A Policy Framework for Internet Intermediaries and Content

January 2025

Internet Society

Executive Summary

Without intermediary functions to carry Internet traffic to and from endpoints (including individuals, servers, service providers, and many others), and without the many other types of intermediary functions that facilitate that traffic, there would not be an Internet.

Intermediary functions are crucial to the Internet's existence. This paper provides a framework for understanding Internet intermediary functions and developing policy concerning responsibility for online content without harming individuals' ability to use the Internet to create content and communicate with each other.

We focus on the functions performed by Internet intermediaries to facilitate online communication, such as transmitting, routing, storing, caching, hosting, securing, curating, and moderating content. This focus recognizes that many intermediaries perform multiple functions that raise differing policy issues and that many types of intermediaries offer fundamentally equivalent functions even though their services may appear quite different.

Our aim in this paper is to help policymakers understand those functions and develop policy relating to them. Well-designed policies can enhance the availability, diversity, security and privacy of individual participation online. However, poorly crafted policies can weaken Internet security, harm competition, restrict online communication, widen the digital divide, and fragment the Internet.

The goal is not to exempt intermediaries from responsibility, but to emphasize the critical role of liability protections in enabling individual participation on the Internet. Poorly designed intermediary-focused policies can have detrimental effects on the Internet and communication. Better alternatives, such as existing privacy, consumer protection, and discrimination laws, are often available.

In this paper, we discuss the **development of intermediary liability protections** and the motivation behind them, beginning with US Section 230, the Brazilian Marco Civil da Internet, and the EU's E-Commerce Directive and Digital Services Act. We explain why they and similar laws have been crucial for the growth of the Internet and individuals' ability to participate online.

We also highlight **some intermediary-focused policymaking trends**, such as notice-and-takedown regimes, upload moderation, and age-specific requirements. We note that these approaches risk harming the Internet by undermining its technical operations and reliability, weakening security and privacy, reducing competition, over-blocking lawful content, and excluding users from participating on the Internet.

We offer several important policymaking principles:

1. **Conduct an Internet Impact Assessment** to understand whether a proposed policy—relating to intermediary functions or more broadly—could have any adverse effect on the Internet and its operations.
2. **Carefully scope any proposed policy** to the specific intermediary function that is causing policy harm. Be alert to potential collateral damage. Avoid affecting an overly broad set of functions and entities.
3. **Protect intermediary functions from liability for content created by others**, including "user-generated content." Entities providing intermediary functions should be protected from liability for the content created by others that they transmit, receive, host, display, filter, or otherwise handle. This ensures that users can continue to speak and share content online.
4. **Protect intermediary functions of curating and moderating user-generated content**. Entities that host user-generated content have a legitimate right to set the "rules of the road" for their services and should be protected from liability for enforcing their own rules and removing objectionable content.
5. **To address concerns about online content, policymakers can use existing or new laws** focused on privacy and security, non-discrimination, accessibility, human rights, competition, user choice and control, transparency and openness, among others.

We include several "**Spotlights**" on policy considerations for specific online sectors including social media, federated networks, online gaming, augmented reality/virtual reality, advertising, as well as pay-for-content business models, managing protected speech, copyright, and artificial intelligence (AI).

The **Annex** at the end of this paper surveys the wide range of **intermediary functions** that enable or facilitate Internet communications. It provides an extensive **listing** and description of intermediary functions, and includes technical and practical considerations for policymaking as well as policy recommendations for each function.

Table of Contents

Internet Society

Internet Society

Internet Society

1 Introduction

This paper provides a framework for understanding Internet intermediary functions and developing policy concerning responsibility for online content. Internet intermediary functions facilitate the delivery and display of content or communications across the Internet. Internet Service Providers (ISPs), social media sites, web hosts, streaming services, and email services are all examples of entities providing intermediary functions. Our goal is to encourage policymakers to build policies that preserve what we believe are the most important characteristics of the Internet: being open, globally connected, secure, and trustworthy.

We provide an overview of the Internet and some significant intermediary functions to aid policymakers working in the area of online content. We discuss how Internet-focused policies can affect intermediary functions and user interactions and, in some cases, undermine the security, reliability, and other key desirable characteristics of the Internet. Finally, we provide specific recommendations for policymakers seeking to address social and policy objectives through policies that affect Internet intermediary functions and the entities that provide them.[1]

What are policies and how are they implemented?

Policies that impact the Internet can take many forms and can include: legal obligations, legal protections, administrative regulations, international agreements, tax incentives, rebates, certification schemes, procurement requirements, and even decisions **not** to legislate or regulate.

1.1 Policy Challenges Concerning Intermediaries

As explained below in Section 2, a broad range of intermediary functions are essential for the operation of the Internet. Consequently, policies

1 Under the intermediary liability protection regimes applicable to the Internet, the focus is on intermediary functions that support creating, discovering, finding, curating, delivering, or displaying content. This could include emails, tweets and other posts by individuals, as well as text, audio, or videos that are hosted and displayed on websites and major online platforms. These liability regimes generally do not cover other types of entities that provide a "middleman" service—such as the transfer of money from one person to another, and this paper does not address this type of non-content focused services..

that apply to Internet intermediary entities or the functions they perform could also significantly affect individuals' ability to create content and communicate with each other.

The influence of policies can be positive and constructive. We believe that most policymakers recognize the value of the Internet in their work. Policies can improve how individuals and communities experience the Internet, such as by encouraging services to secure data and protect their users' privacy, and they can leverage the power of the Internet as a force for good in society.

However, it is also possible to have significant negative consequences from policymaking: weakening of Internet security and privacy, driving out smaller competitors and discouraging new entrants, crippling the ability of users to communicate online, widening the digital divide, and fragmenting of the Internet. We believe that policymakers want to avoid these negative consequences, and this is one reason that the Internet Society is publishing this paper.

For policymakers considering policies that apply to the Internet, it is essential to consider the many and various types of intermediary functions critical for communication on the Internet. In addition, it is important to remember that the entities themselves providing intermediary functions are extremely diverse—from rural ISPs to small and large web hosting companies to Internet backbone services to huge video sharing and social media sites. This diversity means that it is crucial that any proposed obligations are targeted at the precise intermediary function as tightly as possible.

We recognize that not all content on the Internet is legal and beneficial for society and that countries are searching for effective ways to limit the spread of misinformation, harmful content, and criminal activity online. In this regard, intermediaries may present an attractive policy target because of their extensive interaction with user-generated content. We are not arguing that entities performing intermediary functions "cannot" or "should not" be subject to policy in some manner. Our goal is to show that policies affecting intermediary functions might have significant unintended consequences and be harmful to the Internet or the ability of people to communicate over the Internet and, therefore, should be avoided. We also highlight a range of policy tools—such as robust privacy laws—that governments have available to address social issues online.

1.2 The Internet has Transformed Communications With Strong Positive Social and Economic Impacts

The Internet has dramatically transformed how people communicate. Before the Internet era, telephone and postal mail were the main tools available for person-to-person communication. Mass communications such as newspapers, television, and radio offered individuals little ability to speak and participate.

