No. 24-171

In the
Supreme Court of the United States

COX COMMUNICATIONS, INC. and COXCOM, LLC,

Petitioners,

v.

SONY MUSIC ENTERTAINMENT, et al.,

Respondents.

On Writ Of Certiorari
To The United States Court Of Appeals
For The Fourth Circuit

BRIEF FOR INTERNET SOCIETY AS AMICUS CURIAE SUPPORTING COX COMMUNICATIONS, INC. AND COXCOM, LLC,

RAECHEL KEAY ANGLIN
COUNSEL OF RECORD
BRENDAN J. ANDERSON
SPENSER B. JAENICHEN
MOSHE Y. KLEIN
MORGAN, LEWIS & BOCKIUS LLP
1111 PENNSYLVANIA AVE., N.W.
WASHINGTON, DC 20004
(202) 739-3000

TABLE OF CONTENTS

Page

TABLE OF CONTENTS I

INTEREST OF AMICUS CURIAE 1

SUMMARY OF ARGUMENT 1

ARGUMENT 4

I. The Fourth Circuit's Liability Standard Threatens Internet Access for Millions of Americans. 4

A. The Internet Serves Vital Societal Functions 4

B. The Negative Practical Ramifications of Internet Access Termination. 8

II. The Fourth Circuit's Liability Standard Does Not Align with How the Internet Operates 13

A. Numerous Intermediaries Support the Internet's Functions. 13

B. The Fourth Circuit's Liability Standard Would Be Difficult to Administer And Could Undermine the Operation of the Internet 17

III. The Fourth Circuit's Standard Comes with Serious Privacy and Security Risks. 19

A. The Fourth Circuit's Liability Standard Would Radically Change an ISP's Role. 19

B. Requiring ISPs to Police Copyright Infringement Risks Users' Privacy and Security. 19

CONCLUSION 23

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Am. Civil Liberties Union v. *Reno*,
929 F. Supp. 823 (E.D. Pa. 1996) 5

Reno v. *American Civil Liberties Union*,
521 U.S. 844 (1997) 5

Federal Statutes

47 U.S.C. 230(a), (b)(2)-(3) 4

Rules

Rule 37.6 1

Other Authorities

Alex Matthews and Catherine E. Tucker,
Government Surveillance and Internet Search Behavior (Feb. 17, 2017),
https://rb.gy/x7yc2p 21

Biden-Harris Administration Announces Nearly &700 Million to Connect People in Remote and Rural Areas to High-Speed Internet, U.S. DEP'T OF AGRICULTURE (Aug. 21, 2023), https://www.usda.gov/about-usda/news/press-releases/2023/08/21/biden-harris-administration-announces-nearly-700-million-connect-people-remote-and-rural-areas-high 7

Callum Tennant, *What to Look For in Choosing a VPN*, INTERNET SOCIETY (Oct. 24, 2019), https://www.internetsociety.org/blog/2019/10/what-to-look-for-when-choosing-a-vpn/ 21

Community networks: Internet for the people, by the people, WORLD WIDE WEB FOUNDATION (Sept. 2, 2019), https://webfoundation.org/2019/09/community-networks-internet-for-the-people-by-the-people-the-web-untangled..... 10

Community Networks Success Stories, INTERNET SOCIETY (last visited Sept. 4, 2025), https://www.internetsociety.org/issues/community-networks/success-stories/ 11

Data Retention Effectively Changes the Behavior of Citizens in Germany, KREATIVRAUSCHEN (June 4, 2008), https://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/ 22

Encrypted DNS Factsheet, INTERNET SOCIETY (May 2023), https://www.internetsociety.org/resources/doc/2023/fact-sheet-encrypted-dns/ 20

FEDERAL TRADE COMMISSION, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf 21

Internet service provider (ISP), LEGAL INF. INSTITUTE (last visited Sept. 4, 2025), https://www.law.cornell.edu/wex/internet_service_provider_(isp). 19

INTERNET SOCIETY, *A Policy Framework for Internet Intermediaries and Content,* at 20 (Jan. 2025), https://www.internetsociety.org/wp-content/uploads/2024/12/2025-Policy-Framework-Report-EN.pdf 15

Internet Society Perspectives on Internet Content Blocking: An Overview, INTERNET SOCIETY (Mar. 2017), https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf. 20

