.html.

144 Joint Comments, *supra* note 82, at 28.

145 DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, *supra* note 78, at 1.

applications and the content and services provided by them are sometimes viewed as synonymous with the Internet; the Internet, however, is a more general-purpose network over which the Web is layered."[146] Nevertheless, remember that what the Internet connects is computers. "The network, which provides a communications fabric connecting the many computers at its ends, offers a very basic level of service, data transport, while the intelligence, the information processing needed to provide applications, is located in or close to the devices attached to the edge of the network."[147] "ISPs merely provide the transport between the end user and the capability that they are attempting to access."[148] "The [Internet's] architecture, in which the Internet protocol provides the fundamental means of sending data across the Internet, allows any type of communication, application, or service to ride on top of the Internet."[149] That edge service provided might be an information service of some form of communication between humans, but it might not be. One portion of each packets carries a payload without regard to what the payload is—routing instructions, an email, a news article, a software program, a virus, or whatever.

> [T]he Internet was rightly designed to be a dumb network, with most of its features and complications pushed to the endpoints. . . . This use of end-to-end says that packets should be routed between the sender and the recipient without anyone stopping them on the way to ask what they contain.[150]

The Internet Protocol is simply indifferent to the data contained in the payload of the packet.[151] The payload can be anything that can be reduced to binary electronic format. As explained above, only some of that data is payload, the data may or may not be information, the information may or may not be expressive conduct, that expressive conduct may or may not be speech, and that speech may or may not be protected by the First Amendment.

---

146 INTERNET'S COMING OF AGE, *supra* note 72, at 32.
147 *Id*. at 4.
148 Joint Comments, *supra* note 82, at 20.
149 INTERNET'S COMING OF AGE, *supra* note 72, at 138.
150 ZITTRAIN, *supra* note 102, at 164.
151 P. CHIMENTO & J. ISHAC, DEFINING NETWORK CAPACITY 9 (2006) ("IP layer link capacity includes the IP header and is indifferent to the uniqueness of the data contained within the packet payload").

VI. FEDERAL POWER TO REGULATE THE INTERNET

The Commerce Clause of the Constitution provides that Congress has the authority to "regulate commerce with foreign nations, and among the several states, and with the Indian tribes."[152] The Commerce Clause is one of the most heavily relied upon powers by Congress when making laws. The potential power of the Commerce Clause went relatively unutilized until the New Deal, when the Supreme Court significantly expanded regulatory authority under that clause.[153] Only recently has the Court begun to restrict Congress's Commerce Clause authority.[154]

The Supreme Court has interpreted "among the several states" to include three different forms of interstate commerce, including the channels of interstate commerce,[155] the instrumentalities of interstate commerce,[156] and activities that substantially affect interstate commerce.[157]

Congress has relied on the Commerce Clause as the basis for regulating telephone networks as well as the Internet, particularly when it comes to computer crimes.[158] The Eleventh Circuit has ruled that "[t]he Internet is an instrumentality of interstate commerce. . . . Congress clearly has the power to regulate the Internet, as it does other instrumentalities and channels of interstate commerce."[159] Several U.S. Circuit Courts have clearly decided that the Internet is both a channel and instrumentality of interstate commerce.[160] This makes even more sense when

---

[152] U.S. CONST., art. I, § 8, cl. 3.

[153] *See* DAVID FORTE, COMMERCE, COMMERCE, EVERYWHERE: THE USES AND ABUSES OF THE COMMERCE CLAUSE 1 (Heritage Foundation 2011), https://www.heritage.org/the-constitution/report/commerce-commerce-everywhere-the-uses-and-abuses-the-commerce-clause.

[154] *See, e.g.*, United States v. Lopez, 514 U.S. 549, 551 (1995) ("We hold that the Act exceeds the authority of Congress "to regulate Commerce . . . among the several States").

[155] *See, e.g.*, Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 256 (1964) ("[T]he authority of Congress to keep the channels of interstate commerce free from immoral and injurious uses has been frequently sustained").