The Internet—in stark contrast to newspapers, radio, and television—empowers individuals to participate in the conversation, in real time and around the world. The spectrum of Internet-enabled options includes one-to-one communications (e.g., encrypted messaging apps), one-to-many communications (e.g., publishing a website), and many-to-many communications (e.g., social media platforms). During its earliest years, the Internet supported communications through bulletin boards, mailing lists, discussion groups, blogs, and myriad other forms of user engagement.

The ability of individuals to use the Internet for communications, to send and receive information from other people across town or around the world, also brings direct benefits: benefits that accrue to those individuals, their communities, and their countries. People are using the Internet to create new social and economic opportunities for themselves and others. Entrepreneurs can develop products and services that address the needs of their communities. Governments can interact with their citizens far more robustly, quickly, and at less cost.

The Internet Empowers Participation

The Internet Society's goal in writing this paper is to explain why intermediary functions for enabling and facilitating the communication of user-generated content should be protected from liability. We also wish to highlight that there are other policy tools available to constructively address concerns about online services and their users' content. It is not our intent to advise policymakers on how to regulate the Internet, but how to create policy that allows the most important outcome of the Internet, individual communications, to continue to flourish.

"A key characteristic of the Internet—one that sets it apart from every other communications media—is that it was meant to be open for everyone. Individuals can speak, debate, create, invent, and engage with others, whether they are across town or around the world." (Testimony before Congress by Andrew Sullivan, Internet Society CEO, March 8, 2023)

Communications facilitated by the Internet enhance global knowledge and economic opportunity. Beyond these benefits, the Internet has clearly created economic opportunities for nations, companies, organizations, and people around the world.[2]

1.3 The Internet Empowers Active Individual Communications

With the Internet, individuals are no longer passive recipients of mainly corporate-created or government-sanctioned content. People are active participants in creating content and shaping how that content can be made available to people around the world. In this paper, we use the term "**user-generated content**" to refer to anything posted or shared online by a user, rather than the owner of a site.

The concept of **user-generated content** often arises in legal cases and policy debates about who should be legally responsible for such content. **User-generated content** may be an original work created by the user posting it to the Internet, or it could have been created by someone else and posted—with or without permission from the original creator.

The key defining characteristic of **user-generated content** is that it was created or posted to a site or shared online by someone other than the owner of the site or service. It is distinguished from "**original site content**"—content created by the site owner's employees, contractors, and content development services, for which the site owner has clear legal responsibility.

The spectrum of **user-generated content** is broad. It could be content posted by individuals, but it could also be posted by an organization or corporation. There is an unlimited array of types of user-generated content: social media posts, emails, messages, long—or short-form videos, product reviews, poetry, music, or observation data by citizen scientists. **User-generated content** could be serious, silly, artistic, factually correct, factually incorrect, clever, offensive, harassing, profound, useful, useless—anything on the vast spectrum of human ideas and expressions. But, of course, some may be harmful, defamatory, deceptive, threatening, or even illegal.

2 As noted in the 2010 OECD report on The Economic and Social Role of Internet Intermediaries, the growth of entities providing Internet intermediary functions contributed to economic growth and productivity, investment in infrastructure, increased employment and entrepreneurship, innovation, user empowerment choice, trust, and privacy. See https://doi.org/10.1787/5kmh79zzs8vb-en

Original Site Content Compared to User-Generated Content

If an automobile manufacturer decides to create a basic website to display new auto models that are available for purchase, the content of that website would be created by the manufacturer and its employees and contractors. Just as the automobile manufacturer is responsible for the content of a brochure or other printed document, the manufacturer is equally responsible for the content that it posts online. We call that content **original site content**. In general, the manufacturer would have clear responsibility and potential legal liability for the content that it created and made available online.

If the automobile manufacturer chooses to add interactive capabilities to the website and allow individual visitors to post comments about the auto models, those comments would be **user-generated content**. The website would have a mix of mostly original site content and some user-generated content.

In contrast, a typical social media website for automobile enthusiasts would likely contain predominantly **user-generated content**: Individual site visitors post long and short-form content and have discussions with other visitors. Some **original site content** created by the website owners might be present, such as support information and terms of use.

The question of responsibility and liability for the entities that provide intermediary functions that help facilitate the communication of **user-generated content** is a core topic discussed in this paper.

1.4 The Role of Intermediary Functions in Enabling Communication on the Internet

The Internet would not exist without the entities that provide intermediary functions. Its fundamental decentralized and distributed architecture, which is essential for enabling the Internet's social and economic benefits, depends on the hundreds of thousands of entities that provide intermediary functions.

Internet intermediary functions include delivering, securing, hosting, and facilitating Internet communications. To better understand intermediary

functions on the Internet, a comparison with postal services may be useful: postal services use many different intermediaries to deliver the mail: carriers who pick up and deliver the mail, trucks, and airplanes to transport the mail, security guards to protect the mail, mailboxes to store the mail, post offices to administer it all, and others. All these entities are agents of the postal service.

The Internet has intermediary entities performing analogous services and functions, but with a key difference: Internet intermediary functions are provided by independent entities, and there is no central coordinating office controlling the delivery of communications. The postal services control how mail is delivered from the point it is received; on the Internet, there is no single entity controlling how content is delivered or who is responsible for each step in the process. Further, unlike the postal service, content on the Internet is almost always broken into pieces that are transmitted separately and may travel through different independent networks. Moreover, unlike the postal service, many pages on websites are comprised of dynamic components created and hosted by different entities. The open interoperable Internet technical protocols are what enable a huge diversity of communications—including dynamically composed web pages—to flow without a central controller.

But, in both cases, the postal service and its agents, as well as the various intermediaries involved in Internet communications, are communicating user-generated content. Yet the functions of the intermediaries are different.

In this paper, we have chosen to focus on intermediary "functions" (such as "providing access to the Internet") rather than types of entities (such as "Internet Service Provider" or "social media" site). We believe this approach provides greater rigor and precision when defining policy because many entities carry out multiple different intermediary functions, and these different functions raise different policy issues.

For example, an Internet Service Provider (ISP), in addition to providing Internet access to households, may perform additional intermediary functions such as Voice over IP telephony, DNS lookup, email hosting, and content or malware filtering. A social media platform, in addition to providing its members with the ability to post and react to content, may perform other intermediary functions such as one-to-one messaging, website hosting, and live audio/video conferencing. Further, some online services may incorporate the same or equivalent intermediary functions. Introducing policy or rules, for example, regarding the use of embedded

content on social media sites may inadvertently impact everyone's use of embedded content on the Internet.

Our focus is on Internet intermediary functions that are in some way involved in displaying, discovering, curating, or delivering *content that has been* ***created by others***, i.e. user-generated content.

1.5 Comparing Liability for Site-Generated Content and User-Generated Content

A starting point for comparison is that someone who creates online content is responsible for it—and is not an intermediary for that content. However, if they transmit, display, host, or otherwise facilitate content created *by others*, they would be viewed as intermediaries and would generally not be legally responsible for that content.