Internet Way of Networking; Defining Critical Properties of the Internet, INTERNET SOCIETY (Sept. 9, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/ 13, 14, 15

João Paulo de Vasconcelos Aguiar, *What Is Community-Centered Connectivity and Why Should We Care?,* INTERNET SOCIETY (July 17, 2025), https://www.internetsociety.org/blog/2025/07/what-is-community-centered-connectivity-and-why-should-we-care/ 3

Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME LAW REV. 815 (2004) 14

Mary Madden, *Hurricane Katrina: In the face of disaster and chaos, people use the internet to coordinate relief*, PEW RESEARCH CTR. (Sept. 7, 2005), https://www.pewresearch.org/internet/2005/09/07/hurricane-katrina-in-the-face-of-disaster-and-chaos-people-use-the-internet-to-coordinate-relief/ 7

One year later: September 11 and the Internet, PEW RESEARCH CTR. (Sept. 5, 2002), https://www.pewresearch.org/internet/2002/09/05/one-year-later-september-11-and-the-internet-2/#:~:text=The%20Web%20as%20a%20public,on%2046%25%20of%20such%20sites 7

Ravie Lakshmanan, *Over 4,000 ISP IPs Targeted in Brute-Force Attacks to Deploy Info Stealers and Cryptominers*, THE HACKER NEWS (Mar. 4, 2025), https://thehackernews.com/2025/03/over-4000-isp-networks-targeted-in.html 22

Sadia Azim, *Why the Internet Is the New Public Utility*, INTERNET SOCIETY (June 25, 2025), https://pulse.internetsociety.org/blog/why-the-internet-is-the-new-public-utility 6

Stuart A. Thompson and Charlie Warzel, *How To Track President Trump*, N.Y. TIMES (Dec. 20, 2019), N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html..... 22

Trump Administration Invests $86 Million in Rural Broadband Service in Eight States, U.S. DEP'T OF AGRICULTURE (June 24, 2020), https://www.usda.gov/about-usda/news/press-releases/2020/06/24/trump-administration-invests-86-million-rural-broadband-service-eight-states 7

What is a business VPN? Business VPN use and limitations, CLOUDFARE (last visited Sept. 4, 2025), https://www.cloudflare.com/learning/access-management/what-is-a-business-vpn/ 23

INTEREST OF AMICUS CURIAE[1]

Founded in 1992, the Internet Society is a U.S. non-profit organization headquartered in Virginia for the worldwide coordination of, and collaboration on, Internet issues, standards, and applications. The Internet Society's staff—located in more than 30 countries around the world—is composed of technical experts in internetworking, cybersecurity, and network operations, among other fields, as well as policy experts in a broad range of Internet-related areas.

As a global non-governmental organization, the Internet Society believes that the Internet should be for everyone. It supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society, with an overarching goal that the Internet be open, globally connected, secure, and trustworthy. The Internet Society supports communities that seek to connect to each other through the Internet. It advances the development and application of Internet infrastructure, technologies, and open standards. The Internet Society also advocates for policies that protect the Internet and allow it to flourish for all.

SUMMARY OF ARGUMENT

The Internet is an integral part of modern American life. Americans rely on the Internet to work and

---

[1] In accordance with this Court's Rule 37.6, amicus states that no counsel for a party authored this brief in whole or in part, and that no person other than amicus, its members, or its counsel made a monetary contribution intended to fund its preparation or submission.

study remotely; to apply to jobs, universities, and grant programs; and to engage in political and social discourse. Americans count on the Internet for medical, psychological, and pharmacological care. The Internet is key to the American economy, facilitating financial transactions and supporting American businesses, from mom-and-pop businesses to AI innovators. It is essential that all Americans have consistent and reliable access to the Internet.

In rural communities like Enfield, North Carolina, a small family-owned Internet Service Provider ("ISP") may be the primary provider of Internet access to residents and the local public library. Under the Fourth Circuit's standard, if a single library patron were accused of copyright infringement, the ISP could be forced to terminate Internet access entirely, plunging the town back into digital darkness.

The Fourth Circuit's liability standard likely will lead to serious, real-world consequences. The Fourth Circuit's rule would require ISPs to terminate service for any customer account associated with alleged infringement or else risk crippling statutory damages under the Copyright Act. Under the Fourth Circuit's opinion, an ISP could be held responsible for copyright infringement for simply allowing a customer with account users who allegedly engaged in copyright infringement to continue subscribing to the ISP's services. This standard would incentivize ISPs to monitor and attempt to police copyright infringement by terminating any customer with account users suspected of infringement—or else risk incurring high statutory penalties under the Copyright Act.