[156] *See, e.g.*, Hous., E. & W.T.R. Co. v. United States, 234 U.S. 342, 353 (1914) ("Congress . . . may prevent the common instrumentalities of interstate and intrastate commercial intercourse from being used . . . ").

[157] *Lopez*, 514 U.S. at 558–59 (1995).

[158] ORIN KERR, COMPUTER CRIME LAW 675 (3d ed. 2012).

[159] U.S. v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004).

[160] *See, e.g.*, United States v. Gilbert, 181 F.3d 152, 158 (1st Cir. 1999); United States v. Carnes, 309 F.3d 950, 954 (6th Cir. 2002); United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005) (for cases in which the Court held that telecomm unications are channels and/or instrumentalities of interstate commerce).

considering how packets may travel through several different jurisdictions.[161]

In fact, the statute at issue in *Reno*, the CDA, was based on Congress's Commerce Clause authority. Both provisions of the statute that were challenged required that the communication be "in interstate or foreign communications."[162] The authority to regulate the Internet is not in doubt. The extent to which that power enables the government to do so, however, has yet to be realized.

Presumably, under specific circumstances, other portions of the Constitution would empower the federal government to regulate the Internet. If, for example, "[p]otential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests,"[163] then national security powers are implicated, including the President's authority as Commander-in-Chief of the military and Congress's powers to declare war and to regulate the military. "From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001."[164]

The power conferred on the legislative and executive branches by the Constitution are, of course, limited by other provisions of the Constitution. Much has been written about search and seizure in the digital context, for example. To be clear, the argument here is not that the Commerce Clause or some other provision gives the federal government unlimited power to regulate the Internet. The argument to this point is that there exist relevant affirmative grants of power for such regulation, and that regulation of the Internet is not primarily regulation of First Amendment-protected speech.

VII. PACKETS ARE COMMERCE AND CAN BE REGULATED AS SUCH

A truck traveling along an interstate highway in the United States is not exempt from regulation if its cargo is political pamphlets or bibles.[165] Coercive and mandatory laws require that

---

[161] *See supra* Part III for further discussion of how the Internet functions.

[162] 47 U.S.C.A. § 223(a), (d).

[163] U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 9 (2015).

[164] *Id.*

[165] *See* Lone Star Sec. & Video, Inc. v. City of L.A., 989 F.Supp.2d 981, 990, 992 (C.D. Cal. 2013) (holding municipal ordinances that prohibited parking mobile

the truck be of certain dimensions, have specific safety equipment, display a registration plate, be inspected periodically and display confirmation of the same, and be operated by a licensed driver, among many other requirements and restrictions.[166] The presence of speech in the cargo area of the truck does not alter the legality of those many laws concerning the design, construction, equipment, and most importantly operation of the truck. Even vehicles whose primary purpose is to spread messages—such as a loudspeaker car in a political parade or a billboard truck—must follow the highway and motor vehicle laws.[167] At the federal level, they are regulated pursuant to the affirmative grant of power in the Commerce Clause of the Constitution without reference to the limitations imposed upon government by the First Amendment. Try telling a state trooper that she may not stop you or fine you for driving without an operator's license and speeding in a car with no registration plate, no safety inspection sticker, and no brake lights because your vehicle contains your lecture notes and you are on your way to go utter Constitutionally protected speech.

The fundamental change when switching to a Commerce Clause framework of Internet regulation is that the presumption of the ability to regulate shifts. Under a First Amendment speech analysis, the presumption is that the government cannot restrict Internet activity.[168] But when properly viewed through governing authority of the Commerce Clause, the presumption is that the government can regulate.[169] Any disagreement with government action must then be challenged in court. Between a presumption of being able to regulate the Internet, the nature of the movement of packets across state lines, and the broad authority of the

advertising billboards on public streets did not violate free speech as traffic safety, parking control, and aesthetics constituted substantial government interests).

166 *See generally* 49 C.F.R. Parts 300–99 (2011) (for regulations relating to transportation). *See* 49 C.F.R. § 372.001–372.117 (for exemptions to transportation regulations, not including the contents of a truck).

