Congressional Research Service
Informing the legislative debate since 1914

Internet Architecture: A Layer-Based Analysis of Selected Internet Policy Issues

April 10, 2026

Congressional Research Service
https://crsreports.congress.gov
R48902

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48902

April 10, 2026

Ling Zhu
Specialist in Science and Technology Policy

Internet Architecture: A Layer-Based Analysis of Selected Internet Policy Issues

The internet is an information system of geographically distributed, interconnected computer networks (known as "a network of networks"). The term *internet architecture* generally refers to its fundamental design—a set of technical principles and protocols and the network structure of the internet. On the basis of the internet architecture model, the internet runs a wide variety of communication services that enable and facilitate information access, distribution, exchange, sharing, and creation.

Internet architecture can be represented by five hierarchical layers: the application layer, the transport layer, the network layer, the link layer, and the physical layer. Each layer contains *network protocols*, which are *common languages* or *conventions* that internet devices and equipment use to communicate with one another, control data transmission, and deliver an internet service. The application layer represents a variety of online applications available to end users (e.g., websites, email services, social media platforms, digital marketplaces, and online streaming services). In the application layer, users directly interact with the internet (e.g., through a web browser) and communicate with other users (e.g., through a social media mobile app). The transport layer is responsible for transporting data generated by internet applications between devices (e.g., sending a message from one user's laptop to another user's smartphone using an email application). This layer contains a small number of communication protocols. The most commonly used one is the Transmission Control Protocol (TCP), which ensures reliable end-to-end data transmission over the internet in the correct order and without errors, missing data, or duplicate data. The network layer is responsible for finding the most efficient path to route the data across any set of interconnected networks between the source device and the destination device, using Internet Protocol (IP) addresses. Because the internet uses TCP and IP collectively as its core communication protocols, the internet is also known as a "TCP/IP network." The link layer is responsible for moving network-layer data packets from one internet device to the next "neighbor" device through a wired (e.g., a cable) or wireless (e.g., Wi-Fi or 5G) link within a network. The physical layer represents a variety of transmission media used to physically establish the network link. These are the actual media that carry each single piece of data (i.e., a bit of 0 or 1) from one internet device to the next. These media include coaxial and fiber-optic cables for wired connectivity and radio spectrum for wireless connectivity.

Understanding the multilayer internet architecture model may be helpful for analyzing certain internet policy issues. To address the issue of unlawful content on the internet, for example, policymakers may target options at different internet layers. At the application layer, a law enforcement agency may seek to seize a consumer-facing website used for online illegal activities (e.g., offering to sell illegal products or carrying out online financial scams). At the transport layer, it is technically possible for an internet service provider to use certain network management techniques to inspect content being transmitted over its network and detect and block illegal content (e.g., copyright-infringement materials distributed by a peer-to-peer service). At the network layer, a federal agency may notify certain internet service operators of activities (e.g., selling drugs illegally) on a website under the operator's control. The operator could then take actions to render the website inaccessible. At the link and physical layers, some federal law enforcement agencies (e.g., the Federal Bureau of Prisons) receive a special temporary authority from the Federal Communications Commission to implement wireless signal jamming technologies to prevent cell phone usage and internet access by certain individuals in certain areas.

Cloud computing, an internet-based service model, provides an example of how knowledge of internet architecture can be useful for understanding and analyzing selected internet policy issues in the context of global artificial intelligence (AI) competition. For example, at the application layer, the concentration of the small number of service providers in the cloud computing market may raise questions regarding fair competition and access to computational resources for AI development. At the link/physical layer, the construction of AI data centers that host and deliver cloud computing services may raise questions about U.S. energy capacity and impacts of these data centers on nearby communities. Policymakers may also be concerned about safeguarding U.S.-based AI cloud services from foreign adversary access. Several pieces of legislation have been introduced to address this national security concern. If enacted, this legislation might be challenging to effectively enforce. At the application layer, targeted foreign entities might try to access the service through their subsidiaries or shell firms in other countries. At the TCP/IP layer, if a client's data are encrypted on the cloud server, it would be difficult to monitor any specific, malicious uses of cloud resources. At the link/physical layer, internet service providers could disconnect an internet backbone connection with specific countries. This approach, however, could result in a blanket block, cutting off all users within the country, not only those attempting to access restricted U.S. AI resources.

Contents

Figures

Contacts

The internet is an open and global computer network that connects billions of users and devices without a centralized governance mechanism. This interconnected digital communication system facilitates the free and secure flow of information and services across physical distances or geographical boundaries. *Internet policy* refers to the set of public policies, including laws, regulations, guidelines and standards, strategies and public initiatives, government programs, and stakeholder and community consensus, to govern and promote the use of the internet. Contemporary internet policy topics involve broadband (i.e., high-speed internet) deployment and access, use of various internet services and applications, data and content generated and shared over the internet, and a balance between U.S. competitiveness in technological innovation and the trust and safety of internet users. Congress has had long-standing interest in addressing a wide range of internet policy issues, including curbing access to harmful and illegal online content, protecting consumers' online data privacy, strengthening internet infrastructure to bridge the digital divide between communities with and without access to the internet, maintaining U.S. leadership in internet technologies and standards, and safeguarding online computing resources to achieve economic and national security goals.

The emergence and advancement of artificial intelligence (AI) is transforming the internet and poses new policy questions that Congress may consider. For example, *cloud computing*—an internet-based service that provides remote access to computational resources and applications—is playing an increasing role in hosting data, training AI models, and developing consumer-facing applications to support AI development and deployment. An emerging internet policy question is how to safeguard U.S.-based cloud computing services against malicious actors. Another example is the regulation of AI-generated content. An internet user can prompt cloud-based generative AI applications (e.g., an AI chatbot) to create text, images, audio, and video and then share that content over the internet. One central policy question is whether and how this new type of online content and its production and distribution should be regulated, particularly in the cases of nonconsensual intimate images and other unlawful content.

Internet architecture generally refers to the fundamental design of the internet—a set of technical principles and protocols and a network structure that collectively guides how the internet works. The internet was designed and operates based on a multilayer network architecture. Many internet policy issues derive from this network design and may be understood and analyzed when they are mapped into different layers of internet architecture.

This report first introduces the multilayer internet architecture model that describes conceptually how the internet works and data are transmitted. The report then illustrates how a series of internet policy issues are framed by internet architecture. Lastly, the report presents policy issues involving cloud computing, which has become a critical element of AI development and deployment. The report discusses selected cloud-related issues mapped to the multilayered internet architecture model and then focuses on the cross-cutting issue of safeguarding AI cloud services from foreign adversary access. The report also discusses legislative options Congress may consider and potential impacts of these options.

Internet Architecture

The internet is a vast information system of geographically distributed, interconnected computer networks (known as "a network of networks").[1] Internet architecture was established to support

[1] Robert Braden, ed., *Requirements for Internet Hosts—Communication Layers*, Internet Engineering Task Force (IETF), Request for Comments (RFC) 1122, October 1989, p. 7, https://www.rfc-editor.org/rfc/pdfrfc/rfc1122.txt.pdf. CRS uses the term *internet* in this report to refer to the global, public internet. The internet infrastructure also enables (continued...)

an interoperable and cost-effective communication network that was capable of transmitting data between end-to-end devices across different types of networks and physical media (e.g., wired and wireless connectivity) and supporting a variety of communications service (e.g., transmission of text, images, audio, and video).[2] The internet enables and facilitates information access, distribution, exchange, sharing, and creation beyond physical boundaries without a centralized control mechanism.[3]

End users may view the internet as a "black box." Delivery of information and content through various online applications installed on users' devices (e.g., desktops, laptops, tablets, and smartphones) relies on a complex system of protocols, standards, network hardware, and operating entities. While these components are largely invisible to users, many internet policy issues could be understood contextually and analyzed through the lens of the multilayer internet architecture model.

The internet architecture model—the conceptual structure of the internet—describes the basic design of how the internet works and how data are transmitted from one device to another over the internet.[4] While researchers have proposed various models with different numbers of layers, internet architecture is generally represented by five hierarchical layers (listed here from top to bottom):

- the application layer;
- the transport layer;
- the network layer;
- the link layer; and
- the physical layer.

The *application layer* is the top, end-user-facing layer of the internet. The *transport layer* and *network layer* determine how data generated by internet applications are transmitted from the originating device to the destination device through the internet. The *link layer* and *physical layer* are responsible for moving data using wired or wireless technologies across different physical media (see **Figure 1**).[5]

Each layer contains network *protocols*, which are common languages or conventions that internet devices and equipment use to communicate with one another, control data transmission, and deliver an internet service.[6] Computer and network hardware and software implement protocols

applications and services in closed local networks, for example, within an organization. Users generally access the public internet through commercial internet service providers (ISPs).

[2] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," Massachusetts Institute of Technology (MIT), March 14, 2013, https://web.mit.edu/6.033/www/papers/darpa.pdf.

[3] David D. Clark, *Designing an Internet* (MIT Press, 2018), p. 5. See also Brian E. Carpenter, ed., *Architectural Principles of the Internet*, Network Working Group, RFC 1958, Section 2.4, June 1996, p. 4, https://www.rfc-editor.org/rfc/pdfrfc/rfc1958.txt.pdf.