As the Enfield example illustrates, and as this brief will explain, this standard will likely have devastating ramifications that extend far beyond any single alleged infringer. It threatens to cut off Internet access for innocent families, schools, and entire communities, with a disproportionate impact on those who are already underserved and can least afford it.

Internet access is a basic need in the modern economy. Because households and groups, as well as individuals, can all be under a single contract with an ISP, many innocent *non-infringing* users could have their main, or only, source of Internet access cut off if a single individual associated with an account engages in alleged infringement. At a minimum, the cost of preventing liability could make it impossible for groups such as non-profit ISPs or community networks[2]—connectivity solutions built for, with, or by local communities—to operate, with a potentially disproportionate and grievous impact on those communities that are already underserved or cannot afford Internet service options.

Furthermore, the Fourth Circuit's rule is unworkable. It ignores the complex, collaborative structure of the Internet, where dozens of independent intermediaries are required to deliver a single piece of data, making it both impractical and unjust to hold one ISP responsible for the actions of a user. To avoid liability,

---

[2] João Paulo de Vasconcelos Aguiar, *What Is Community-Centered Connectivity and Why Should We Care?,* INTERNET SOCIETY (July 17, 2025), https://www.internetsociety.org/blog/2025/07/what-is-community-centered-connectivity-and-why-should-we-care/.

ISPs would be incentivized to monitor their users' private communications, violating fundamental privacy expectations and creating new security risks.

For each of these independent reasons, the Fourth Circuit should be reversed, and the Court should adopt a liability standard that does not require ISPs to police copyright infringement or terminate users. Copyright holders will not be left without recourse, because they can take direct legal action against the owners of the accounts that are asserted to be infringing copyright.

ARGUMENT

I. The Fourth Circuit's Liability Standard Threatens Internet Access for Millions of Americans.

Requiring ISPs to terminate Internet access to accounts allegedly used for copyright infringement—or face potentially crippling copyright liability—threatens Internet access for millions of Americans. Internet access is vital, and the Fourth Circuit's rule puts the Internet unnecessarily at risk.

A. The Internet Serves Vital Societal Functions

The Internet is a critical component of American society. The Internet allows participants access to a vast "free market" of resources and information, including the ability to "control" what information is received and, most novelly, participate in shaping communication and content. See 47 U.S.C. 230(a), (b)(2)-(3). Much like the U.S. Postal Service and telephone service companies, both of which have been relied

upon for the dissemination of critical information during some of the nation's most difficult times, ISPs provide a general means of communication to further expand the dissemination of information and ideas across the country. To accomplish these interactivity goals, Congress enacted a law—Section 230—that upended traditional publisher liability and made clear that Internet service and content providers would not be liable for content posted by other online participants.

Section 230 has facilitated a vast amount of communication (artistic, political, intellectual, pedestrian, and otherwise) that now flows through the Internet—whether through blogs; message boards; social media both large and small; videos, podcasts, or music uploaded to the Internet; or other means. The "dramatic expansion of this new marketplace of ideas" has only continued since this Court's decision in *Reno* v. *American Civil Liberties Union*, 521 U.S. 844, 885 (1997); see also *Am. Civil Liberties Union* v. *Reno*, 929 F. Supp. 823, 881 (E.D. Pa. 1996) (observing the beneficial "democratizing" effects of Internet interactivity and noting "that the Internet has achieved, and continues to achieve the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen"). The Internet provides Americans the opportunity to exercise the basic founding principles this nation was built upon, including liberty, social mobility, and freedom of speech and religion. The open ecosystem of the Internet allows Americans to connect both publicly and privately with others nationally (and globally) in a manner that did not exist even 50 years ago.

An Internet connection is essential to access many essential services and aspects of American life. The Internet connects people to federal, state, and local governments for information related to events, elections, town halls, and proposed and enacted legislation. Americans also use the Internet to access critical governmental benefits, such as Social Security, Medicare and Medicaid, and the Supplemental Nutrition Assistance Program. Furthermore, Americans of all ages use the Internet for various reasons daily, furthering their education, careers, and finances, and accessing medical care. Most Americans need an Internet connection to apply to a job, receive communications from their employer, and manage their finances—whether they seek a manufacturing or cashier job or a high-tech position. Americans living in rural communities have access to global resources via the Internet. Elderly Americans have immediate access to loved ones and healthcare no matter where they reside.