167 *See, e.g.*, Ctr. for Bio-Ethical Reform, Inc. v. City of Springboro, 477 F.3d 807, 821–22 (6th Cir. 2007) (holding billboard trucks driven by pro-life plaintiffs that depicted graphic abortion images constituted First Amendment-protected expressive conduct but giving no indication that the drivers and their vehicles were exempt from other laws).

168 Jeremy H. Lipschultz, *Social Media and the First Amendment*, THE HUFFINGTON POST (Dec. 6, 2017), https://www.huffingtonpost.com/jeremy-harris-lipschultz/social-media-and-the-first-amendment_b_4976694.html.

169 *See generally* Michelle Armond, *State Internet Regulation and the Dormant Commerce Clause,* 17(1) BERKELEY TECH. L.J. 379 (2002) (for further discussion of State Internet regulation efforts).

Commerce Clause as it is currently defined, the government would have the ability to regulate the vast majority of Internet activity.

Of course, the power to regulate is separate from the wisdom of regulating. We are not necessarily calling for the Internet to be regulated as thoroughly as interstate highways and the vehicle and operators who move on them are. We submit that the best paradigm for reviewing the Constitutionality of Internet regulation by the United States Government is that of a transportation system in which service providers—usually private and commercial—move goods (data) from one place to another. Regulating this network of networks would be akin to regulating the brakes on a truck because its cargo bay might contain religious or political tracts. In the event that some regulation of the Internet is sufficient to bring into play the First Amendment, then *O'Brien*'s test for incidental burdens on speech[170] should be employed, with great deference for the government's legitimate interests in "highway safety"—here, for example, stopping attacks on the electrical power grid and other critical infrastructure or the spread of malware.

VIII. THE IMPLICATIONS

With greater authority also comes greater responsibility. If the government has the authority to control what happens on the Internet, citizens might hold it responsible when things there do not go well. General cybersecurity issues, the spread of extremist ideology, and other problems that stem from the Internet are now squarely within the government's authority to control, although not always within its ability. The onus is with the federal government to respond to, and ideally fix, these problems.

A. How might the governments regulate in cyberspace, especially the Internet?

There a number of ways in which governments can implement policies to affect conduct on the Internet. That is, the federal government has a number of tools in its toolbox that it can use. The available tools include, at least, administrative law, criminal law, civil law, monetary incentives, education, leadership or displaying best practices, and the use of military force.

The first tool is administrative law. Consider, for example, the

[170] *See supra* Part IV for more on the interplay of the First Amendment and the Internet.

Federal Communications Commission and the Interstate Commerce Commission trying to assert themselves into net neutrality.[171] They regulate, not at the congressional level, but at an agency level. Television and radio are regulated on the theory that they are a limited good and, therefore, the use of it is something that needs to be licensed and controlled.[172] Some federal agencies have used this same logic to argue that the Internet itself is a limited spectrum and should be regulated the same way.[173] One part of that argument is that packets are not all equal. Packets with news should take precedence over less crucial Internet traffic such as Netflix.[174] An entire regulatory regime could be created for the Internet, complete with licensing, fines, renewals, reviews, and all the administrative procedure that comes with it.

Such administrative law may seem punitive, and, therefore, like criminal law, but it is different in two significant ways. First, enforcement of administrative law usually does not lead to a trial in front of jurors, and it does not require proof beyond a reasonable doubt as the standard.[175] Second, it can control things in the future more than criminal law. That is, you may not broadcast until you get a license so you are limited from access, whereas criminal law, at least historically, has looked for misdeeds in the past.

---

[171] *See Restoring Internet Freedom*, FEDERAL COMM. COMMISSION, https://www.fcc.gov/restoring-internet-freedom (elaborating on prior FCC regulations with respect to Internet service providers).

[172] *See* Stuart N. Brotman, *Revisiting the Broadcast Public Interest Standard in Communications Law and Regulation*, BROOKINGS INSTITUTION (Mar. 23, 2017), https://www.brookings.edu/research/revisiting-the-broadcast-public-interest-standard-in-communications-law-and-regulation/ ("[B]ecause of the limited availability of broadcasting frequencies, the FRC was entitled to consider the 'character and quality of the service being rendered.'").