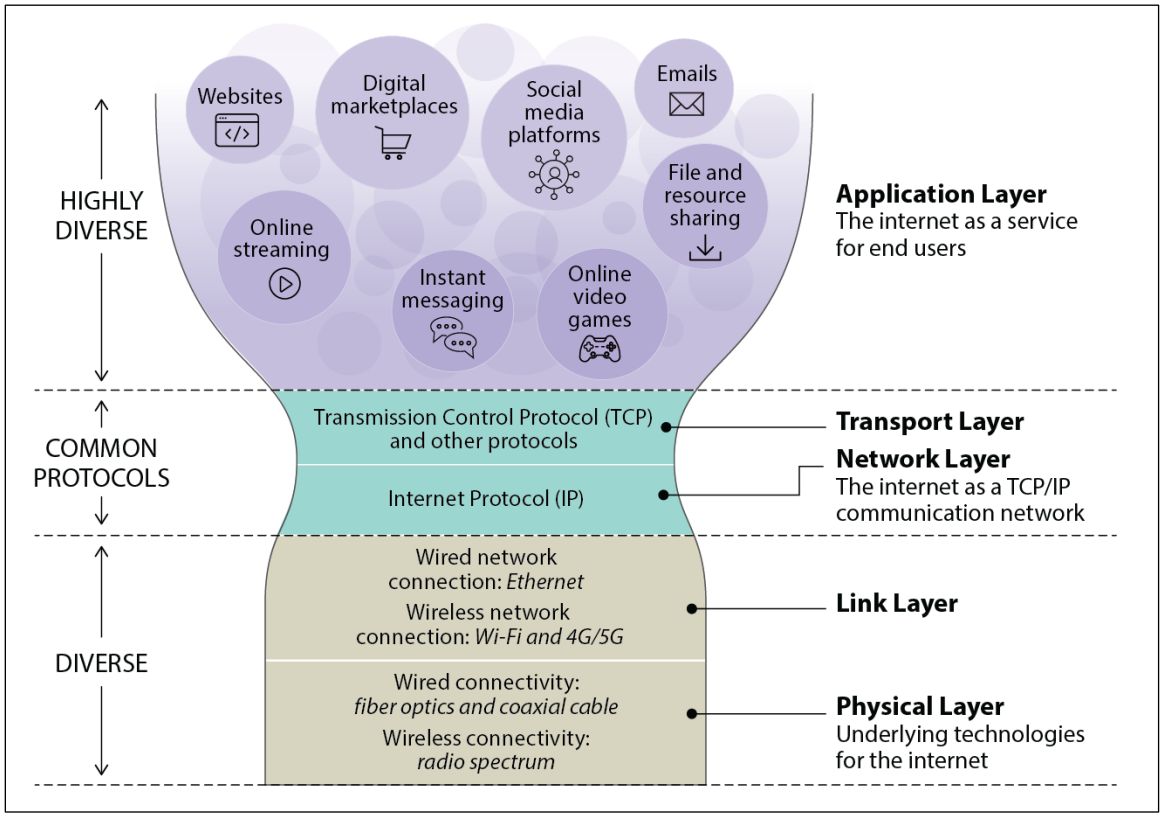
[4] Vinton G. Cerf and Edward Cain, "The DOD Internet Architecture Model," *Computer Networks*, vol. 7, no. 5 (October 1983), pp. 307-318. See also Braden, *Requirements for Internet Hosts—Communication Layers*, pp. 8-10.

[5] Scholars and practitioners have not reached a consensus on the number of layers in the internet architecture model, varying between three and seven. For the discussion of internet policy issues in this report, CRS uses the five-layer model adopted and described in Andrew S. Tanenbaum et al., *Computer Networks*, 6th ed. (Pearson Education, 2020), p. 67; James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. (Pearson Education, 2021), p. 50; and Christopher S. Yoo, "Protocol Layering and Internet Policy," *University of Pennsylvania Law Review*, vol. 161, no. 6 (May 2013), p. 1741.

[6] Cerf and Cain, "The DOD Internet Architecture Model," pp. 307-311. See also Clark, *Designing an Internet*, p. 8.

in each layer.[7] A particular internet service determines the set of protocols needed, each depending on the protocols used at lower layers.[8] The internet runs a wide variety of communication services across distinct, interconnected networks seamlessly based on this internet architecture model.[9]

Figure 1. The Multilayer Model of Internet Architecture



Source: CRS, adapted from Christopher S. Yoo, "Protocol Layering and Internet Policy," *University of Pennsylvania Law Review*, vol. 161, no. 6 (May 2013), p. 1751; and David D. Clark, *Designing an Internet* (MIT Press, 2018), p. 7.

Notes: This graphic shows internet architecture in an hourglass shape. The application layer is considered highly diverse, as the internet hosts billions of websites and millions of mobile apps that provide a variety of online services to end users. Despite their diversity, the majority of these applications rely on a few common protocols at the transport layer (e.g., TCP) and the network layer (e.g., IP). In the link and physical layers, a diverse array of wired and wireless connectivity technologies and physical media support data transmission over the internet.

Description of the Five Layers

The application layer represents a variety of online applications available to internet users. The application layer is where end users directly interact with the internet (e.g., through a web browser) and communicate with other users (e.g., through a social media mobile app). Examples of end-user applications include websites, email services, social media platforms, digital marketplaces, online streaming services, instant messaging tools, online video games, and file and

[7] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 49.

[8] Cerf and Cain, "The DOD Internet Architecture Model," pp. 307-311.

[9] Barbara van Schewick, *Internet Architecture and Innovation* (MIT Press, 2010), p. 84.

computing resource sharing.[10] Each type of application requires a particular communication protocol (i.e., a predefined set of rules and procedures that internet devices must follow to communicate with one another).[11] For example, to visit a website, an end user's web browser uses hypertext transfer protocol (HTTP) to send requests from the user's computer and receive information from the server hosting the website.

The transport layer is responsible for transporting data generated by internet applications between devices (e.g., sending a message from one user's laptop to another user's smartphone using an email application). This layer contains a small number of communication protocols. The major one is the Transmission Control Protocol (TCP), which is intended to ensure reliable, end-to-end data transmission over the internet in the correct order and without errors, missing data, or duplicate data.[12] TCP also breaks a long message into multiple, shorter segments for transmission and controls data transmission rates when the network is congested.[13]

The network layer (also referred to as the *internet layer*) is responsible for finding the most efficient path to route the data across any set of interconnected networks between the source device and the destination device.[14] The principal protocol at this layer is the Internet Protocol (IP). IP defines the basic unit of data carried at this layer as a *data packet*.[15] A data packet contains both content—a transport-layer segment (a portion of the original application-layer message)—and the routing information—the source's and the destination's unique identifiers (known as "IP addresses").[16] The function of the network layer is to deliver the complete set of data packets containing the application-layer message from its source to its destination.[17] This layer is also essential to link multiple networks together and create the internet as a network of networks.[18] Because the internet uses TCP and IP collectively as its core communication protocols, the internet is also known as a "TCP/IP, packet-switched network."[19]

The link layer (also referred to as the *data link layer*) is responsible for moving network-layer data packets from one internet device to the next neighboring device through a link within a network.[20] There are a variety of link-layer protocols, corresponding to specific types of network links.[21] The Standards Association of the Institute of Electrical and Electronics Engineers (IEEE) develops and maintains some major protocols. For example, the IEEE 802.3 Ethernet protocol is for a wired network link (e.g., through a fiber-optic cable) that connects two adjacent devices,[22] the IEEE 802.11 family of protocols supports Wi-Fi technology for a wireless network connection

[10] van Schewick, *Internet Architecture and Innovation,* pp. 87-88.

[11] Cerf and Cain, "The DOD Internet Architecture Model," p. 307.

[12] van Schewick, *Internet Architecture and Innovation*, p. 87.

[13] Kurose and Ross, *Computer Networking: A Top-Down Approach*, pp. 50-51.

[14] Tanenbaum et al., *Computer Networks*, p. 67. See also van Schewick, *Internet Architecture and Innovation*, p. 85.

[15] Tanenbaum et al., *Computer Networks*, p. 62.

[16] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 51.

[17] Tanenbaum et al., *Computer Networks*, p. 62.

[18] Tanenbaum et al., *Computer Networks*, p. 67.

[19] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 5. See also Lawrence Lessig, *Code: Version 2.0* (Basic Books, 2006), p. 43.

[20] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 51. See also van Schewick, *Internet Architecture and Innovation*, p. 84.

[21] Braden, *Requirements for Internet Hosts—Communication Layers*, p. 10.

[22] Braden, *Requirements for Internet Hosts—Communication Layers*, pp. 24-25. See also Institute of Electrical and Electronics Engineers (IEEE) Standards Association, *IEEE Standard for Ethernet*, IEEE 802.3-2022, July 29, 2022, https://standards.ieee.org/ieee/802.3/10422/.

within a local area network,[23] and protocols such as Radio Link Control are for a mobile network connection (e.g., through the fourth or fifth generation of mobile wireless technologies [i.e., 4G or 5G]).[24] A link layer protocol would encapsulate each data packet from the network layer into a data *frame*, which adds additional device-addressing information to the data packet. The protocol then moves the data frame across multiple network links along its route from the source device to the destination device.[25]

The physical layer represents a variety of transmission media used to physically establish the network link.[26] These are the actual media that carry each single piece of data (i.e., a bit of 0 or 1) from one internet device to the next.[27] These media include coaxial and fiber-optic cables for wired connectivity and radio spectrum for wireless connectivity. Some internet architecture models treat the physical layer as part of the link layer because the physical transmission medium determines the communication protocol used by the corresponding network connection at the link layer.[28] For example, a fiber-optic cable used to establish a network link between two internet devices determines that these devices will use the Ethernet protocol at the link layer.