Given its importance, countries have increasingly recognized access to the Internet as a human right.[3]

---

[3] Sadia Azim, *Why the Internet Is the New Public Utility*, INTERNET SOCIETY (June 25, 2025), https://pulse.internetsociety.org/blog/why-the-internet-is-the-new-public-utility ("Estonia led the way in 2000 by declaring Internet access a human right, while Finland became the first country in 2010 to make broadband a legal entitlement for every citizen;" "These precedents underscore a global shift toward treating Internet connectivity not as a luxury but as a critical infrastructure for participation in modern life.").

Access to the Internet remains a bipartisan issue even in the United States.[4]

In times of crisis, such as natural disasters, Internet access is a necessity. For example, following the events of September 11, 2001, Americans took to the Internet for updated information on the attacks and to provide support and assistance to victims, connect with others to seek relief, and reconnect with loved ones.[5] In the aftermath of Hurricane Katrina in 2005, New Orleans natives turned to the Internet for disaster relief communications and updates when cell phone towers and landline telephone services were knocked out.[6] Simply put, in times of crisis, the Internet provides the timely and accurate information that keeps people safe.

---

[4] *Trump Administration Invests $86 Million in Rural Broadband Service in Eight States*, U.S. DEP'T OF AGRICULTURE (June 24, 2020), https://www.usda.gov/about-usda/news/press-releases/2020/06/24/trump-administration-invests-86-million-rural-broadband-service-eight-states; *Biden-Harris Administration Announces Nearly &700 Million to Connect People in Remote and Rural Areas to High-Speed Internet*, U.S. DEP'T OF AGRICULTURE (Aug. 21, 2023), https://www.usda.gov/about-usda/news/press-releases/2023/08/21/biden-harris-administration-announces-nearly-700-million-connect-people-remote-and-rural-areas-high.

[5] *One year later: September 11 and the Internet*, PEW RESEARCH CTR. (Sept. 5, 2002), https://www.pewresearch.org/internet/2002/09/05/one-year-later-september-11-and-the-internet-2/#:~:text=The%20Web%20as%20a%20public,on%2046%25%20of%20such%20sites.

[6] Mary Madden, *Hurricane Katrina: In the face of disaster and chaos, people use the internet to coordinate relief*, PEW RESEARCH

B. The Negative Practical Ramifications of Internet Access Termination.

Because of the structure of the Internet, the Fourth Circuit's liability standard would punish not just an alleged infringer but potentially all the individuals who access the Internet through a public or shared Internet resource. Frequently, Internet access and devices are shared, whether within the same household, school, library, government building, or community center. And, due to cost, lack of reliability, and provider scarcity, many Americans have few or only one option for Internet access.

Importantly, an IP address does not identify a specific person. For most households, a single IP address assigned by an ISP is shared by every person and every device on the home network—including family members' laptops, guests' smartphones, smart TVs, and gaming consoles. From the outside, all their online activity appears to come from this single address, making it impossible to reliably determine which individual is responsible for any particular action.

This ambiguity is magnified in places like libraries, schools, apartment buildings, hotels, and coffee shops, where one IP address can serve dozens or even hundreds of different users in a single day. Furthermore, a home Wi-Fi network could be compromised or

---

CTR. (Sept. 7, 2005), https://www.pewresearch.org/internet/2005/09/07/hurricane-katrina-in-the-face-of-disaster-and-chaos-people-use-the-internet-to-coordinate-relief/.

used by a neighbor without the account holder's knowledge. Consequently, an allegation of infringement tied solely to an IP address is, at best, an accusation against a location, not a person. To hold the account holder strictly liable under these circumstances is to punish them for the untraceable actions of others, creating a form of collective punishment that harms innocent users who depend on that shared connection.

Because the Fourth Circuit's rule would incentivize ISPs to terminate Internet access to an entire account when possibly a single user is accused of infringement, given the interdependent web of Internet access—where numerous people rely on the same account—the Fourth Circuit's rule may result in ISPs cutting off access to the Internet not just for one allegedly bad actor but for an entire household or, in other cases, for thousands, if not tens of thousands, of Americans. This is because a single account with an ISP might include many users, and an ISP may not always be able to determine precisely which user allegedly committed infringing conduct nor whether the conduct was infringing. Rather than face financially crippling liability, the ISPs may find themselves terminating entire accounts.