[173] *See, e.g.*, Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601, 5611 (2015), *abrogated by* Restoring Internet Freedom, 2018 WL 305638 (F.C.C.) (2018). *See also* Cecilia Kang, *Court Backs Rules Treating Internet as Utility, Not Luxury*, THE NEW YORK TIMES (Jun. 14, 2016), https://www.nytimes.com/2016/06/15/technology/net-neutrality-fcc-appeals-court-ruling.html; Jonathan Aberman, *Access to Internet is a Public Benefit. It Should be Regulated that Way.* THE WASHINGTON POST (Nov. 27, 2017), https://www.washingtonpost.com/news/capital-business/wp/2017/11/27/access-to-internet-is-a-public-benefit-it-should-be-regulated-that-way/.

[174] *See* U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 762–63 (D.C. Cir. 2016) (Williams, J., concurring in part and dissenting in part) (explaining consumption habits of Internet users); Richard Epstein, *The Irrelevance of the First Amendment to the Modern Regulation of the Internet*, ICARUS 14, 23–24 (2013) (discussing net neutrality).

[175] John F. Duffy, *Jury Review of Administrative Action*, 22(2) WM. & MARY BILL RTS. J. 281, 281 (2013); 5 C.F.R. § 2423.32 (2018).

The second tool is the aforementioned criminal law, which is a traditional way for nation states to enforce their will, including on the Internet.[176] Some of the earliest attempts in 1984 and 1986 were the Computer Fraud and Abuse Act (CFAA)[177] coupled with the opinion in *United States v. Morris*.[178] The CFAA establishes unauthorized access to a protected computer as the fundamental unit of prosecution.[179] The *Morris* case concerned the first virus to be released on the Internet—back before the public even had Internet access.[180] In that case, "unauthorized" was viewed as not just someone who didn't have permission to access the system at all—because the defendant actually did have a username and password for the Internet—but "unauthorized" in the sense that the person used it for some purpose other than what the owners, developers, and operators of the hardware intended.[181] The definition of "protected computer" under the Computer Fraud and Abuse Act includes any computer connected to a network that crossed interstate lines.[182] That, of course, now includes any computer that is connected to the Internet.

The Wiretap Act and the Electronic Communications Privacy Act[183] and similar measures outlawed unauthorized[184] eavesdropping upon electronic communications. The Espionage Act criminalizes the exploitation, or even espionage, involved in stealing trade secrets, including what could be done online or by computer hacking.[185] The material support for designated foreign terrorist organization statutes have been interpreted to include providing communications capabilities, such as the Internet, to either designated terrorist organization or for the purpose of carrying out terrorist attacks.[186] In addition to those examples,

---

[176] *See generally* KERR, *supra* note 159 (for more on using criminal law to regulate Internet behavior).

[177] 18 U.S.C.A. § 1030.

[178] 928 F.2d 504 (2d Cir. 1991).

[179] 18 U.S.C.A. § 1030(a)(1).

[180] Morris, 928 F.2d at 505.

[181] *Id*. at 510.

[182] 18 U.S.C.A. § 1030(e)(2)(B).

[183] Wiretap Act, 18 U.S.C.A. § 2511 (West, Westlaw through P.L. 115-140 approved 03/20/18) (amended 2018), *invalidated by* Hutton v. Woodall, 70 F.Supp.3d 1235 (D. Colo. 2014); Electronic Communications Privacy Act of 1986, 18 U.S.C.A. § 2510–22 (West, Westlaw through P.L. 115-140 approved 03/20/18).

[184] 18 U.S.C.A. § 2510–22 (including among its provisions prohibited acts to intercept communications and methods by which government actors could intercept communications).

[185] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996).

[186] 18 U.S.C.A § 2339A, § 2339B (West, Westlaw through P.L. 115-140

there are a variety of other criminal laws that apply to the Internet, even if not specifically written with the Internet in mind.