Functionality and Standards

The functionality of one layer depends on the functionality provided by the lower layers.[29] Data to be transmitted from the source device are passed by one layer to the layer immediately below it, until the data reach the physical layer and are actually transmitted to the destination device. **Figure 2** illustrates an example of how a short text message would be transmitted from a source device (a user's laptop) to a destination device (a computer server).[30]

[23] van Schewick, *Internet Architecture and Innovation*, p. 83. See also IEEE Standards Association, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE 802.11-2024, April 28, 2025, https://standards.ieee.org/ieee/802.11/10548/.

[24] 3GPP, *5G; NG-RAN; Architecture Description*, Technical Specification 38.401, Version 18.2.0, Release 18, August 2024, pp. 18-21.

[25] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 51.

[26] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 52.

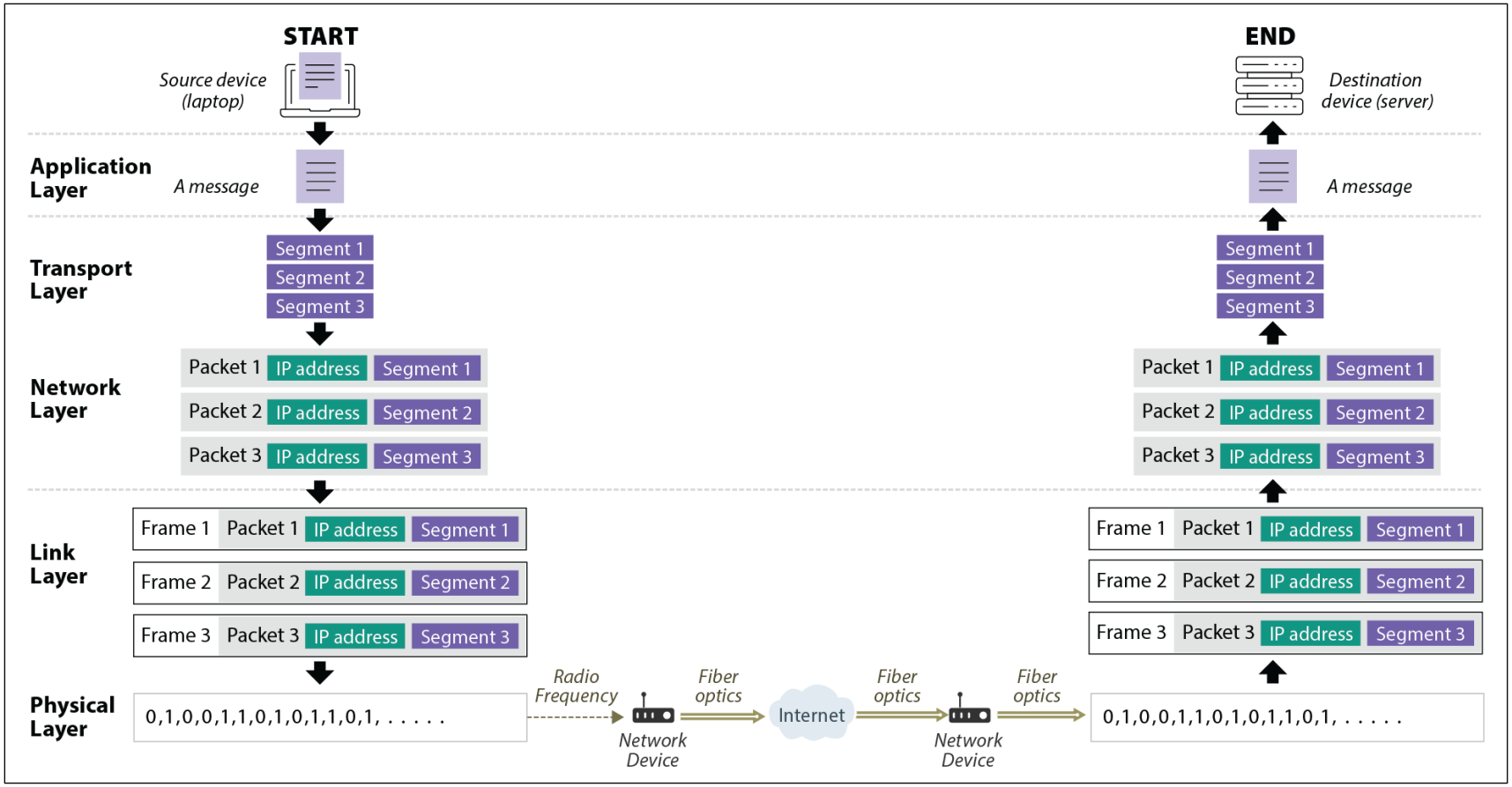
[27] Kurose and Ross, *Computer Networking: A Top-Down Approach*, p. 52.

[28] Braden, *Requirements for Internet Hosts—Communication Layers*, pp. 8-10.

[29] Tanenbaum et al., *Computer Networks*, p. 50.

[30] Tanenbaum et al., *Computer Networks*, p. 50.

Figure 2. An Example of Data Transmission Between Devices in the Five-Layer Internet Architecture Model



Source: CRS.

Notes: This graphic illustrates how information is transmitted at each layer using the example of a short text message sent from a laptop to a server. After the message is sent through an application (e.g., an instant messaging app) at the application layer, the message is broken into three segments by the Transmission Control Protocol (TCP) at the transport layer. At the network layer, the Internet Protocol (IP) encapsulates each segment into a data packet containing source and destination IP addresses. A link layer protocol then encapsulates each packet into a frame, adding additional data of device addresses. At the physical layer, each frame is transformed into a string of binary codes (0 and 1) to be transmitted over a physical medium. This particular example shows a laptop connected to the next network device using a

Wi-Fi router, which transmits the binary codes at the physical layer using radio frequency. The remainder of the network connections at the physical layer in this example use fiber-optic cables to transmit the binary codes via wired connections. When the binary codes reach the destination device of a server, they are reassembled into frames, packets, segments, and eventually the original message at each layer, in turn.

The core design of this architectural model emerged from a consensus among a group of researchers, primarily from U.S.-based institutions of higher education and the U.S. government, in the 1970s and 1980s.[31] Since the 1990s, several nongovernmental, multistakeholder communities have collaboratively developed and maintained voluntary, consensus-based standards, protocols, and technical specifications within the original internet architecture framework. These organizations include the Internet Engineering Task Force (IETF), the Internet Architecture Board, the Internet Research Task Force, the World Wide Web Consortium, and other specialized standards development bodies and projects.[32] The internet standards developed by these organizations are voluntarily adopted by users, network operators, and equipment vendors worldwide without requirements imposed by any government.[33] The IEFT, a major internet standards development organization, states that "technical concepts such as decentralized control ... resonate with the core values of the IETF community."[34] The organization commits to internet openness and fairness by not requiring membership for any individual or organization to participate in its technical working groups. These working groups represent the majority of the IETF's work, which is to produce technical documents to define how the internet works.[35]

The internet's core architecture has remained largely unchanged for decades despite advances in supporting information and communications technologies.[36] From internet connectivity using traditional dial-up phone lines to fiber-optic cables and 5G wireless technologies, and from interactive technologies collectively known as "Web 2.0" that enable user-generated content (e.g., social media platforms) to online chatbots that enable AI-generated content, the underlying design and structure of the internet has stayed the same. A wide range of internet services (including many consumer-facing AI applications) have been developed over time and run on this common, interoperable core network architecture.[37] By design, users can access these universally provided services no matter what devices they use, how they connect to the internet, or where they are, without limitations imposed by governments.[38]

A Layer-Based View of Internet Policy

The internet architecture model may provide a helpful approach to understand and analyze certain internet policy issues. Some researchers have suggested that understanding internet architecture is

[31] Barry M. Leiner et al., *A Brief History of the Internet*, Internet Society, 1997, https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

[32] Internet Society, "How Standard Setters Run the Internet," *Internet Governance* (blog), July 15, 2025, https://www.internetsociety.org/blog/2025/07/how-standard-setters-run-the-internet/.

[33] IETF, "Introduction to the IETF," https://www.ietf.org/about/introduction/. See also Internet Society, "How Standard Setters Run the Internet."

[34] IETF, "Introduction to the IETF."

[35] IETF, "Introduction to the IETF."

[36] See Randy Bush and David Meyer, *Some Internet Architectural Guidelines and Philosophy*, Network Working Group, RFC 3439, December 2002, https://www.rfc-editor.org/rfc/rfc3439.

[37] Clark, *Designing an Internet*, pp. 5-6.

[38] See U.S. Department of State (DOS), Bureau of Cyberspace and Digital Policy, "Declaration for the Future of the Internet," https://www.state.gov/declaration-for-the-future-of-the-internet.

essential for developing sound internet policy.[39] Several legal and policy scholars have called for developing an internet regulatory framework based on the multilayer model.[40]

To address the issue of unlawful content on the internet, for example, policymakers may consider options at different internet layers. At the application layer, a law enforcement agency may seek to seize a consumer-facing website used for online illegal activities (e.g., selling illegal products or carrying out online financial scams).[41] At the transport layer, an internet service provider (ISP) could use certain network management techniques to inspect content being transmitted over its network and detect and block illegal content (e.g., copyright-infringing materials distributed by a peer-to-peer service).[42] At the network layer, a federal agency may notify certain internet service operators (called *domain name registries*) of activities (e.g., selling drugs illegally) on a website under the operator's control. The operators may take actions to render the websites inaccessible.[43] At the link and physical layers, some federal law enforcement agencies (e.g., the Federal Bureau of Prisons) may receive a special temporary authorization from the Federal Communications Commission (FCC) to implement wireless signal jamming technologies to prevent cell phone usage and internet access by certain individuals in specified areas.[44]

The following subsections discuss selected internet policy issues at the application layer, the transport/network (TCP/IP) layer, and the link/physical layer of internet architecture.