Consider a city government initiative providing super-fast, free public Wi-Fi with hotspot structures that also offer free phone calls, device charging, and a tablet for access to city services, maps, and directions as a replacement for pay phones.

Under the Fourth Circuit's rule, an initiative that provides public Wi-Fi would be incentivized to monitor its users' access on its Wi-Fi to prevent infringement. Were they to learn of alleged infringement, the service could be required to take down free public Wi-Fi in one of the largest cities in the world, depriving numerous individuals of reliable Internet access, especially if it could not identify the particular infringing user. Alternatively, if the public Wi-Fi contracts with an ISP to provide its services, the ISP may be required to terminate the public Wi-Fi's access because it may not be able to identify the users on its network that are allegedly committing copyright infringement.

The potential impact would be even worse in rural areas. Local rural ISPs and community networks[7]—often providing service in rural areas and underserved communities—rely on ISPs to provide "backhaul" Internet access to community members, connecting them to the global Internet, the national and global public forum, allowing access to governmental benefits and facilitating education and employment.

Consider also the role of regional ISPs in towns and rural communities. For example, in Enfield, North Carolina, Wave 7 is a locally and family-run

---

[7] *Community networks: Internet for the people, by the people*, WORLD WIDE WEB FOUNDATION (Sept. 2, 2019), https://webfoundation.org/2019/09/community-networks-internet-for-the-people-by-the-people-the-web-untangled. ("Community networks deliver access to underserved areas with infrastructure built, managed and used by local communities, oftentimes in areas that are financially unattractive for mainstream [ISPs]").

ISP. Through a partnership between the Internet Society and a large financial institution, Wave 7 connects over 70 households in Enfield and runs on wireless technology to provide free Internet access to the local public library, as well as training and online services to the local residents.[8]

The Fourth Circuit's liability standard would likely require small ISPs like Wave 7 to expend significant resources on monitoring their consumers for potential copyright infringement in a manner that could run these ISPs out of business, depriving such rural communities of consistent, reliable access to the Internet.

Rural community and education networks may also have only one ISP option, and a single user's infringing use could deprive countless other users of the ability to access the Internet for non-infringing purposes.

Even within a contained network, like a single four-person household, the Fourth Circuit's rule likely would lead to unjust effects. Consider a hypothetical household where the Internet is a shared resource. In this household, one, if not both, of the parents depend on the Internet for remote work and income to support the family—but the teenager may be infringing a copyright. Should a child's errant choice to illegally download digital audio files deprive an entire household of Internet access, resulting in loss of work and income to the parent(s)? Even parents' attempts to

---

[8] *Community Networks Success Stories*, INTERNET SOCIETY (last visited Sept. 4, 2025), https://www.internetsociety.org/issues/community-networks/success-stories/.

gain in-person employment—when many job applications require applicants apply online—could easily be hindered as a result of the teenager's alleged infringement. Further, the family could be prevented from accessing telemedicine, online banking, and resources needed for school homework. The Fourth Circuit's rule could be crippling for families and communities alike.

The great majority of Internet subscribers share their accounts—from a single household to libraries, hotels, universities, military barracks, and even small regional Internet service providers. Most of the unresolved copyright infringement claims in this case are for these "shared access points" with dozens, hundreds, or even thousands of users.

Should a larger Internet service provider be required to cut off access for regional providers and entire communities that rely on them? Must university students lose access to the Internet to learn and complete their schoolwork because of an allegation that someone illegally downloaded copyrighted songs? Should a hotel or coffee shop lose Internet access for patrons because someone allegedly used the Wi-Fi network for copyright infringement? Can you imagine having your home Internet turned off and not being able to do your job or attend a virtual doctor's appointment because your child (or your neighbor's child), downloaded songs they shouldn't have, unbeknownst to you?

II. The Fourth Circuit's Liability Standard Does Not Align with How the Internet Operates.

The Fourth Circuit's liability standard also fails to fully account for how the Internet operates. The structures that allow the Internet to flourish require the participation of and interaction between a broad range of intermediaries. The Fourth Circuit's standard myopically focuses on a subscriber/user's interaction with an ISP. Because the standard does not consider the multi-faceted aspects of the Internet's operation, it will create uncertainty and will likely have a detrimental, chilling effect on the cooperation required to make the Internet as useful as it is.