For some entities, *all* content on their websites or in their services is created "by others." Other entities ' websites may contain a mix of content created "by others" (thus deserving of intermediary liability protections) and content that they themselves created (thus not protected from liability). Three examples can help illustrate the distinction:

- For a residential Internet Service Provider, *all* content transmitted to and from that house is created by an entity distinct from the ISP. The ISP does not create any content; it is only responsible for carrying it. The ISP typically only provides intermediary functions for the content it handles between the end user and the rest of the Internet. From a liability point of view, the ISP is not responsible for the content it transports.
- For a car manufacturer with a website that describes their products, but *also* allows users to post reviews or comment on the content, the company is responsible for most of the content on the website and is not viewed as providing an intermediary function for that particular content. However, the company ***is*** *providing an intermediary function* regarding the customers' comments posted on the company website. This is because those comments were created by someone other than the company. The car manufacturer is legally responsible for the content it created and posted, but the content posted by others requires a different approach to liability.
- For the independent web hosting company that operates the servers and infrastructure used by the car manufacturer, the function is pure intermediary: *all* the content on the website (car company

created along with customer comments) is user-generated content. As with the ISP, the web hosting company should not be liable for content published by others on the websites that it hosts.

Importance of Intermediary Functions to Individuals' Ability to Use the Internet and Share Content

At the neighborhood level, people rely on intermediaries—ISPs and community networks—to connect to the Internet. Once connected, *every* communication over the Internet requires the participation of numerous independent entities providing intermediary functions to transport, host, protect, and deliver billions of communications every day.

Everyone uses the Internet for different things, but any use requires people—often unknowingly—to access and rely on dozens or hundreds or more entities providing intermediary functions every hour they are online. This dependence on intermediary functions is fundamental to the day-to-day operation of the Internet. For this reason, policy that affects intermediary functions must be crafted very carefully so as not to negatively affect the operation of the Internet.

2 The Internet and Intermediary Liability

This section briefly reviews some technical aspects of the Internet and introduces some important characteristics of the Internet, part of what we call "The Internet Way of Networking." We also describe the critical role that intermediary functions and the entities that provide them play in all Internet communications.

2.1 The Critical Flaws of the 19th Century "Circuit-Switched" Model of Communications that Predated the Internet

Before the Internet, the primary person-to-person communications system was the "circuit-switched" telephone system, in which switches were used to create a dedicated electric circuit between the originator of a phone call and the recipient. Sixty years ago, to enable a phone call from New York City to Johannesburg, the American phone company would chain local wiring to create a circuit to connect to an undersea cable that would connect to the South African phone company, and the South African phone company would build a circuit on the other end to carry the voices across the ocean. After the call, the circuit would be dismantled, and the resources used for the call would be available to carry out another phone call. For most of the 20th Century, most telephone calls within a country were handled by a single monopoly telephone company that controlled the network, charged for calls, and was responsible for the maintenance and extension of the network. In some countries, the companies were government-owned or operated.

The circuit-switched approach of traditional telephony is extremely inefficient. The resource reservation required for a telephone call meant that a household or community with a single phone line could only have a single conversation at any moment and may have to wait until lines to the recipient were available. The network had to be overbuilt to handle peak loads, and costs were very high. There was often insufficient capacity

at peak times, such as holidays like Christmas and New Year's Eve. Using a dedicated circuit for a single phone call was inefficient by itself because the wires could carry more content than a single call. The technical and economic inefficiency of traditional telephony was a critical driver in the development of "packet-switched" networks, the basis for the Internet of today.

Circuit-switched telephony had other risks and costs. A top-down, centrally controlled network is vulnerable to disruption from failures of key command centers or portions of the network[3]. The monopoly national phone company, with no incentive to bring new products and services to market, tended to stifle innovation in consumer services with onerous regulation or unaffordable costs. It may be that additional competition in circuit-switched telephony would have led to more innovation, but the intrinsic centralization of circuit-switching meant that, at some point, every network came under the exclusive control of one entity, which had little economic incentive to invest in new services.

These and other drawbacks led researchers in the 1960s and 1970s to develop and refine "packet switching" and, ultimately, to develop what became the Internet.

2.2 Understanding the Internet Way of Networking

Often called a "network of networks," the Internet is a connected network built up from networks that have chosen to connect with each other. Early Internet designers recognized the benefits of a flexible design to enable new technologies to emerge and for new networks to connect. They also recognized that the best way to deploy a very large, distributed network was to take advantage of existing networks, linking them together with simple, low-cost, commonly-available technology.

Unlike circuit-switched telephony, Internet communications flow over this network of networks using packet switching:[4] every communication is broken into small "packets," and each packet travels independently. For example, each email is split into multiple smaller packets, which can, and often do, take different paths across the Internet to reach the intended

3 The Internet, in comparison, is highly distributed which enhances its reliability and robustness and ability to route around network problems.

4 For a description of packet switching, see https://www.internetsociety.org/blog/2022/04/common-internet-network-interconnection-and-charging-practices/; see also https://en.wikipedia.org/wiki/Packet_switching.

recipient. As they arrive, the destination reassembles them seamlessly before delivering the email to the end user. This was a major innovation in how content was communicated over networks.

The Internet is itself made up of almost 76,000 independent networks that use the same technical protocols and choose to operate with one another. Many of these networks are privately owned, but some are owned or controlled by governments. Each network makes independent decisions on how to route traffic to its neighbors based on its own needs, business model, and local requirements. In addition, there are hundreds of thousands of other entities—such as web-hosting providers, email services, domain services, identity services, and security providers—that provide critical services to support and facilitate communications across the Internet. There is no centralized control or coordination of the networks or supporting entities.[5]

This distributed and decentralized design is fundamental to the success of the Internet. The Internet has spread across the world and grown so large due to this essential design principle. As new needs, areas of operation, or inventions come along, new networks easily and inexpensively join the Internet. In particular, this design has allowed even small or remote networks to connect to the Internet at a relatively modest cost, usually without any negotiations or agreements other than with local service providers.

The Internet is fundamentally different from the circuit-switched communications networks of the past, and these differences in distributed operation and decentralized design are critical for the continued health and growth of the Internet.

2.3 The Role of Intermediary Functions

Entities that provide intermediary functions play an essential role not only in providing global connectivity and content sharing, but also in providing security, safety, privacy, and accessibility. The Internet depends on a range of intermediary functions to work.

A wide diversity of intermediary functions supports the modern Internet. Some may be familiar to users and policymakers, such as those provided

5 An Internet Society paper, "The Internet Way of Networking: Defining the critical properties of the Internet," Internet Society, 9 September 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/, identifies the critical properties that make the Internet 'The Internet' and underpin the growth and adaptability of the Internet. This paper is part of a larger effort called The Internet Way of Networking, with additional resources at https://www.internetsociety.org/action-plan/internet-way-of-networking/.

by ISPs, "transit providers" that connect other networks to each other, hosting services that support web content and email, search engines, and social media services. Other types of intermediary functions may be less familiar, including content caching, network, and cyber defense, "domain name system" (DNS) resolution, and domain registration.[6] Even some types of software, such as web browsers, provide intermediary functions by receiving content from the Internet and displaying it to an end user (often with security blocking of malicious websites).