Application Layer

In the last two decades, the internet has become more and more interactive, allowing users not only to consume but also to create and distribute a variety of digital content in multiple formats, such as text, images, audio, and video. The broad availability of internet applications enables virtual access to many services provided by the business, education, health care, and government sectors.

---

[39] See, for example, United Nations Conference on Trade and Development, *Information Economy Report 2006: The Development Perspective*, 2006, p. 281, https://unctad.org/system/files/official-document/sdteecb20061ch7_en.pdf.

[40] See, for example, Yoo, "Protocol Layering and Internet Policy," pp. 1707-1771; Lawrence B. Solum and Minn Chung, "The Layers Principle: Internet Architecture and the Law," *Notre Dame Law Review*, vol. 79, no. 3 (2004), pp. 815-948; and Kevin Werbach, "A Layered Model for Internet Policy," *Journal on Telecommunications and High Technology Law*, vol. 1, no. 1 (2002), pp. 37-68.

[41] See, for example, Department of Justice (DOJ), "Federal Authorities Seize Two Website Domains Used to Import Illegal Machine Gun Conversion Devices and Silencers from China," press release, January 13, 2026, https://www.justice.gov/usao-ma/pr/federal-authorities-seize-two-website-domains-used-import-illegal-machine-gun-conversion; and DOJ, "Justice Department Announces Seizure of Tai Chang Scam Compound Domain Used in Cryptocurrency Investment Fraud," press release, December 2, 2025, https://www.justice.gov/opa/pr/justice-department-announces-seizure-tai-chang-scam-compound-domain-used-cryptocurrency.

[42] See, for example, Milton Mueller et al., "Policing the Network: Using DPI for Copyright Enforcement," *Surveillance & Society*, vol. 9, no. 4 (June 2012), pp. 348-364, https://doi.org/10.24908/ss.v9i4.4340. *DPI* refers to deep packet inspection.

[43] See, for example, Jaisha Wray, "NTIA, FDA Pilot Program to Curb Access to Illegal Opioids Online Delivers Promising Results," *Domain Name System* (blog), National Telecommunications and Information Administration (NTIA), January 19, 2021, https://www.ntia.gov/blog/ntia-fda-pilot-program-curb-access-illegal-opioids-online-delivers-promising-results.

[44] See, for example, John Shaffer et al., *Cell Phone Jamming Technology for Contraband Interdiction in Correctional Settings*, Urban Institute, Research Report, June 2023, p. 2, https://www.urban.org/sites/default/files/2023-07/Cell%20Phone%20Jamming%20Technology%20for%20Contraband%20Interdiction%20in%20Correctional%20Settings.pdf. See also Federal Communications Commission, *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Third Further Notice of Proposed Rulemaking, GN Docket No. 13-111, September 9, 2025, https://docs.fcc.gov/public/attachments/DOC-414416A1.pdf.

Internet identifiers enable users to locate online resources and services (e.g., web pages, email services, and online file-hosting servers).[45] At the application layer, the primary identifier is the domain name of a website (e.g., crs.gov). Users and websites rely on the domain name system (DNS) to translate domain names into corresponding IP addresses. A website could be rendered inaccessible if the DNS disables the translation service. See the "Domain Name System" text box for an explanation of related terms.

Domain Name System

A *domain name* is a text-based unique identifier of a particular information resource located on the internet, known by internet users as a "website" (e.g., *crs.gov*).[46] The computer server that hosts the website and is attached to the internet has another numeric identifier called an "Internet Protocol (IP) address" (e.g., 140.147.15.67 for *crs.gov*).[47] For a user to connect to a website, the user's device must know the hosting web server's IP address.

The *domain name system* (DNS) is a distributed online database serving as the internet's "address book," which maps domain names to IP addresses.[48] With the DNS, users can simply enter a website's domain name in a web browser without knowing its IP address, even if the website is relocated to a different hosting server or cohosted by multiple servers, all with different IP addresses.[49] Users can thus easily navigate the internet using domain names, regardless of the IP addresses of websites' hosting servers.[50]

If the DNS service became unavailable, users' devices would not be able to locate and connect to a hosting web server, and users would experience difficulties accessing any website. Users might also be vulnerable to cyberattacks if they attempt to access a website using an unverified or spoofed IP address not provided by the DNS.

A *top-level domain* (TLD) is the rightmost textual segment preceded by the dot in a domain name. For example, the TLD of the domain name *crs.gov* is "gov." TLDs fall into two classes—generic TLDs, such as *.gov*, *.com*, *.org*, and *.edu*, and two-letter country-code TLDs, such as *.jp* (reserved for use in Japan) and *.ru* (reserved for use in Russia).[51] The textual segment to the left of the TLD represents a second-level domain that the owner of the website registers under that TLD. In *crs.gov*, "crs" is the second-level domain that CRS registers under the generic TLD of *.gov*.

A *registry* is an authoritative master database containing a record for each domain name registered under a particular TLD.[52] A *registry operator* is an organization that maintains a registry, including adding, deleting, or modifying a record of a domain name under the TLD.[53] For example, the U.S.-based company Verisign, Inc., is the

[45] Internet Governance Project, "What Is Internet Governance?," Georgia Institute of Technology School of Public Policy, 2026, https://www.internetgovernance.org/what-is-internet-governance/.

[46] Internet Corporation for Assigned Names and Numbers (ICANN), "ICANN Acronyms and Terms: Domain Name," https://www.icann.org/en/icann-acronyms-and-terms/domain-name-en.

[47] ICANN, "ICANN Acronyms and Terms: Internet Protocol Address (IP Address)," https://www.icann.org/en/icann-acronyms-and-terms/internet-protocol-address-en.

[48] ICANN, "ICANN Acronyms and Terms: Domain Name System (DNS)," https://www.icann.org/en/icann-acronyms-and-terms/domain-name-system-en.

[49] Tanenbaum et al., *Computer Networks*, pp. 613-614.

[50] Tanenbaum et al., *Computer Networks*, p. 614.

[51] ICANN, "ICANN Acronyms and Terms: Top-Level Domain (TLD)," https://www.icann.org/en/icann-acronyms-and-terms/top-level-domain-en. The two-letter country codes are defined in International Organization for Standardization (ISO), *ISO 3166-1:2020(en) Codes for the Representation of Names of Countries and Their Subdivisions – Part 1: Country Code*, 2020; the codes are available on ISO's online browsing platform at https://www.iso.org/obp/ui/#search/code/.

[52] ICANN, "ICANN Acronyms and Terms: Registry," https://www.icann.org/en/icann-acronyms-and-terms/registry-en.

[53] ICANN, "ICANN Acronyms and Terms: Registry Operator (RO)," https://www.icann.org/en/icann-acronyms-and-terms/registry-operator-en.

registry operator for the *.com* and *.net* generic TLDs.[54] The DNS relies on the TLD registry and servers operated by the registry operator to resolve a website's domain name under that TLD into the corresponding IP address.[55]

Until late 2016, management of the DNS and related internet governance matters were within the purview of the U.S. Department of Commerce (DOC).[56] In January 2017, DOC completed a decade-long process to transfer the stewardship from the U.S. government to a multistakeholder community led by the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization headquartered in California.[57] ICANN coordinates and delegates administrative responsibilities (e.g., domain name registrations) to independent organizations of registry operators around the world.[58] For example, U.S.-based Verisign, Inc., is the registry operator for the ".com" top-level domain.[59] ICANN's bylaws state that the organization "does not hold any governmentally authorized regulatory authority" and "shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide."[60] In March 2022, ICANN denied the Ukrainian government's request to disconnect domains associated with Russia from the internet, saying that "ICANN does not control internet access or content."[61]

The evolution of the DNS governance model reflects the long-held positions of the U.S. government that the internet is an open, global, interoperable, and decentralized network of networks and that the principles of internet policy are to (1) enable the private sector to develop and offer innovative internet services and (2) adopt a bottom-up, multistakeholder policymaking approach, which incorporates views and expertise of the technical community, industry, civil society, and academia, alongside governments and public authorities.[62]

The private-sector-led governance mechanism makes it more challenging for the U.S. government to directly regulate access to certain harmful or illegal online content. Some federal agencies have taken approaches, such as voluntary programs or legal proceedings, to curb access to certain

[54] For example, see ICANN, ".com Registry Agreement," December 1, 2012, https://www.icann.org/en/registry-agreements/com/com-registry-agreement-1-12-2012-en.

[55] ICANN, "ICANN Acronyms and Terms: Registry Operator (RO)."

[56] See U.S. Department of Commerce (DOC), "Request for Comments on the Registration and Administration of Internet Domain Names," 62 *Federal Register* 35896, July 2, 1997, https://www.govinfo.gov/content/pkg/FR-1997-07-02/pdf/97-17215.pdf. See also NTIA, "Exchange of Letters," January 6, 2017, https://www.ntia.gov/files/ntia/publications/ntia-icann_affirmation_of_commitments_01062017.pdf.

[57] See letter from Lawrence E. Strickling, DOC's Assistant Secretary for Communication and Information, to Stephen D. Crocker, ICANN's Chairman of the Board of Directors, January 6, 2017, https://www.ntia.gov/files/ntia/publications/ntia-icann_affirmation_of_commitments_01062017.pdf.