A. Numerous Intermediaries Support the Internet's Functions.

The Internet is a "network of networks."[9] The Internet is made up of over 70,000 independent networks choosing to connect and collaborate.[10] Unlike some communications means, there is no central authority directing all traffic on the Internet. Rather, the interactions between the various networks are the results of numerous pieces of infrastructure, agreed specifications, and protocols.[11]

---

[9] *Internet Way of Networking; Defining Critical Properties of the Internet*, INTERNET SOCIETY (Sept. 9, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/.

[10] *Ibid.*

[11] *Ibid.*

The architecture of the Internet can be described as a "layered stack."[12] Each layer provides separate but integral components in order to provide Internet connection. There are many different intermediaries with different roles at each Internet layer. As well as many different intermediaries operating between levels, several different intermediaries operate on a single level.

Most relevant here, there are several different players that help transmit data over the network at the network level. As discussed above, ISPs provide users access to the Internet, but the ISP a user subscribes to is far from the only intermediary that allows a user to connect and interact with the broader Internet.

i. For example, when someone uses an application to find a website, any content flowing from the user's computer to the Internet is contained in a "packet."[13] The "header" of this packet contains the Internet Protocol ("IP") address of the computer on the network it is going to be sent to, as well as the unique

---

[12] Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME LAW REV. 815, 816 (2004).

[13] INTERNET SOCIETY, *Internet Way of Networking; Defining Critical Properties of the Internet*, *supra*.

IP address of the computer or device the packet is being sent from.[14] The information in the packet is generally encrypted and not immediately visible to the ISP transmitting the packet.[15]

ii. Figure 1 details the many intermediaries and their respective roles in connecting a user's computer to a given webhost.[16] As Figure 1 illustrates, a "last-mile ISP" connects users to the Internet, and a Domain Name System (DNS) resolver translates a domain name, like "internetsociety.org," into an IP address, like "104.18.16.166," that can be located on the Internet. Those ISPs connect with other networks, known as "transit providers," and those networks connect with hosting, cybersecurity, and content delivery networks that make Internet traffic faster and more secure.

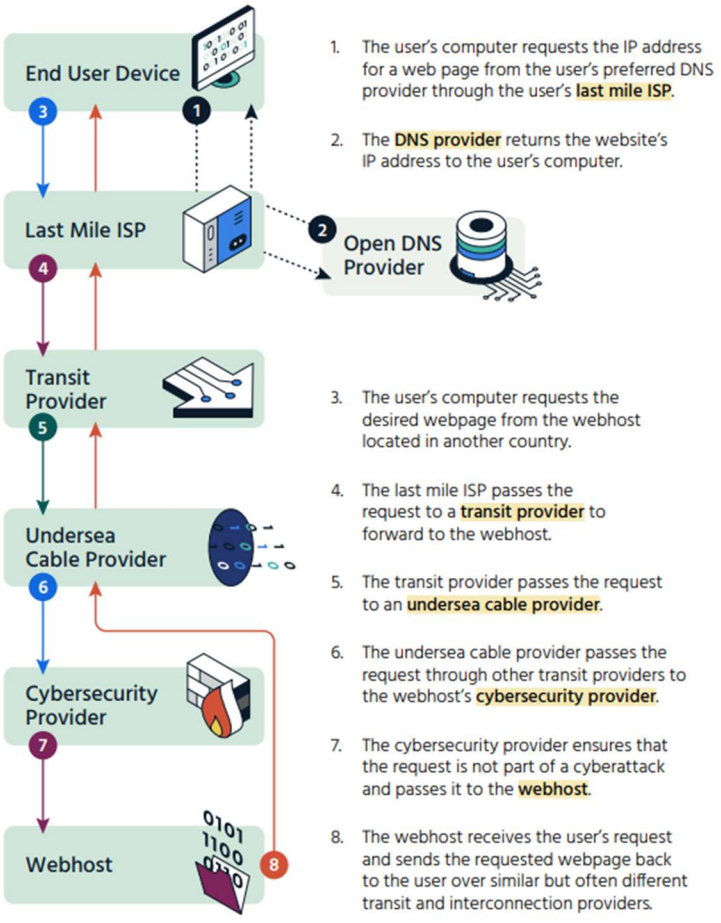
---

[14] *Ibid.*

[15] *Internet Way of Networking Use Case: Intermediary Liability, supra.*

[16] INTERNET SOCIETY, *A Policy Framework for Internet Intermediaries and Content,* at 20 (Jan. 2025), https://www.internetsociety.org/wp-content/uploads/2024/12/2025-Policy-Framework-Report-EN.pdf.