Without intermediary functions to carry Internet traffic to and from end-points (including individuals, servers, service providers, and many others), and without the many other types of intermediary functions that facilitate that traffic, there would not be an Internet.

Users may choose to interact directly with some providers of intermediary functions, such as their Internet Service Provider to access the Internet, their preferred search tool, and their browser to display and sometimes filter content. Having a variety of options available also enables greater user choice and control. For example, users can choose to use intermediary functions that focus on privacy protection, or that provide "family-friendly" online experiences.

However, most users do not know or even understand the huge range of intermediary functions that facilitate their communication. For example, users may not know about DNS lookup or who is providing the DNS lookup function for their web searches, or who and what facilitates transit for their packets once they leave their home ISP. Further, many of those entities providing the intermediary functions may have no relationship (legal or otherwise) with the user initiating the communication or the recipient, nor with each other. While many entities are commercial, some Internet intermediary functions are provided by non-profit or volunteer communities. Entities may be in different jurisdictions from both the sender and the recipient. This decentralized and distributed approach is "a feature, not a bug." It would be impossible to have direct one-to-one relationships for all intermediary functions at the Internet's scale. The Internet's distributed approach provides flexibility, resilience, and the ability to scale up and down as needed.

Entities that make the Internet work and help users access it (sometimes loosely termed "infrastructure intermediaries") generally are not aware

6 The Annex to this paper provides a longer list of intermediaries, covering dozens of types, along with specific recommendations for policymakers with advice on pitfalls to be aware of regarding each type of intermediary.

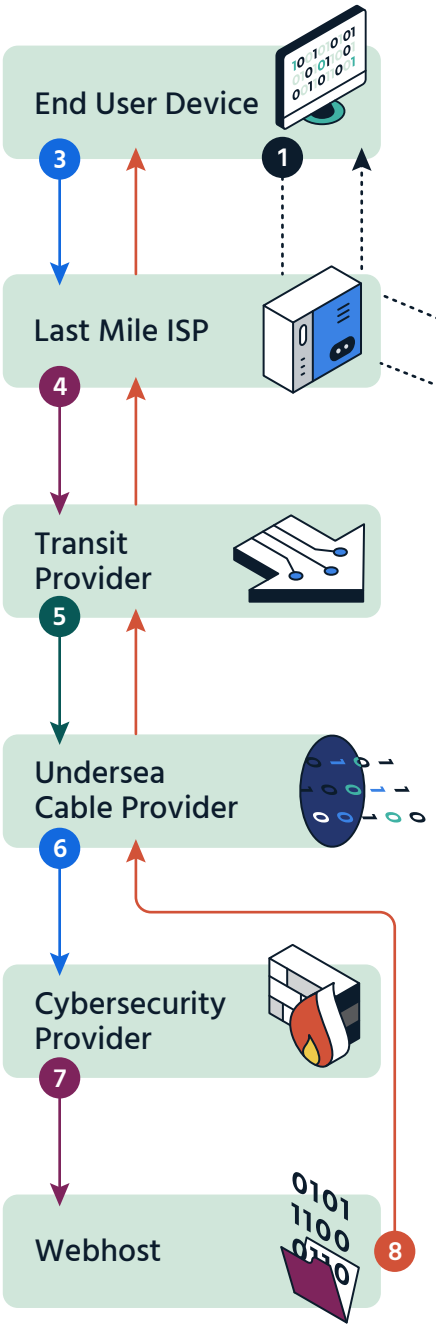
of the specific content that is being communicated[7]. By contrast, entities that help users interact with content on the Internet (e.g., a video-sharing platform or a social media platform) are usually directly involved in how content is displayed, curated, shared, *etc.* However, there is not always a clear, bright line between these entities, and not all "platforms" are aware of the content being delivered to users.[8]

7 Infrastructure intermediaries not only don't care about the specific content being communicated but also can't see content due to the increasing use of end-to-end encryption across the Internet.

8 For example, most on-line one-to-one messaging services such as WhatsApp and Signal employ end-to-end encryption between end users, making the actual content they transmit opaque and unknown.

Providers of Intermediary Functions

Very simplified view of some of the **providers of intermediary functions** implicated when a user requests a web page.



1. The user's computer requests the IP address for a web page from the user's preferred DNS provider through the user's **last mile ISP**.
2. The **DNS provider** returns the website's IP address to the user's computer.
3. The user's computer requests the desired webpage from the webhost located in another country.
4. The last mile ISP passes the request to a **transit provider** to forward to the webhost.
5. The transit provider passes the request to an **undersea cable provider**.
6. The undersea cable provider passes the request through other transit providers to the webhost's **cybersecurity provider**.
7. The cybersecurity provider ensures that the request is not part of a cyberattack and passes it to the **webhost**.
8. The webhost receives the user's request and sends the requested webpage back to the user over similar but often different transit and interconnection providers.

3 Liability Protections for Intermediary Functions

This section discusses liability protections, beginning with a brief history of the origins and key elements of the United States Section 230. We also describe Brazil's 2014 Marco Civil da Internet and Europe's E-Commerce Directive of 2000 and the Digital Services Act of 2022, and then move to discuss other related national or regional approaches.

We close by discussing recent trends in policies relating to intermediary functions and identify some specific risks that these approaches can raise for the Internet and Internet users.

3.1 The Initial Development of Intermediary Protection Laws: Setting the Context

The early Internet was developed in the 1970s based on funding provided by the United States (US) Government. Initially used for collaboration and research by a small set of academic, government, and commercial researchers, it started as a US-only network but quickly grew to include Europe, Asia, and Oceania connections. Personal and commercial traffic prohibitions were gradually removed in the 1990s. In 1995, the US Government formally transferred the network to the private sector, which began to bring ordinary people onto the Internet.[9]

As more and more individuals were able to speak publicly on the Internet, questions quickly arose about how liability for harmful or illegal content would be assigned in the online context. In the US, lawsuits were filed arguing that the companies that allowed people to post online should

9 Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), held that an online service provider would not be held liable for speech made by a participant in an online forum, but only because the provider had not moderated any content. Then Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), held an online service provider liable for participants' speech because the provider engaged in some content monitoring and regulation.

be legally liable for the words that those people had posted. In the 1990s, two seminal US court decisions decided that the online hosts of content—the intermediaries—**would** be liable for the words posted by their users *if those hosts had taken actions to moderate the online speech and remove sexual, offensive, or other content.*

Those court decisions created two unworkable and unappealing scenarios for the emerging Internet.

On the one hand, if companies took actions to "moderate" online speech from their users, then they would be liable for that content, but these entities[10] did not have the staff or resources to review, block, or remove any content that might cause liability.[11]

On the other hand, companies could avoid liability if they took *no* actions to remove sexual, offensive, or otherwise objectionable content from what users posted. But such an environment would have yielded online conversations and postings flooded with objectionable content. Rather than becoming a useful platform for social and civic interaction and economic growth, the Internet would have lost its usefulness as a tool for individual communication, expression, and commerce.

These court decisions created significant uncertainty and potentially crippling liability for user-generated content for the developing Internet.