The third possibility for how nation states could assert authority in the Internet is civil law. This could be tort law, such as not exercising the appropriate duty of care to protect data that gets stolen or liability actually for stealing data. There are also civil components of both copyright law and trademark law. Other than licensing, civil law has struggled to develop in the cyber area, because courts have difficulties in determining what a reasonable standard of care is.[187] Courts have used different methods to determine these standards, but an alternative would be having Congress or an administrative agency set the standard. This method of having people assert their own rights by suing for damages is an area in which there can be much more development.

Another tool for governments is monetary incentives, which can be effective far beyond just the major companies such as Internet service providers. The incentives, either the giving or withholding of money, could be in the form of taxes or grants. One example is the Rockefeller-Snowe bill, which never became law but was once the biggest headline proposal around.[188] That had a provision in it that essentially required anyone who received federal money to meet federal security standards on their computers, and provided for the recruitment and training of information technology workers and security managers.[189] Nearly every university, state, and town receives federal funding and would be affected. In addition, any company that is a contractor that does business with the federal government would have been covered.[190]

---

approved 03/20/18). *See, e.g.*, United States v. Mustafa, 406 Fed.Appx. 526 (2d Cir. 2011); Pennie v. Twitter, 281 F.Supp.3d 874 (N.D. Cal. 2017); United States v. Elshinawy, 2018 WL 1521876 (D. Md. 2018) (entertaining the interplay between Internet conduct and the material support statutes). *See also* Benjamin Wittes & Zoe Bedell, *Tweeting Terrorists, Part II: Does it Violate the Law for Twitter to Let Terrorist Groups Have Accounts?* LAWFARE (Feb. 14, 2016), https://www.lawfareblog.com/tweeting-terrorists-part-ii-does-it-violate-law-twitter-let-terrorist-groups-have-accounts.

[187] *See* Katie B. Williams, *Judges Struggle with Cyber Crime Punishment,* THE HILL (Jan. 9, 2016), http://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment (elaborating on struggles "to determine the appropriate punishments for cyber crimes").

[188] Cybersecurity Act of 2009, S. 773, 111th Cong. (2010).

[189] *Id.* at § 5, 12.

[190] *Id.* at § 5. *See also* National Highway System Designation Act of 1995, Pub. L. No. 104-59, 109 Stat. 568 (1995). As a similar example of federal funding restrictions, Congress had at one time prohibited any state that set its own speed limit above 55 m.p.h. from being eligible for federal highway dollars.

The remaining tools—education, leadership, and military force—are available to the government but likely do not fit with the Commerce Clause model of regulation. Government education campaigns have been largely effective in changing public behavior, such as with smoking and drunk driving.[191] The federal government could follow a similar model to push for improved cyber hygiene. The government can also lead by example by adopting best practices internally and requiring those who want to do business with the government to do the same. The federal government desegregated the military in 1948[192] while the rest of society desegregated itself in the 1960s. Finally, of course, the government can use military force, but it is unlikely (and illegal) for Congress to use military force domestically to enforce a Commerce Clause authority.

B. So, what are the implications of this paradigm shift?

When viewed as regulation of a transportation system rather than direct regulation of speech, the government is more likely to have the authority to require a wide variety of cybersecurity measures. Some, no doubt, have not yet been conceived. Here is a sampling of possibilities.

Deep packet inspection: Law might require Internet service providers to examine all packets for known signatures of malware. Given the drain on resources that such comprehensive inspection would entail, regulations might require the inspection of the data in packets only when they originate from certain locations and networks or are of a specified type. If the requirements for selection of packets to be inspected do not hinge upon the contents of the packets, this would be a content-neutral regulation if challenged under the First Amendment. Just as trucks may be inspected to see if their contents are hazardous, the government might have authority to inspect packets for hazardous payloads.