Figure - Providers of Intermediary Functions



Further, multiple intermediaries may be involved in delivering, receiving, and/or displaying the content, such as the Web Host in Figure 1. For example, a user sharing a link to a video might locate the link using a

browser and a search engine or Large Language Model, and then the user might share the link with other users via a social media app.

In sum, a single online interaction can involve and depend on the interaction of numerous intermediaries, not just ISPs. The collaboration between these various intermediaries is what allows the Internet to operate effectively worldwide.

B. The Fourth Circuit's Liability Standard Would be Difficult to Administer and Could Undermine the Operation of the Internet.

A reliable Internet depends on many different intermediaries being able to exchange traffic without regard to its contents. In this context, the Fourth Circuit's standard raises more questions than it answers about the scope of liability and in turn risks interfering with the Internet's architecture. By focusing on the relationship between the user and the ISP that the user pays for access, the Fourth Circuit raises questions about whether, and to what extent, *other* intermediaries that facilitate that user's access to the Internet could be liable. Is only the user's primary ISP liable? Or is any ISP or other intermediary that helps transmit that user's traffic liable, as long as they receive some warning about the user's alleged copyright infringement?

This uncertainty likely would have a destabilizing impact on Internet intermediaries. Smaller ISPs may be most impacted because they generally rely the most on larger ISPs and transit providers. Larger ISPs typically own the network infrastructure that

smaller ISPs purchase to facilitate their users' traffic, and they may be less inclined to allow smaller ISPs to connect to their networks. If larger ISPs do allow connections to smaller networks, they may require the ability to inspect the packets being sent. This could lead to a higher transit cost, which could make it unaffordable for smaller ISPs to operate and negatively impact Internet access (especially for lower income users).

To the extent ISPs and other transit providers believe that there is a greater risk of incurring copyright infringement liability by contracting with smaller ISPs from particular areas, those ISPs may choose not to allow traffic from those areas.

The Fourth Circuit's standard also raises perplexing issues regarding how to avoid liability. Would an upstream network provider that does not directly contract with the allegedly infringing user account, but rather contracts with an ISP serving that account, be required to cut off access to the downstream ISP's customer? If so, how is the ISP supposed to do this? If an individual's Internet access were terminated, how would the individual know which intermediary was responsible for that termination? Would an upstream network provider be required to cut off access to an entire downstream ISP if a rights holder alleged infringement by a downstream ISP's customer? What recourse would individuals denied Internet access have, and against which entity? These questions do not have easy, or readily apparent, answers.

III. The Fourth Circuit's Standard Comes with Serious Privacy and Security Risks.

The Fourth Circuit's rule would radically change an ISP's role from providing access to a communication service to being responsible for how its users use the service. This standard likely would incentivize ISPs to monitor and retain user data.

A. The Fourth Circuit's Liability Standard Would Radically Change an ISP's Role.

As discussed above, the primary role of an ISP has been—and should continue to be—to give users access to the Internet, not to monitor, police, or dictate what the users do on the Internet once they access it.[17] By making ISPs liable for user actions based on providing continued access, the Fourth Circuit's standard effectively requires ISPs to have a more active role in what their users do on the Internet. This more active role will incentivize ISPs to collect, analyze, and retain even more minute data on users' online activity, so that they can use that data to defend against further actions by copyright holders.

B. Requiring ISPs to Police Copyright Infringement Risks Users' Privacy and Security.

The Fourth Circuit's standard incentivizes ISPs to take serious steps to avoid copyright liability. ISPs

---

[17] *Internet service provider (ISP)*, LEGAL INF. INSTITUTE (last visited Sept. 4, 2025), https://www.law.cornell.edu/wex/internet_service_provider_(isp).

could start requiring users to provide additional identity verification when they use the Internet. The Fourth Circuit's rule may also incentivize ISPs to engage in expanded "deep packet inspection," a "computationally very intensive" process that "uses devices between the end user and the rest of the Internet that filter based on specific content, patterns, or application types."[18] Such actions would affect users broadly, not just users that might be infringing copyrights.