3.2 The First Internet Intermediary Liability Laws: US Section 230

In the face of this challenge to the potential of the Internet and the ability of individuals to engage online, from 1995 to 1996, the United States Congress decided to confront the reality that existing liability regimes did not work for the Internet:

- Publisher-based liability that applied to offline newspapers would lead either to massive potential liability that would cripple individual speech on the Internet, or an Internet on which sites could not enforce rules of behavior and courtesy.

10 While today's large social networking sites are an obvious example, the Internet of the 1990s had fewer "mega-sites" and there was often no clear intermediary who had the right or responsibility to moderate content. When a moderator was identified, as often as not it could be a private individual volunteering their time rather than a private company.

11 Even in an environment of abundant resources, some types of moderation, such as for defamatory content, are themselves problematic, as the question of whether content is defamatory or not is often impossible for an individual moderator to ascertain.

- The common carriage regime applicable to basic telephone service could not apply to either Internet access networks, which had some aspects of communications carriers but not enough to fit that model, or content hosts, which operate completely differently than common carriers.
- The liability regime that applied to radio, television, and cable video—which is based on individually negotiated contractual agreements between networks and the corporations providing content—could not possibly apply to a world with millions and ultimately billions of online users.

We needed a new approach to liability.

It is against this backdrop that the US Congress considered and enacted the "Internet Freedom and Family Empowerment Act," which became 47 United States Code (USC) Section 230 (often called simply "Section 230").[12] One of Congress's explicit goals for Section 230 was "to promote the continued development of the Internet and other interactive computer services and other interactive media."[13] The Congress recognized that interactive computer services in general, and the Internet in particular—even at its early stage when Section 230 was enacted—offered a profoundly different platform for interactive communication by individuals.

The US Congress observed in the statute that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[14] Congress concluded that these interactive communications, which foster public discourse, should be encouraged. The Internet, unlike prior "published" forms of mass communication, transforms the individual from a passive recipient of mainly corporate-created products into an active participant in shaping communication and content. Congress recognized that this individual-driven "interactivity" was an essential attribute of the emerging Internet that warranted protection.

12 The text that became Section 230 originally came from a House of Representatives legislative proposal, the Internet Freedom and Family Empowerment Act. During the House/Senate conference to reconcile legislation for the Telecommunications Act, the Section 230 text was placed immediately following and in the same statutory section as the Senate bill, known as the Communications Decency Act. Additional context around the new Telecommunications Act is available at "What's in a Name" (https://www.lawfaremedia.org/article/whats-name-quite-bit-if-youre-talking-about-section-230), "Section 230: An Overview" (by the Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R46751), among others. The final text can be found at https://www.congress.gov/bill/104th-congress/senate-bill/652.

13 47 USC § 230(b)(1), available at https://www.congress.gov/104/statute/STATUTE-110/STATUTE-110-Pg56.pdf.

14 47 USC § 230(a)(3).

Key text from Section 230:

§ 230(c)(1): **Treatment of publisher or speaker**. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

§ 230(c)(2): **Civil liability**. No provider or user of an interactive computer service shall be held liable on account of—

> (A)any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B)any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph ([A]).

§ 230(f): **Definitions**.

(2) **Interactive computer service**

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) **Information content provider**

The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) **Access software provider**

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

> (A) filter, screen, allow, or disallow content;
>
> (B) pick, choose, analyze, or digest content; or
>
> (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

The **United States**' Section 230 contains three critical elements:

1. Interactive computer services (a statutory term used in Section 230 that essentially refers to entities that provide intermediary functions) on the Internet are not legally responsible for content that other entities—individuals, corporations, and other content providers—post on the Internet. Instead, the legal liability for the content remains with the person or entity that created or posted the content. This element is what allows ISPs, web hosting services, and many others to carry or host content without fear of potentially massive liability.
2. Interactive computer services are not liable if they decide to block or remove unwanted content on their platforms. This element assures that online hosts and platforms are protected if they remove hateful, offensive, or otherwise objectionable content from their sites. If, for example, an individual posts sexually explicit content to an online platform, the individual could not sue the platform if it removed or blocked that content. Thus, intermediaries are protected for their moderation decisions.
3. Companies that develop technology tools to allow users to filter and block unwanted content on the Internet cannot be held liable for creating that blocking capability. If, for example, a website containing hateful and malicious content is blocked by software installed by a parent on a home computer, the website cannot sue the maker of the software for blocking its content. This element encourages the development of tools to allow users to choose to limit the types of lawful content they (and their families) can access.

All of the above protections extend very broadly to any interactive computer service that is involved in transmitting, carrying, hosting, curating, displaying, or otherwise facilitating the transmission or display of content that others have created, not just the service where the content was posted or shared.

Section 230 does not use the terms "intermediary" or "intermediary function"; instead, the law broadly defines the term "interactive computer services" to refer to the basic functions of Internet access, transit, hosting, search, and related services. Then, Section 230 applies the above liability protections to any "provider or user of an interactive computer service."

Note that even individual users are protected by Section 230 in circumstances when they, for example, forward an online posting to another recipient.

Section 230 is viewed as a critical reason that individual speech has thrived on the Internet within the United States.[15] At the same time, the US Congress also was seeking to protect and encourage the economic potential of the Internet. And the combined economic and social benefits from the Internet that the United States experienced led other major governments to adopt similar rules.

The United States was the first nation to adopt legal liability protections for Internet intermediaries. Other nations and regions have adopted similar protections, but with some important differences.

3.3 Initial Intermediary Protections in Europe

In 2000, the **European Union** (EU) adopted the Electronic Commerce Directive (2000/31/EC),[16] or "E-Commerce Directive" to address intermediary protections. As a practical matter, the E-Commerce Directive adopted an approach very similar to Section 230, but with three significant distinctions:

- The EU directive divided intermediaries into the basic categories of (a) mere conduits, (b) caching providers; and (c) hosting providers.
- The directive did not define the types of entities that are covered, but instead addressed specific types of "activities" that would receive liability protection (much as this paper focuses on intermediary "functions" rather than categories of intermediaries).
- Most importantly, the EU directive requires that intermediaries who obtain knowledge of content alleged to be illegal take steps to remove the content reasonably promptly.[17]

The E-Commerce Directive governed intermediary protection issues in the European Union for more than 20 years, until it was modified and supplemented by the Digital Services Act and other actions discussed below.

15 Jeff Kosseff, a US legal scholar, went so far as to write an entire book, "The Twenty-Six Words that Created the Internet," referencing Section 230 as being singularly responsible for much of the US Internet industry. See also https://www.propublica.org/article/nsu-section-230 for additional context.

16 See https://eur-lex.europa.eu/eli/dir/2000/31/oj; https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000.

17 The "notice and takedown" regime that the E-Commerce Directive created stands in contrast to the approach in the United States, in which the First Amendment of the US Constitution generally (outside of the copyright context) prohibits legal mandates to remove content without a specific judicial determination that the content is illegal.