[58] See, for example, ICANN, "Accredited Registrars," https://www.icann.org/en/contracted-parties/accredited-registrars/list-of-accredited-registrars.

[59] ICANN, ".com Registry Agreement."

[60] See Section 1.1(c) of ICANN, "Bylaws for Internet Corporation for Assigned Names and Numbers: A California Nonprofit Public-Benefit Corporation," as amended January 9, 2025, https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[61] Letter from Goran Marby, ICANN's President and CEO, to Mykhailo Fedorov, Ukraine's Deputy Prime Minister, March 2, 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf.

[62] See Bureau of Cyberspace and Digital Policy, "Declaration for the Future of the Internet"; Roxana Radu, "Privatization and Globalization of the Internet," in *Negotiating Internet Governance* (Oxford University Press, 2019), pp. 75-112; Mehan Grosse, "Public Goods and Private Interests: Setting the Table for the Commercial Internet in the 1990s," *Critical Studies in Media Communication*, vol. 38, no. 5 (2021), pp. 408-422; NTIA, "ICANN77 Policy Forum Governmental Advisory Committee," https://www.ntia.gov/speechtestimony/2023/icann77-policy-forum-governmental-advisory-committee; and Clinton Administration, "The Framework for Global Electronic Commerce," July 1997, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

websites involving illegal activities. For example, federal agencies have taken action against websites used for making illegal online opioid sales,[63] providing illegal access to copyrighted materials,[64] and posting nonconsensual intimate images and personal information,[65] as well as websites used by foreign adversaries for malicious cyber activities.[66] The efficacy of these actions may depend on the registry operators that manage domain names associated with the websites. These domain name operators, not ICANN, are able to restrict access to websites.

Legislation targeting domain name operations at the application layer has been introduced in Congress to address unlawful online activities and content. For example, in the 118th Congress, the Domain Reform for Unlawful Drug Sellers Act (DRUGS Act; S. 4108) would have amended the Federal Food, Drug, and Cosmetic Act (FD&C Act, as amended; codified at 21 U.S.C. §§301 et seq.) by adding a new Section 524C "Domain Names Used to Facilitate the Online Sale of Drugs Illegally." The new section would have required a top-level domain name operator to "disable the functionality" of a domain name within seven days of receipt of a notice from a "trusted notifier" that the domain name "is used to facilitate the online sale of drugs illegally and … under the control of" the operator.[67] If S. 4108 had been enacted, a domain name operator that failed to comply with the new Section 524C would have been subject to legal proceedings and penalties provided for "prohibited acts" under Section 301 of the FD&C Act.[68] In the 119th Congress, the Foreign Anti-Digital Piracy Act (H.R. 791) would amend the Copyright Act of 1976 (codified at Title 17 of the *U.S. Code*) by allowing a U.S. District Court to issue a blocking order under certain circumstances to direct covered "service providers" to "take reasonable and technically feasible measures to prevent users … from accessing the foreign website or online service" engaging in certain copyright infringement activities. The "service provider" covered in the legislation would include certain providers of "public domain name resolution services ... that are accessible to the general public."

Transport/Network (TCP/IP) Layer

According to some scholars who were involved in designing the internet architecture in the 1970s and 1980s, the internet was not designed to sufficiently address subsequent public policy concerns resulting from the proliferation of internet adoption and use since the 1990s.[69] These concerns are often in tension with one another, one example being the balance between protecting end users' privacy with the legitimate monitoring or interception of disruptive or illegal online activities.[70] The scholars involved in the original design argued that it was not clear how the

[63] Wray, "NTIA, FDA Pilot Program to Curb Access to Illegal Opioids Online Delivers Promising Results."

[64] DOJ, "United States Seizes Six Websites Providing Illegal Access to Copyrighted Music," press release, June 27, 2022, https://www.justice.gov/opa/pr/united-states-seizes-six-websites-providing-illegal-access-copyrighted-music.

[65] Federal Trade Commission (FTC), "FTC, Nevada Obtain Order Permanently Shutting Down Revenge Porn Site MyEx," press release, June 22, 2018, https://www.ftc.gov/news-events/news/press-releases/2018/06/ftc-nevada-obtain-order-permanently-shutting-down-revenge-porn-site-myex.

[66] DOJ, "Justice Department Disrupts Russian Intelligence Spear-Phishing Efforts," press release, October 3, 2024, https://www.justice.gov/opa/pr/justice-department-disrupts-russian-intelligence-spear-phishing-efforts.

[67] Section 2(a) of S. 4108 (118th Congress). In S. 4108, the term *trusted notifier* includes federal agencies—the Food and Drug Administration (FDA), DOJ (including the Drug Enforcement Administration [DEA]), and the Department of Homeland Security—as well as a state attorney general; a state board of pharmacy; certain nonprofit organizations; any entity associated with the FDA or DEA, which share information related to online drug sales; and certain entities identified by the FDA as trusted notifiers.

[68] Section 2(b) of S. 4108.

[69] Clark, "The Design Philosophy of the DARPA Internet Protocols."

[70] Clark, "The Design Philosophy of the DARPA Internet Protocols," p. 27.

internet architecture would materially affect how the internet could be regulated.[71] For example, the IP at the network layer requires any internet-connected device to be assigned a unique IP address. Using IP addresses, the internet could determine how to efficiently route data between an end user's device and a computer server operated by an online interactive service provider. This internet "addressing mechanism" has policy implications for data privacy. Unless using a masking technology such as a virtual private network (VPN), the user would inevitably reveal the digital identity of the device (i.e., the IP address) to the service provider, enabling the provider or third parties (e.g., data brokers) to track the device's online activities and the device's physical location.[72] It is technically infeasible to prevent a company's computer server from collecting IP address data from its consumers.

The IP addressing mechanism and many other technical standards at the transport and network layers are governed by a multistakeholder community called IETF. IETF develops these voluntary standards and publishes technical documentation as requests for comments (RFCs), which describe technical specifications of the internet.[73] For example, RFC 9293 "describes the TCP segment format, generation, and processing rules that are to be implemented in code."[74] RFC 791 specifies the IP.[75] There is another internet standard development organization called the International Telecommunication Union (ITU). ITU is the United Nations' specialized agency for information and communications technology, with 194 member states and more than 1,000 member organizations.[76] ITU's Telecommunication Standardization Section (ITU-T) develops "international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of information and communication technologies."[77] Many of ITU-T's standards have focused on the operation of the physical connectivity of telecommunication networks, such as wireless radio spectrum and broadband cables.[78] Telecommunication networks support the transmission of voice and data, including over the internet. As for now, the IETF, not ITU, has largely set internet standards, particularly at the TCP/IP layer, that are voluntarily adopted by users and developers.

In September 2019, the Chinese company Huawei Technologies Co., Ltd., submitted a set of proposals (known as "New IP") to an advisory group of ITU-T.[79] The New IP proposal called for the development of "new network protocols and architectures 'by extending and redesigning the traditional IP' to support new services for a 'new internet' by 2030."[80] Huawei reportedly claimed in its proposal that the existing TCP/IP standards were "unstable" and "vastly insufficient" to support the requirements of emerging technologies by 2030, including those for self-driving cars, the ubiquitous Internet of Things, and the holoportation technology that would enable 3D models

[71] Clark, "The Design Philosophy of the DARPA Internet Protocols," p. 27.

[72] See CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu.

[73] IETF, "Introduction to the IETF."

[74] Wesley M. Eddy, ed., *Transmission Control Protocol (TCP)*, IETF, STD 7, RFC 9293, August 2022, https://doi.org/10.17487/RFC9293.

[75] Jon Postel, ed., *Internet Protocol*, IETF, STD 5, RFC 791, September 1981, https://doi.org/10.17487/RFC0791.

[76] See ITU, "About the International Telecommunication Union (ITU)," https://www.itu.int/en/about/Pages/default.aspx.

[77] ITU, "ITU-T in Brief," https://www.itu.int/en/ITU-T/about/Pages/default.aspx.

[78] ITU, "ITU-T Recommendations," https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx.

[79] Internet Society, "Huawei's 'New IP' Proposal – Frequently Asked Questions," February 22, 2022, https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/.

[80] Internet Society, "Huawei's 'New IP' Proposal – Frequently Asked Questions."

of objects and users to be transmitted over the internet in real time.[81] The proposal submitted by the Chinese company reportedly gained the support of Russia but caused concerns among some other countries, including the United States, which worried that the new system "would splinter the global internet and give state-run internet service providers granular control over citizens' internet use."[82] Concerns about the proposal included the lack of interoperability with the existing global internet architecture, incompatibility with the existing IP addressing schemes developed by the IETF, and unnecessary functionalities reported to be built into the internet, such as "tracking features" and a "shut up command," "where a central point in the network could effectively cut off communication to or from a particular address."[83]

While discussion of the New IP proposal at ITU-T was discontinued, countries such as China and Russia have continued to advocate for a top-down, government-led model for internet standard setting on the ITU platform. This proposed model is intended to replace the bottom-up, multistakeholder, and consensus-based model currently used by the IETF and other standards development organizations.[84] With some ITU members' support, Russia submitted a proposal to ITU in January 2021 to discuss a new "global governance system" for internet resources and "possible ways to overcome the challenges associated with dependence on the decisions of one national administration for further building an independent [and] democratic" internet governance system.[85] In February 2026, the U.S. Assistant Secretary of Commerce for Communications and Information made the following remarks regarding ITU and internet standard setting:

> [W]e must remain vigilant against efforts to transform the ITU into a centralized 'internet regulator.' Certain member states have advanced proposals to convert the ITU's mandate from technical coordination toward a broader regulatory or governance role over the internet … This would shift decision-making authority from decentralized private sector innovators and engineers to a forum where many member states reject free expression as a governing principle.[86]

Congress has enacted legislation to address concerns involving technical standards setting. Section 10245 of the CHIPS and Science Act (Division B of P.L. 117-167) requires the Director of the National Institute of Standards and Technology (NIST) to "lead information exchange and coordination among Federal agencies and communications from Federal agencies to the private sector … to ensure effective Federal engagement in the development and use of international technical standards" and consider "support for activities to encourage the adoption of technical standards developed in the United States to be adopted by international standards organizations." Some Members introduced legislation in the 118th and 119th Congresses to address similar concerns. The Realizing Economic and Strategic Objectives While Leading with Values and Engagement (RESOLVE) Act of 2024 (S. 5491, 118th Congress) would have directed the President to establish an interagency working group (chaired by the Secretary of Commerce and vice-chaired by the Secretary of State) "to provide assistance and technical expertise to enhance

[81] Anna Gross and Madhumita Murgia, "China and Huawei Propose Reinvention of the Internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2. See also Microsoft Research, "What Is Holoportation?," https://www.microsoft.com/en-us/research/project/holoportation-3/.