The Fourth Circuit's liability standard could also incentivize ISPs to reduce users' ability to use technologies that help protect their security and privacy, potentially impacting the use of Virtual Private Networks (VPNs), encrypted Domain Name System (DNS) lookups,[19] and other encrypted protocols (such as encrypted peer-to-peer communications), as well as other security tools, such as proxy servers. ISPs might fear that users could employ these tools to hide their copyright infringement, and that ISPs' continued allowance of those tools could be viewed as "willful blindness," which might lead ISPs to discourage their use, weaken their functionality, or, in some instances, outright ban these protective measures. These tools are used not only to keep Internet use private, but also

---

[18] *Internet Society Perspectives on Internet Content Blocking: An Overview*, INTERNET SOCIETY (Mar. 2017), https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlocking-Overview.pdf.

[19] *Encrypted DNS Factsheet*, INTERNET SOCIETY (May 2023), https://www.internetsociety.org/resources/doc/2023/fact-sheet-encrypted-dns/

for security purposes.[20] Weakening or banning their use could put users at greater risk of their data falling into the wrong hands.

One study found that users regard search and website viewing history "as among the top five most important pieces of personal information."[21] This makes sense. In our society, revolutionized by the Internet, people use the Internet in countless, sometimes very personal ways. Users who are not engaged in copyright infringement but believe that their activity is being monitored more closely and their data stored for longer periods of time may change how they use the Internet, including avoiding seeking information on sensitive topics that the users might not want others to know about.[22] And that could be very harmful: in Germany, researchers found that people were less

---

[20] Callum Tennant, *What to Look For in Choosing a VPN*, INTERNET SOCIETY (Oct. 24, 2019), https://www.internetsociety.org/blog/2019/10/what-to-look-for-when-choosing-a-vpn/ ("Any VPN worth its salt will offer the latest and most secure levels of encryption, a wide selection of strong protocols, and a range of additional security features including kill-switches, split-tunneling, and Tor compatibility.").

[21] FEDERAL TRADE COMMISSION, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[22] See Alex Matthews and Catherine E. Tucker, *Government Surveillance and Internet Search Behavior*, (Feb. 17, 2017), https://rb.gy/x7yc2p.

likely to seek help online for mental health challenges if they knew ISPs recorded their activity.[23]

The Fourth Circuit's rule likely would also increase security risks. Any time new data is mined and stored, there is a risk that this data could be compromised. ISPs have already experienced data breaches,[24] and there is no reason to think that this threat has lessened. Data breaches can have severe consequences for anyone, including identity theft and financial losses. When public officials are included in breaches, it creates national security concerns. For instance, President Trump's location data was identified and tracked using publicly available information, some of which was leaked from past data breaches.[25]

These privacy and security concerns are serious and weigh heavily against the Fourth Circuit's rule.

---

[23] *Data Retention Effectively Changes the Behavior of Citizens in Germany*, KREATIVRAUSCHEN (June 4, 2008), https://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/.

[24] Ravie Lakshmanan, *Over 4,000 ISP IPs Targeted in Brute-Force Attacks to Deploy Info Stealers and Cryptominers*, THE HACKER NEWS (Mar. 4, 2025), https://thehackernews.com/2025/03/over-4000-isp-networks-targeted-in.html.

[25] Stuart A. Thompson and Charlie Warzel, *How To Track President Trump*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

Put simply, the Fourth Circuit's standard raises significant risks for users' privacy and security on the Internet without dealing with those risks at all.[26]

CONCLUSION

For these reasons, the Internet Society respectfully requests that this Court reverse the Fourth Circuit.

Respectfully submitted,

RAECHEL KEAY ANGLIN
COUNSEL OF RECORD
BRENDAN J. ANDERSON
SPENSER B. JAENICHEN
MOSHE Y. KLEIN
MORGAN, LEWIS &
BOCKIUS LLP
1111 Pennsylvania
Avenue, N.W.
Washington, DC 20004
(202) 739-3000

SEPTEMBER 2025

[26] Many of these tools are used by both businesses and the government to enable remote employees to connect with the entities mainframes. See, e.g., *What is a business VPN? Business VPN use and limitations*, CLOUDFARE (last visited Sept. 4, 2025), https://www.cloudflare.com/learning/access-management/what-is-a-business-vpn/.