3.4 The Marco Civil da Internet in Brazil

Beginning in 2009, a broad set of stakeholders in Brazil—including the government, academia, civil society, and industry—undertook a collaborative effort to develop a set of laws addressing the Internet. Through multistakeholder engagement, the effort received extensive commentary and input, and drafts were developed and refined. The resulting legislation was enacted in 2014 as the Marco Civil da Internet, Brazilian Federal Law No 12.965/2014.[18] The Brazilian Government states that the Marco Civil "establishes the principles, guarantees, rights, and duties for the use of the Internet in Brazil."[19]

Section III of the Marco Civil offers a very direct statement of intermediary liability protection, with additional provisions to permit court-ordered removal of content and protection of privacy with notice. Key provisions of the intermediary provisions include:

> Article 18. The provider of Internet connection shall not be civilly liable for damages arising from content generated by third parties.
>
> Article 19. In order to ensure freedom of expression and prevent censorship, providers of Internet applications can only be civilly liable for damages resulting from content generated by third parties if, after specific court order, they do not make arrangements to, in the scope and technical limits of their service and within the indicated time, make unavailable the content identified as infringing, otherwise subject to the applicable legal provisions.
>
> ...
>
> Article 20. If the provider of Internet application has the information of contact of the user directly responsible for the content referred to in article 19, it will be the responsibility of the provider to communicate to the user the reasons and information related to the unavailability of the content, with information allowing the adversarial and full defence in court, unless there is express legal provision or express judicial determination based on the contrary.
>
> ...

18 See https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6, or English official version of the law at https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180 and https://www.daniel-ip.com/en/articles/the-brazilian-internet-bill-of-rights-and-online-infringement-of-ip-rights/.

19 English version of the Marco Civil, available at http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf.

> Article 21. Providers of Internet applications who make available the content generated by third parties shall be held subsidiarily responsible for the breach of privacy resulting from the disclosure, without the participants' permission of images, videos or other materials containing nudity or sexual acts of private character when, upon receipt of notification by the participant or their legal representative, fails to diligently promote, within the technical limits of their service, the unavailability of that content.

The Brazil approach has been regarded in the region as a path towards providing protection for intermediary functions while standardizing a judicial route to address government and citizen concerns about illegal or harmful content.

3.5 Updated Intermediary Protections in Europe

In 2022, the **European Union**, motivated by concerns about online safety, the spread of disinformation and hate speech, and other unlawful or harmful conduct on large platforms and widely used services, adopted a significant update and expansion of the 2000 E-Commerce Directive, continuing its general approach of addressing services (many of which encompass "intermediary functions" discussed here), rather than companies. This recognizes that some entities may provide different intermediary functions, and thus be entitled to different kinds of protections or have different obligations depending on the specific function being executed.

The overarching objective of the EU *Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act)[20] is to provide a single market for online services in the EU. The Digital Services Act includes liability protections for user-generated content (except where the service provider knows it is illegal), but couples them with "due diligence" requirements. These obligations make providers more accountable and responsible for what happens on their services. Rather than imposing liability, the Digital Services Act uses fines to deter and punish non-compliance with those obligations.

20 See https://eur-lex.europa.eu/eli/reg/2022/2065/oj, as well as the FAQ provided by the European Commission at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 and summary information at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

Drawing from the E-Commerce Directive, the Digital Services Act applies to a subset of "information society services" defined as three categories of an "intermediary service":[21]

1. A 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.
2. A 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate, and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request.
3. A 'hosting' service consisting of the storage of information provided by, and at the request of, a recipient of the service.

Additionally, the Act applies particular obligations to two categories of services: designated very large search engine providers (VLOSES) and very large online platforms (VLOPS) (defined as having more than 45 million EU users/month). They include:

- A point of contact for EU authorities and users.
- User-friendly terms and conditions.
- Transparency regarding advertising, recommender systems, and content moderation decisions.
- A risk-based assessment of their service and appropriate mitigation measures.
- Independent auditing.
- Data sharing with authorities for compliance purposes and with vetted researchers to understand systemic risks.
- An obligation to provide a recommender system option not based on user profiling.[22]

21 Ibid., Article 3, "Definitions" of Digital Services Act.

22 See European Commission guidance at https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

3.6 Intermediary Protections in Other National and International Contexts

Various countries in the early 2000s also adopted Internet-focused national legislation, enacting varying levels of protections for intermediary functions.

For example, in 2000, **India** passed the Information Technology Act 2000, which provided that intermediaries would not be liable for third-party content available if they could prove that the offense or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such offense or contravention.[23] The Act also permits governmental directives to remove certain online content.

In **Nigeria**, in 2003, the Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission provided that Internet service providers acting as mere conduits (i.e., hosting or caching) would not be liable for user-generated content and communications with some conditions: They must act without delay to remove or disable access to the information on receipt of any takedown notice, or when they become aware that the information at the initial source of the transmission has been removed or disabled.[24]

South Africa, in its Electronic Communications and Transactions Act 2002, adopted a similar approach, but made the limitations of liability conditional on the service provider being a member of a representative body and bound by the representative body's code of conduct recognized by the Minister, as well as a notice and takedown process.[25]

New Zealand's Harmful Digital Communications Act 2015 protects "online content hosts" from liability, provided they comply with the statutory complaint process. The Act includes a requirement for the online content host to notify the person making a complaint and may involve a requirement to take down or disable content.[26]

23 See Article 79 of the Information Technology Act of 2000 (India), available at https://www.meity.gov.in/writereaddata/files/itbill2000.pdf.

24 Guidelines for the Provision of Internet Service published by the Nigerian Communications Commission in 2003 pursuant to Section 70(2) of the Nigerian Communications Act 2003, available at https://ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file.

25 Electronic Communications and Transactions Act 2002 (South Africa) available at https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

26 Harmful Digital Communications Act 2015 (New Zealand) available at https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM6512504.

Australia is actively moving forward in 2024 to adopt an intermediary liability protection regime focused on legal claims for defamation.[27] The proposed Model Defamation Amendment (Digital Intermediaries) Provisions 2023 would amend Australia's "uniform" defamation laws, which came into effect in 2006, to harmonize defamation laws throughout Australia. The new provisions are intended to clarify the legal position of intermediaries regarding digital defamatory content. They provide exemptions for liability for defamation for digital intermediaries providing caching, conduit, storage, and search services.[28] However, those exemptions will not be available if the digital intermediary, among other things, selected any of the recipients or promoted the defamatory content. It is unclear whether that would include promoting content to users via recommender algorithms. The exemption for search engines would not apply to "sponsored search results," that is, "the results [that] are promoted or prioritized by the search engine provider because of a payment or other benefit given to the provider by or on behalf of a third party."

In addition to binding laws adopted by governments, several multilateral or multistakeholder organizations have issued statements of support for intermediary liability protections. These international agreements and statements reflect a growing consensus on the value of such protections. We provide a summary of some of these statements in the table below.

Multilateral and Multistakeholder Statements on Intermediary Liability Protections

2011

The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information[29] issued a joint declaration calling for protections of "mere conduit" intermediaries, and for other intermediary functions, expressing the view that they should

27 See https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf or https://www.parliament.nsw.gov.au/bill/files/18503/Passed%20by%20both%20Houses.pdf (New South Wales version).