[82] Gross and Murgia, "China and Huawei Propose Reinvention of the Internet."

[83] Gross and Murgia, "China and Huawei Propose Reinvention of the Internet." See also Internet Society, "Huawei's 'New IP' Proposal – Frequently Asked Questions."

[84] Internet Society, "Huawei's 'New IP' Proposal – Frequently Asked Questions."

[85] ITU, "Report of the Fifteenth Meeting of the Council Working Group on International Internet-Related Public Policy Issues (CWG-Internet)," January 28, 2021, pp. 3-4, https://www.itu.int/md/S21-RCLINTPOL15-C-0012/en.

[86] NTIA, "Remarks of Assistant Secretary Arielle Roth at The Media Institute Communications Forum Luncheon Series," February 25, 2026, https://www.ntia.gov/speech/testimony/2026/remarks-assistant-secretary-arielle-roth-media-institute-communications-forum-luncheon-series.

the representation and leadership of the United States at international bodies that set standards for equipment, systems, software, and virtually defined networks that support 5th and future generation mobile telecommunications systems and infrastructure, such as [ITU].” The Securing Global Telecommunications Act (H.R. 4506, 119th Congress) would direct the Secretary of State to report on “Russian and Chinese strategies and efforts (1) to expand the mandate of [ITU] to cover internet governance policy; and (2) to advance other actions favorable to authoritarian interests and/or hostile to fair, industry-led processes.”

Link/Physical Layer

One example of an internet policy issue at the link/physical layer is federal support for internet infrastructure deployment. Congress has tasked federal agencies such as the National Telecommunications and Information Administration (NTIA), the FCC, and the U.S. Department of Agriculture with administering a variety of federal programs to facilitate the deployment of high-speed, reliable, and affordable internet service throughout the country. For example, in Section 60102 of the Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58), Congress directed the establishment of the Broadband Equity, Access, and Deployment (BEAD) Program and appropriated $42.45 billion for the program. NTIA is tasked with making BEAD grants to 50 states, the District of Columbia, Puerto Rico, and four other territories to fund broadband projects. An internet network to be built with BEAD funding must be capable of providing broadband service with (1) at least 100 megabits per second (Mbps) for download and 20 Mbps for upload; (2) a low network latency enabling real-time, interactive internet applications; and (3) a low network outage rate (less than 48 hours over any 365-day period).[87]

One debate surrounding the BEAD Program is about which broadband connectivity technologies at the physical layer of the internet architecture are capable of providing BEAD-qualified broadband service to end users. These technologies could include end-to-end fiber cable from network facilities to each end-user’s premises, low Earth orbit (LEO) satellites connecting end-user devices to the internet, and wireless radio antennas broadcasting network signals to a nearby end user’s fixed location (called “fixed wireless”). Experts have generally agreed that no single broadband connectivity technology is universally suitable for all locations, considering factors such as network performance (e.g., internet speed, latency, and reliability), near- and long-term deployment and operational costs, and technical and regulatory requirements (e.g., network architecture and permitting processes). For example, among all commercially available technologies, fiber supports the highest speed ranges at the gigabit level,[88] though its initial deployment could be labor and capital intensive and involve various permitting processes (e.g., statutory environmental review and permits to access rights of way on federal, state, or local land).[89] LEO satellite broadband service is relatively new to the commercial market, and its technology is still evolving. Its network performance is more susceptible to weather and limited by the coverage of a satellite constellation.[90] With an existing constellation, satellites could connect end users living in remote or rural locations to the internet with relatively lower effort than fiber, requiring only terminal equipment such as a satellite antenna (also known as a “dish”).[91] Lastly, fixed wireless technologies are “effective in delivering short-range service to

[87] 47 U.S.C. §1702(h)(4)(A)(i).

[88] One gigabit per second (Gbps) is approximately equal to 1,000 megabits per second (Mbps).

[89] See NTIA, “Permitting,” *BroadbandUSA*, https://broadbandusa.ntia.gov/assistance/permitting.

[90] Mateusz Kaczmarek, “Satellite vs Fiber Internet: The 2025 Latency & Bandwidth Showdown,” *TechStock²*, June 4, 2025, https://ts2.tech/en/satellite-vs-fiber-internet-the-2025-latency-bandwidth-showdown/.

[91] CRS Report R46896, *Low Earth Orbit Satellites: Potential to Address the Broadband Digital Divide*, by Colby Leigh Pechtol.

closely grouped households in urban and suburban settings" but may not be suitable for geographically dispersed locations such as rural communities.[92] The speed and capacity of fixed wireless technologies is limited by the available bandwidth of assigned wireless spectrum. Similar to satellites, the performance and coverage of a fixed wireless network is "adversely affected by line-of-sight obstructions (including buildings and seasonal foliage) and weather."[93]

The latest NTIA guidelines adopt a technology-neutral approach, permitting states to select from any link/physical layer connectivity technology that meets the performance requirements set forth in the IIJA.[94]

Policy Issues Involving Cloud Computing

This section uses the example of cloud computing to illustrate how the internet architecture model can be applied to understand and analyze some selected policy issues. As the cost and complexity of data processing, storage, and security increases, cloud computing has become a common information technology (IT) solution adopted by many public and private organizations, especially those with limited resources. In recent years, cloud computing has become a major approach to powering AI development, enabling many organizations to engage in AI development without significant investments in hardware and software.[95]

While the term *cloud* represents the internet-based service model in a broad, undifferentiated way, policymakers could understand cloud-related policy issues in terms of internet architecture layers. By using the layered framework, policymakers could identify which entities operate, control, or bear responsibilities for cloud computing services at different layers, what the possible policy concerns are, and where regulation may be necessary and feasible. For an overview of cloud computing technology, see the "Cloud Computing" text box.

Cloud Computing

Cloud computing is an internet-based service model that allows users to remotely access a shared pool of computational resources, such as data processing chips, data storage devices, databases, software, and networks, as well as other computing services, such as business applications, data analytics, and machine learning.[96] With cloud computing service, users do not need to acquire, install, deploy, manage, or perform updates of particular hardware, software, data, networks, or services for their on-premises information systems. Instead, a cloud computing service provider delivers these computing resources, capabilities, and services virtually to users on demand, mostly over internet-based networks, or the *cloud*.[97] Cloud computing customers generally pay based on

[92] Andrew Afflerbach, *Fixed Wireless Technologies and Their Suitability for Broadband Delivery*, Benton Institute for Broadband and Society, June 2022, p. 2, https://www.benton.org/sites/default/files/FixedWireless.pdf.

[93] Afflerbach, *Fixed Wireless Technologies and Their Suitability for Broadband Delivery*, p. 1.

[94] NTIA, *BEAD Restructuring Policy Notice*, June 6, 2025, pp. 8-13, https://www.ntia.gov/sites/default/files/2025-06/bead-restructuring-policy-notice.pdf.

[95] Jeffrey Erickson, "The Role and Benefits of AI in Cloud Computing," *Oracle Cloud Infrastructure*, June 21, 2024, https://www.oracle.com/artificial-intelligence/ai-cloud-computing/.

[96] For more information on cloud computing's definition and its "essential characteristics," "service models," and "deployment models," see Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST), NIST Special Publication 800-145, September 2011, p. 2, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[97] An example of a basic cloud computing service is web-based email, in which users log into their online accounts to receive, compose, send, store, and organize emails. All functions are delivered to the user from the email service provider's server via the internet. Even if the user uses a different device at a different location, the user can still access the same online email service, so long as the user has internet access.

the information technology (IT) services they use but do not assume initial investment costs or direct operating and maintenance costs of the services.[98]

Cloud computing service offers computing resources and capabilities to customers with flexibility and scalability through the service provider's cloud infrastructure of hardware, software, and networks.[99] There are three typical service models:

- *software as a service* (SaaS), which enables customers to remotely run software applications hosted on the service provider's cloud infrastructure;
- *platform as a service* (PaaS), which enables customers to develop, deploy, and manage their own web-based or mobile applications using the software development environment and infrastructure supported by the service provider; and
- *infrastructure as a service* (IaaS), which enables customers to access and use data processing, storage, networks, and other computing resources provided by the cloud computing service.[100]

A Layer-Based Analysis of Cloud Computing for AI

Cloud computing services enable AI developers and users to access computational resources hosted in geographically distributed data centers.[101] Cloud computing plays an important role in AI development and deployment. For example, datasets used to train AI models could be stored on a cloud computing server; AI model training could be conducted on a cloud computing server; a trained AI model could be stored on the server for deployment; based on the AI model, a variety of online applications could be developed using a cloud computing service; and end users could remotely access those AI-enabled applications and prompt the AI model to generate content.