Carrier Liability: Current law exempts Internet service

---

191 *See, e.g.*, *Increases in Quitline Calls and Smoking Cessation Website Visitors During a National Tobacco Education Campaign—March 19-June 10, 2012*, CTR. FOR DISEASE CONTROL AND PREVENTION (Aug. 31, 2012), https://www.cdc.gov/mmwr/preview/mmwrhtml/mm6134a2.htm; *What Works: Strategies to Reduce or Prevent Drunk Driving*, CTR. FOR DISEASE CONTROL AND PREVENTION (Mar. 22, 2016), https://www.cdc.gov/motorvehiclesafety/impaired_driving/strategies.html ("Mass media campaigns spread messages about the physical dangers and legal consequences of drunk driving. They persuade people not to drink and drive and encourage them to keep other drivers from doing so.").

192 Exec. Order No. 9981, 13 Fed. Reg. 4313 (1948).

Note: Typographical error on this page corrected 7/4/2019.

providers from liability for the contents of the packets they transport.[193] The carriers, like trucking companies, might be held responsible for unsafe or illegal contents of packets, with liability being of the civil or criminal or regulatory type.

Software liability: As car manufactures are responsible if their airbags do not work properly to protect occupants,[194] software marketers might be responsible for security vulnerabilities in their products.

Design regulations: Trucks must have a certain configuration of lights for safety.[195] Devices connected to the Internet might be required to have certain features, such as the ability update their software remotely. This problem is demonstrated by the "KRACK" Wi-Fi bug, which revealed that many devices of the "Internet of Things" could not be updated to patch a newly discovered software vulnerability without uninstalling them and onerous actions by the user.[196] This regulation might apply to manufacturers, distributors, or end users, or some combination thereof.

Identity requirements: By federal law, commercial vehicles must plainly state in signs on their doors the name and address of the operator.[197] A wide variety of identification and authentication schemes for Internet users might be considered and either incentivized or employed.

These and a host of other cybersecurity measures each have policy and legal drawbacks. But, when viewed as possible regulations of the packet transportation system, the people's elected representatives are free to weigh those costs and benefits and choose what is most in everyone's interest to create an Internet that is safe for everyone to obtain its benefits.

Critics of increased regulation fear a restriction on free speech. Advocates of the marketplace of ideas worry that any regulation will lead to government control of content. In fact, however, the network is neutral as to the content of packets, and regulation of the packet transport system is quite different from regulating speech. Incidental effects on speech can be balanced against the public safety benefits of the regulation.

---

193 *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (laying out the limitations on carrier liability for copyright infringement).

194 49 U.S.C. § 30127 (1998).

195 49 C.F.R. § 393.24 (2005).

196 Brian Barrett, *Why the Krack Wi-Fi Mess Will Take Decades to Clean Up*, WIRED (Oct. 17, 2017), https://www.wired.com/story/krack-wi-fi-iot-security-broken/.

197 49 C.F.R. § 390.21 (2000).

Other policy concerns abound. One of the fundamental tenets of the Internet is that it should be a free and self-governed space. Yet cyber crime and even threats to national security are real. They should not be disregarded on the strength of the erroneous argument that Internet packets are speech, and the First Amendment precludes most regulation of it.

IX. CONCLUSION

The Supreme Court in *Reno* set a legal standard for the review of regulation of the Internet that remains divorced from the reality of how that network of networks actually functions. To borrow Justice Kennedy's words in the 2017 case *Packingham v. North Carolina*, the Court did not yet understand the nature of the revolution that is the cyber age. Rather than viewing these networked computers that are used to control critical and dangerous objects and services through the lens of a constitutional limit on government power—such as the First Amendment—the Court should view the Internet as it does the interstate highway system—through the lens of affirmative grants of power such as the Commerce Clause or national security powers. What Internet service providers do is conduct, not speech. They move packets of data from one place to another. Much of that data represents information that does not exist in any human mind and, therefore, could not possibly be expressive of anyone's thoughts or speech by any person.

Even if some of the data transported by the Internet were to be considered speech, the Internet would be a very different medium than its historical predecessors. A different balance of interests would be required. Much like trucks on a highway might carry caustic acid or political tracts, the presence of expressions of human thoughts in some packets will rarely outweigh legitimate government interests in public safety and security.

It is time to move on from cases like *Reno v. American Civil Liberties Union* and enact and uphold tech-informed policies to make the Internet a safe transportation system for data.