28 Schedule 1, Sections 10C and 10D of the Model Defamation Amendment (Digital Intermediaries) Provisions 2023 available at https://pcc.gov.au/uniform/2023/pcc-584-d40.pdf.

29 https://www.osce.org/representative-on-freedom-of-media/78309.

not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression.

2013

At the African Internet Governance Forum, a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation in Africa, published the African Declaration on Internet Rights and Freedoms,[30] which contained the very simple intermediary protection principle: "No-one should be held liable for content on the Internet of which they are not the author."[31]

2014

The Organisation for Economic Co-operation and Development (OECD) released broad guidance on limiting intermediary liability:[32]

> **Limit Internet intermediary liability**. Appropriate limitations of liability for Internet intermediaries play a fundamental role in promoting innovation and creativity, the free flow of information, incentives for co-operation among stakeholders and economic growth. Internet intermediaries, like other stakeholders, also play an important role in addressing and deterring illegal activity, fraud and misleading and unfair practices conducted via their networks and services. Proportionality and compliance with the protections of all relevant fundamental rights are important in this regard.

Although the principles are non-binding, this OECD guidance reflected a broad acknowledgement by many governments that intermediary liability protections play an important role in facilitating online expression and creative engagement.

2018

The Council of Europe in 2018 adopted the Recommendation of the Committee of Ministers to member States on the roles

30 https://africaninternetrights.org/en.

31 https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf.

32 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387.

and responsibilities of internet intermediaries (CM/Rec(2018)2)[33], applying a human rights-based approach to States and Internet intermediaries' responsibilities, leaving aside questions of liability.

3.7 Recent Intermediary Liability Trends and Risks to the Internet

Protections for intermediaries are viewed as having been instrumental in the growth of the Internet and for individual speech thriving on the Internet. Some countries, recognizing the benefits of safeguards for intermediaries, have codified liability protection in law. In other countries, the absence of laws protecting intermediaries may lead to court-crafted protections or more problematic treatment of intermediary functions.

In this section, we identify some recently proposed approaches to policymaking for Internet intermediary functions. Depending on the exact implementation, these approaches can create significant risks to the Internet and Internet users, including:

- Undermining the technical operations and reliability of the Internet.
- Weakening security and privacy on the Internet.
- Reducing Internet competition in a country because of the burdens or liabilities imposed on the ISP.
- Limiting the ability of individuals to share opinions and other speech on the Internet.
- Over-blocking of lawful content.
- Inappropriately excluding segments of the population from participating in the Internet.

We recommend a careful weighing of the risks listed above and other potential impacts on the Internet when considering these approaches to policymaking for intermediary functions. In later sections of this paper, we provide both general and specific advice to policymakers in how to avoid these and other risks.

Notice and Takedown: Not every regulatory regime has taken the same approach to intermediary liability. In one common variant, intermediaries may be held responsible and even liable for their users' content if they do not take certain actions. For instance, some legal jurisdictions have a "notice and takedown" approach, which requires an intermediary to

33 https://rm.coe.int/1680790e14.

remove content on receipt of a legally authorized notice from a court or authorized government agency. Significantly, there is usually no general obligation on intermediaries to monitor content.[34]

Knowledge: Others have required intermediaries to remove illegal or harmful content when they become aware of it, with varying levels of "knowledge" required, with the strictest being "actual knowledge."[35]

These modifications (notice and takedown, and knowledge) to the general approach operate after content has been uploaded or shared by a user.

Upload Moderation: Increasingly, there is growing interest in holding intermediaries, especially content-hosting intermediaries, responsible for filtering out certain types of content before it is shared, such as child sexual abuse material (CSAM). This is sometimes referred to as "upload moderation," and in some proposals, there is a desire to impose this obligation even on end-to-end encrypted messaging applications.[36]

These types of pre-publication content responsibilities are starting to be termed "due diligence" or "duty of care" responsibilities. Sometimes, they are also "conditional liability" approaches, where an intermediary will not be held liable **provided** they do something or prevent something.

Age-Specific Requirements: Some countries have pushed to impose greater responsibilities on intermediary entities to exclude certain age groups from their services or to modify the services or content they display to those users. Failing to take these steps may cause the intermediary service to be banned, blocked, or could make the intermediary entity liable depending on how the policy is implemented.

For example, intermediaries may be protected from liability for user-generated content in Indonesia if they ensure their systems do not contain or facilitate the dissemination of prohibited content. They must also have a governance framework for user-generated content that includes rights, obligations, reporting, complaints, accountability, and

34 However, the Zimbabwe Cyber and Data Protection Act 2021 amendments to the Criminal Procedure and Evidence Act provide that a hosting provider must, if it "obtains knowledge or becomes aware of any illegal information stored, promptly inform the appropriate authority to enable it to evaluate the nature of the information and if necessary, issue an order for its removal." Text available at https://www.law.co.zw/download/cyber-and-data-protection-act-chapter-1207/.

35 See, for example, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE) (Spain), available at https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758.

36 Obviously, if an intermediary providing end-to-end encrypted messaging is required to moderate content being sent between users, then the messaging can't be called end-to-end encrypted any longer.

provide information on users that make prohibited uploads and respond to "takedown notices."[37]

This policy approach is driving interest in technical mechanisms to verify a user's age and identity before they can use services or access content. Currently available mechanisms, however, raise serious concerns about effectiveness, privacy, security, and prevention of access to lawful online content.[38]

Traceability Requirements: Another approach that has emerged is to require intermediaries to be able to identify who posted content, even when a communication is end-to-end encrypted. As an example, in India, large social media messaging intermediaries must be able to identify the first originator of a message when required by judicial order.[39]

Removal of Intermediary Liability Protections: Reactions to early experience with Internet-specific policies have inspired some sweeping proposals. For example, in the United States, concerns about the largest platforms have resulted in overbroad proposals to remove *all* intermediary protections from *all* entities that are protected by the relevant law, Section 230. Similarly, in Brazil, questions about the ongoing validity of the approach taken in the Marco Civil da Internet to intermediary liability have been raised. Such proposals to amend or repeal intermediary protections, even at the proposal stage, have the direct impact of threatening the existence of the Internet's operations by creating uncertainty and the threat of unfettered liability for content produced by others.

Mandated industry codes: Some jurisdictions are mandating enforceable industry codes or standards[40] to create new legal obligations (such as safety-by-design, risk assessments, and enforcement of terms of services) for categories of intermediaries, e.g., social media, search engines, especially in the context of online safety.

37 Regulation of the Minister of Communications and Information, The Republic of Indonesia, Number 5 of 2020 on Private Electronic System Operators, see article 11, available at https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

38 See Internet Society, "Texas' Mandatory Age Verification Law Will Weaken Privacy and Security on the Internet," 23 Sep. 2024, available at https://www.internetsociety.org/blog/2024/09/texas-mandatory-age-verification-law-will-weaken-privacy-and-security-on-the-internet/.

39 Available on the MeitY website at https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf. At the time of this paper, the constitutionality of these rules is subject to various legal proceedings.

40 See, for example, the register of Australian online safety industry codes and standards, available at https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards.