At the application layer of the internet architecture model, large-scale cloud service providers (CSPs; also known as "hyperscalers") offer end users services ranging from hosting data and computing hardware and software to training models and deploying AI-powered applications. The cloud service market is currently dominated by a relatively small number of hyperscalers. AI development requires intensive computational work on large amounts of data. Many AI developers rely on cloud computing services to access computational resources (e.g., by renting data processing chips and large storage devices).[102] An industry survey in 2023 reported that over 50% of professional AI developers have used Amazon's cloud computing platform Amazon Web Services (AWS), followed by Microsoft Azure at 28% and Google Cloud at 24%.[103] For example, OpenAI has used Microsoft Azure to power its workloads, including research, development, and customer-facing services.[104] Using rental prices charged by major CSPs for accessing computing hardware and processing data, researchers estimated that training costs of three leading AI models

[98] Erickson, "The Role and Benefits of AI in Cloud Computing."

[99] Mell and Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, p. 2.

[100] Mell and Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, pp. 2-3.

[101] CRS In Focus IF12899, *Data Centers and Cloud Computing: Information Technology Infrastructure for Artificial Intelligence*, by Ling Zhu.

[102] Nestor Maslej et al., "Artificial Intelligence Index Report 2024," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, April 2024, p. 270, https://hai.stanford.edu/assets/files/hai_ai-index-report-2024-smaller2.pdf. See also Megha Shrivastava, "The China-US Tech War Comes to the Cloud," *The Diplomat*, February 7, 2024, https://thediplomat.com/2024/02/the-china-us-tech-war-comes-to-the-cloud/.

[103] Maslej et al., "Artificial Intelligence Index Report 2024," p. 270.

[104] Microsoft Corporate Blogs, "Microsoft and OpenAI Extend Partnership," January 23, 2023, https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/.

ranged from $41 million to $170 million in 2024.[105] A research report estimated that total enterprise spending on cloud service worldwide in 2025 was $419 billion, a 30% increase from 2024.[106] The spending growth has been largely driven by AI-specific service demand since 2022. The report also noted that the three largest U.S.-based CSPs together (AWS, Microsoft Azure, and Google Cloud) accounted for over 60% of the worldwide cloud service market share in the last quarter of 2025.

Federal agencies have started to look into the business practices of CSPs to help ensure fair competition and access to the computational resources. The concentration of the cloud service market, and particularly the partnership between hyperscalers and leading AI model developers, has been under scrutiny by the Federal Trade Commission (FTC). A January 2025 FTC staff report identifies three "areas to watch regarding potential [antitrust] implications of the AI partnerships":

- A CSP could limit access to computational resources for AI developers other than its business partners.
- Contractual commitments may restrict an AI developer's use of multiple CSPs or make it difficult to switch between providers.
- The partnership may provide the CSP with access to sensitive information from the AI developer related to the AI model, its development methods, confidential technical and financial information, and customer usage and revenue numbers.[107]

Since it relies on internet technology to deliver services, the cloud computing service model shares the same technical solutions at the TCP/IP layer used by other internet services to transmit data and address certain cybersecurity threats. For example, a cloud service uses the common TCP and IP to manage high volumes of internet traffic between cloud servers and user devices. The cloud service could also use software-based firewalls to monitor data transmission and irregular network behavior at the TCP layer.[108] In addition to TCP, the cloud service often implements a cryptographic protocol called Transport Layer Security (TLS) to encrypt data transmitted between the server and user device.[109] NIST has published several technical standards and guidelines regarding security and access control for cloud computing.[110]

At the link/physical layer, an emerging issue of cloud computing is the construction of AI data centers, the physical facilities that pool, host, and deliver cloud computing resources and services supporting AI development and deployment. In addition to advanced AI chips, data storage, and network devices, a data center contains supporting equipment for power distribution and

[105] Maslej et al., "Artificial Intelligence Index Report 2024," pp. 66-67.

[106] Synergy Research Group, "GenAI Helps Drive Quarterly Cloud Revenues to $119 Billion as Growth Rate Jumped Yet Again in Q4," press release, February 5, 2026, https://www.srgresearch.com/articles/genai-helps-drive-quarterly-cloud-revenues-to-119-billion-as-growth-rate-jumped-yet-again-in-q4.

[107] FTC, Office of Technology Staff, *Partnerships Between Cloud Service Providers and AI Developers: FTC Staff Report on AI Partnerships & Investments 6(b) Study*, January 2025, p. 3, https://www.ftc.gov/system/files/ftc_gov/pdf/p246201_aipartnerships6breport_redacted_0.pdf.

[108] See, for example, Cohesive Networks, "Cloud Security Best Practices: Part 3 Network Layers 4–7," June 7, 2017, https://medium.com/@cohesivenet/cloud-security-best-practices-part-3-network-layers-4-7-3574a28eeace.

[109] Internet Society, "TLS Basics," https://www.internetsociety.org/deploy360/tls/basics/.

[110] See, for example, Vincent C. Hu et al., *General Access Control Guidance for Cloud Systems*, NIST, NIST Special Publication 800-210, July 2020, https://doi.org/10.6028/NIST.SP.800-210; and Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, NIST Special Publication 800-144, December 2011, https://doi.org/10.6028/NIST.SP.800-144.

environmental control.[111] AI's intensive computational tasks have led to increasing demand for data storage, processing capacities, and network performance in data centers. To meet the demand, the private sector (particularly large CSPs and AI developers) is reportedly investing billions of dollars to construct large data centers that could house thousands of computer servers and associated power and cooling equipment to support AI. These data centers could draw more than 100 megawatts (MW) of electric power at peak times.[112] The number and size of data centers are projected to increase over the next few years. As an example, as of October 2025, a multinational joint venture had identified seven sites in five U.S. states to build AI data centers with a total peak power draw of 8,000 MW and more than $450 billion in investment.[113] According to an online database, as of January 2026, the United States had 140 data center projects designed for AI purposes, and 65 of them had over $1 billion investment each and were designed to have over 500 MW power capacity.[114]

Some stakeholders have raised policy concerns regarding the large scale, number, and power demands of the planned AI data centers. Policymakers may consider whether future U.S. energy capacity will be sufficient to meet AI and cloud computing demands. A potential complication in addressing these and other policy concerns is the limited jurisdiction of the federal government in the siting, construction, operation, and energy permitting of data centers. These activities are largely under state and local jurisdiction.[115] Questions remain regarding the growth of AI data centers, their consumption of electricity and water, and their potential effects on local communities' utility rates, air and water quality, and job markets.

Safeguarding AI Cloud Services from Foreign Adversary Access

Some policymakers and commentators have expressed concern that cloud services may enable or facilitate foreign adversary access to computational resources for AI development. AI development is leading to a global competition for available computing power, especially through cloud services.[116] Since October 2022, DOC's Bureau of Industry and Security (BIS) has issued "a series of export control rules aimed at limiting access by China to the most advanced chips used for AI computations."[117] Some commentators argue that there is a loophole in these rules

[111] For a definition of data center, see Section 3.1.9 in ISO, *Information Technology – Data Centre Facilities and Infrastructure – Part 1: General Concepts*, ISO/IEC DIS 22237-1, October 2021, https://www.iso.org/obp/ui/#iso:std:iso-iec:22237:-1:dis:ed-1:v1:en.

[112] Phill Powell and Ian Smalley, "What Is A Hyperscale Data Center?," IBM, https://www.ibm.com/think/topics/hyperscale-data-center. Roughly, 100 megawatts of electric power are sufficient to support the electricity needs of 80,000 U.S. households. See also OpenAI, "Expanding Stargate to Michigan," October 30, 2025, https://openai.com/index/expanding-stargate-to-michigan/.

[113] OpenAI, "Expanding Stargate to Michigan."

[114] Server Country, "Project Database: The Most Comprehensive Database of U.S. Data Center Development," https://servercountry.org/data/projects/.

[115] For more information on federal permits related to data centers' energy infrastructure, see CRS Report R48762, *Data Center Energy Infrastructure: Federal Permit Requirements*, by Paul W. Parfomak et al.

[116] Erickson, "The Role and Benefits of AI in Cloud Computing." See also Shrivastava, "The China-US Tech War Comes to the Cloud."

[117] John Villasenor, *The Tension Between AI Export Control and U.S. AI Innovation*, Brookings Institution, September 24, 2024, https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation/. For more information on export controls on AI chips, see CRS In Focus IF12497, *Semiconductors and Artificial Intelligence*, by Laurie Harris. Examples of existing export control rules include DOC, Bureau of Industry and Security (BIS), "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," 87 *Federal Register* 62186, October 13, 2022, https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-(continued...)

because they prevent physical access to actual computing chips but have limited effectiveness when these chips can be accessed remotely through cloud services.[118] Foreign AI developers (including those in China) have reportedly rented, or sought to rent, advanced computing chips through U.S.-based CSPs to train their AI models.[119] In a debate on whether this practice is lawful, some experts and CSPs argued that existing export control rules do not restrict targeted foreign companies from accessing U.S.-based cloud services and from using advanced chips owned by these service providers, and thus they argue that commercial transactions between those companies and U.S. CSPs are allowed.[120]

In a response to the debate, some Members of Congress have introduced legislation to clarify the export control regulations and address potential national security concerns. For example, in the 118th Congress, the Closing Loopholes for the Overseas Use and Development of Artificial Intelligence Act (CLOUD AI Act; H.R. 4683) would have directed the Secretary of Commerce to issue regulations to prohibit U.S.-based CSPs from supporting Chinese entities for the cloud use of certain high-performance computing chips or computers that contain such chips.[121]

Some Members of the 119th Congress have introduced bills to address foreign access to U.S. computing resources. For example, the Remote Access Security Act (H.R. 2683) would expand export controls to include remote access to a commodity, software, or technology for purposes such as training AI models. The bill would define the term *remote access* using the following criteria:

- "access on a purposeful, knowing, reckless, or negligent basis to an item subject to the jurisdiction of the United States under [the Export Control Reform Act of 2018]";

controls-certain-advanced-computing-and-semiconductor; and DOC, BIS, "Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections; and Export Controls on Semiconductor Manufacturing Items; Corrections and Clarifications," 89 *Federal Register* 23876, April 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-07004/implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and. See also DOC, BIS, "Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls," press release, May 13, 2025, https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens.

[118] John Leyden, "U.S. Chip Export Control Rules Circumvented by AI Cloud Services, Says Report," *Computerworld*, June 7, 2024, https://www.computerworld.com/article/2139697/us-chip-export-control-rules-circumvented-by-ai-cloud-services-says-report.html. See also Villasenor, *The Tension Between AI Export Control and U.S. AI Innovation*; Mackenzie Hawkins and Anna Edgerton, "US Wants Cloud Firms to Report Foreign Users Building AI," *Bloomberg Law*, January 26, 2024, https://news.bloomberglaw.com/artificial-intelligence/raimondo-floats-cloud-reporting-rules-on-non-us-ai-developers.

[119] Anissa Gardizy, "China's Nvidia Loophole: How ByteDance Got the Best AI Chips Despite U.S. Restrictions," *The Information*, June 6, 2024, https://www.theinformation.com/articles/chinas-nvidia-loophole-how-bytedance-got-the-best-ai-chips-despite-u-s-restrictions.

[120] Raffaele Huang, "China's AI Engineers Are Secretly Accessing Banned Nvidia Chips," *Wall Street Journal*, August 26, 2024, https://www.wsj.com/tech/ai/chinas-ai-engineers-are-secretly-accessing-banned-nvidia-chips-58728bf3. See also Yuka Hayashi and John D. McKinnon, "U.S. Looks to Restrict China's Access to Cloud Computing to Protect Advanced Technology," *Wall Street Journal*, July 4, 2023, https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613.

[121] The bill refers to "any integrated circuit listed under Export Control Classification Number 3A090 and 4A090 of the Export Administration Regulations." For more information on DOC's Export Control Classification Numbers 3A090 and 4A090, see "The Commerce Control List," Supplement No. 1 to Part 774 of Title 15 of the *Code of Federal Regulations*.

- access "by a foreign person through a network connection, including the internet or a cloud computing service, from a location other than where the item is physically located"; and
- access in cases where "the use of the item could pose a serious risk to the national security or foreign policy."

The version of H.R. 2683 introduced in the Senate (S. 3519) contains similar provisions.

The China AI Power Report Act (H.R. 6275) would require the Secretary of Commerce to submit to selected congressional committees an annual report on "the advanced [AI] capabilities of China." The annual report would be expected to include "an assessment of the degree to which entities in China remotely accessed [AI] computational resources, including through cloud services, international data centers, or ... circumvention or avoidance of United States export controls."

The Artificial Intelligence Oversight of Verified Exports and Restrictions on Weaponizable Advanced Technology to Covered High-Risk Actors Act (AI OVERWATCH Act; H.R. 6875) would direct the Secretary of Commerce, in conjunction with specified agencies, to submit to appropriate congressional committees a "national security strategy" that would detail "the national security implications of and goals that should govern the physical and remote access by countries of concern" to certain U.S. chip technologies. The bill would also require the Under Secretary of Commerce for Industry and Security to prescribe regulations that require U.S. companies to establish "reasonable security standards, including … remote access … and other measures designed to prevent the illicit transfer, diversion, or access" to certain U.S. chips.

The Full AI Stack Export Promotion Act (H.R. 6996) would make it U.S. policy to "ensure global deployment of [AI] is based on [U.S.]-developed AI models, run by [U.S.] cloud operators, run by data centers owned or operated by [U.S.] firms, and functioning on [U.S.]-designed [AI] semiconductors." To "prevent illicit or unauthorized foreign adversary access" to the U.S.-based AI technologies, the bill would direct the Secretary of Commerce, in coordination with specified agencies, to work with foreign purchasers "to institute security measures" and report to Congress on them, including how foreign purchasers would prevent transfer of U.S. AI technologies to foreign adversaries, "including by remote access."

Congress may also consider specifying certain requirements for U.S.-based CSPs, such as exercising due diligence to identify and vet foreign customers and reporting large acquisitions or usage of AI computing resources to federal agencies. In addition to the identification and reporting requirements, Congress may consider requiring CSPs to seek government permission (e.g., a license) before selling services that use advanced computing chips to certain foreign customers.[122]

Congress may also consider potential impacts of such legislative options, for example, in the context of balancing the protection of national security interests with maintenance of U.S. leadership in cloud computing services. Some of the options presented above could provide some agencies with regulatory authority over U.S.-based CSPs, which have operated with limited government oversight.[123] Some U.S.-based CSPs, currently leading in the global cloud service

[122] See Hayashi and McKinnon, "U.S. Looks to Restrict China's Access to Cloud Computing to Protect Advanced Technology."

[123] In the FedRAMP Authorization Act (Section 5921 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023; P.L. 117-263), Congress codified the authority of the Federal Risk and Authorization Management Program (FedRAMP) to provide "a standardized, reusable approach to security assessment and authorization for cloud (continued...)

market, have reportedly argued that a statutory requirement for disclosing customers and workloads could "undermine customer trust and weaken [U.S. cloud companies'] competitiveness."[124] Without comparable measures by allied countries, cloud companies competing overseas might gain an advantage over U.S. companies.[125]

Because of the virtual and global nature of the internet that underlies cloud computing services, it might be technically challenging to effectively restrict foreign entities from accessing U.S.-based cloud computing resources. For example, at the application layer, U.S.-based CSPs might implement an identification program to determine whether a potential customer is an entity based in the United States. A CSP could require a potential customer to submit online information such as the name, principal place, and payment method of the business before opening an account. Some experts caution that this identity disclosure requirement might have some unintended consequences, such as causing privacy concerns for customers outside the United States.[126] Moreover, targeted foreign entities might "still try to access AI cloud computing services through a series of hard-to-disentangle intermediaries."[127] Chinese AI developers, for example, have reportedly worked with third-party brokers to access computing power, masking their identities by using cryptocurrency for payment and making transactions through their subsidiaries or shell firms in other countries.[128] At the TCP/IP layer, some CSPs might implement "zero-knowledge" encryption, which refers to "a method of storing data in the cloud so that only the owner of the data can access it."[129] If the client's data were encrypted on the cloud server, it would be difficult for the CSP to know whether the client's usage of online computational resources and services is malicious.[130] CSPs could also use IP addresses to block access from specific locations or countries, a practice known as *geo-blocking*.[131] While some IP addresses could be approximately mapped to a region, the geolocation information is not always reliable and accurate. Moreover, a client might use other internet technologies such as VPNs and anonymizing network services (e.g., The Onion Routing [Tor] Project) to circumvent geo-blocking systems.[132] At the link/physical layer, CSPs might rely on other ISPs to disconnect an internet backbone connection with specific countries. However, this approach would result in a blanket block, cutting off all users within the country, not only those attempting to access U.S. chips for AI development.

computing products and services that process unclassified information used by agencies" (see 44 U.S.C. §3608). For more information on the FedRAMP, see General Services Administration, Technology Transformation Services, "FedRAMP20X," https://www.fedramp.gov/20x/.

[124] Huang, "China's AI Engineers Are Secretly Accessing Banned Nvidia Chips."

[125] Hawkins and Edgerton, "US Wants Cloud Firms to Report Foreign Users Building AI." See also Shrivastava, "The China-US Tech War Comes to the Cloud."

[126] Madison Alder, "Commerce Proposes Rule Aimed at Protecting Cloud Services from Foreign Cyber Threats," *FedScoop*, January 30, 2024, https://fedscoop.com/commerce-proposes-rule-aimed-at-protecting-cloud-services-from-foreign-cyber-threats/.

[127] Villasenor, *The Tension Between AI Export Control and U.S. AI Innovation.*

[128] Huang, "China's AI Engineers Are Secretly Accessing Banned Nvidia Chips." See also Shrivastava, "The China-US Tech War Comes to the Cloud."

[129] Ben Wolford, "What Is Zero-Knowledge Cloud Storage?," *Proton*, June 23, 2023, https://proton.me/blog/zero-knowledge-cloud-storage.

[130] DOC, BIS, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 89 *Federal Register* 5698, January 29, 2024, https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious#sectno-reference-7.308.

[131] John Burke, "What Is Geo-Blocking?," *TechTarget*, August 20, 2025, https://www.techtarget.com/searchnetworking/definition/geo-blocking.

[132] ScienceDirect, "Onion Router," https://www.sciencedirect.com/topics/computer-science/onion-router.

Author Information

Ling Zhu
Specialist in Science and Technology Policy

Disclaimer