We observe that policies in every jurisdiction are frequently crafted very broadly. Sometimes this is intentional, a way of being able to keep up with changing technology and uses of the Internet. Often, however, these broad policies have a profound adverse effect on the Internet and the ability of individuals to speak online.

3.8 A Global Diversity of Countries

This paper seeks to provide helpful policy guidance to countries around the world, from those with high levels of Internet penetration and well-developed Internet industries to those that are still expanding access and their digital economies.

We recognize that there are vast differences in law, culture, economics, politics, values, and even policy objectives concerning content on the Internet. We believe our policy recommendations will be useful for any policymaker considering regulations that would apply to intermediaries. The paper starts with a focus on the policy approach of protecting intermediaries from liability and why that approach has been important in enabling individuals to participate online. We also provide some constructive policy recommendations to address a wide variety of policy concerns.

We note that legal systems differ in how they approach problematic content online: some primarily focus on the person who posts the content, while others focus on the intermediaries that hosts or transmits that content. Further, while most countries have both public and private litigation to address problematic content online, some have more private litigation than others. These differences may have led countries to focus to different degrees on the issue of intermediary protections from liability. In all situations, however, a key recommendation is to avoid placing liability—whether civil or criminal—on intermediary functions because of content that a user or other third party posted. If such liability is imposed, it would undermine the ability of Internet users to speak and post content online. However, as noted in Section 4, there are many ways in which governments can constructively address policy concerns regarding online service providers.

It is also important when making policy to appreciate that entities providing intermediary functions vary by size, revenue, profit margins, and business model. Some are non-profit, and some, depending on

the country and business environment, may also be operated by governments. Some provide just one narrow function, while others are heavily integrated across a variety of related businesses. This leads to very diverse and sometimes opposite interests even within the same industry, and significant differences in their ability to effectively contribute to policymaking in this area.

Jurisdiction over online service providers may also vary from country to country. Depending on where an entity providing an intermediary function is located, jurisdictional issues may be difficult. It may be easier for countries to exert jurisdiction when an entity providing intermediary functions has business offices or infrastructure in that country. When content is hosted outside the country, jurisdiction may be more challenging, particularly when countries reach differing conclusions about the lawful nature of the same content.

Jurisdictional issues are important because incompatible laws and extra-territorial jurisdictional claims make it costly and perhaps even impossible for entities to deliver Internet intermediary functions globally. We urge policymakers to avoid creating laws with extra-territorial effects and to consider risks to the Internet globally.

4 Policymaking Principles for Internet Intermediary Functions

This section sets out three sets of principles the Internet Society believes will be useful for policymakers considering policies that affect Internet services:

1. Overarching principles that are applicable to any policymaking regarding the Internet or its use.
2. Principles specifically focused on protecting intermediaries from liability.
3. Broader examples of legal and policy principles that can be applied to intermediary functions without undermining intermediary protections from liability.

The Annex to this paper goes beyond these principles and provides detailed policy recommendations about a wide range of Internet intermediary functions. In the Annex, we also discuss technical and practical considerations for each of the **intermediary functions**. The information in the Annex is grouped by type of intermediary function, ranging from commonly recognized content intermediary functions such as content hosting and content delivery to crucial functions that enable data to be communicated, content to be located, and communications to be secured over the Internet.

4.1 Overarching Principles for Prudent Policymaking Concerning the Internet

The following principles should broadly guide any policymaking actions regarding the Internet in general, and intermediary functions in particular:

A. **Include stakeholders in policy development**: Policies will be more effective and more readily implemented if policymakers include other stakeholders throughout the policy development

process. Close involvement of stakeholders will ensure that relevant expertise and perspectives are included. We strongly recommend governments ensure the broadest participation of all relevant stakeholders in developing policies that affect the Internet.

B. **Conduct an Internet Impact Assessment**: The technical architecture and operations of the Internet can be directly—and often unintentionally—affected by policies, regulations, or laws applied to content on the Internet or intermediary functions that enable Internet communication. We strongly recommend policymakers undertake an Internet Impact Assessment of any new policy proposal, even one that seems narrowly tailored, to understand whether there could be any adverse effect on the Internet and its operations. The Internet Society has analyzed the critical properties and enablers that are essential for the Internet to exist and thrive and has developed an Internet Impact Assessment Toolkit to assist policymakers in this process.[41]

C. **Carefully scope any proposed regulation or law** to the specific intermediary functions that are causing the policy harm: There is a risk of sweeping in an overly broad set of intermediary functions, especially when the social policy concern is raised by a very narrow set of companies or intermediary functions. For example, if there is a concern about particular types of content being hosted by a group of websites, a policymaking proposal should be narrowly targeted to that type of content and that specific group of websites. Because intermediary functions are so critical to basic Internet operations and the ability of individuals to engage in speech online, any policymaking should be carefully targeted to avoid affecting an overly broad set of intermediary functions and entities.

D. **Don't use intermediary protections as a threat or bargaining chip**: Intermediary function protections are so foundational to the operation of the Internet that they should not be used as leverage in a public policy debate or as a penalty in regulation or law. A legislature should not, for example, enact a bill that says if a set of companies do not comply with a particular requirement, they would lose their intermediary protections. The ability of individuals to speak online should not be held hostage to other policymaking objectives. Policymakers should directly regulate or legislate

41 See Internet Society, The Internet Way of Networking: Defining the Critical Properties of the Internet, Sep. 9, 2020, available at https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/; Internet Society, Internet Impact Assessment Toolkit, Nov. 8, 2021, available at https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/introduction/.

to achieve their objective without threatening protections for intermediary functions or undermining how the Internet operates.

E. **Policy should promote openness**: Access to the Internet, services, applications, sites, and content facilitates individual participation. Open access enhances the user experience and the Internet's potential to drive innovation, creativity, and economic development. Policymakers should avoid limiting or blocking the availability of intermediary functions that provide access to the Internet, its applications, and services.

F. **Policy interventions should be as close to the harm as possible**: There is less likely to be collateral harm to other Internet users and the Internet if policy interventions focus on the problematic content and its origin. For example, rather than trying to block access to content via IP address or DNS blocking—which could also prevent access to legitimate content and disrupt Internet traffic—the person posting the content could be required to remove it.

4.2 Specific Principles Regarding Protecting Intermediaries from Liability

The following four principles focus on different aspects of the operations and work of entities that provide intermediary functions, and the need to provide protections for that work:

G. **Protect intermediary functions that enable communications on the Internet from liability for "user-generated content"—that is, content created by others**: Without liability protections, Internet infrastructure, as well as the basic tools that people use to access and interact with content, would be crippled with unbounded potential legal action. Without protections for these intermediary functions, the Internet could not practically operate. We strongly recommend that entities providing these Internet intermediary functions be protected from liability for the content created by others that they transmit, receive, cache, filter, or otherwise handle.

H. **Protect intermediary functions that host, facilitate, and optimize the delivery of "original site content" (that is, content created by the site owner)**: Entities that host the Internet's more than 1 billion websites should be protected from liability for content that their customers put online. If hosting companies were made responsible for the content put online by their customers, most could not

continue this service. This would especially affect small and medium-sized web hosts, driving up costs, stifling competition, and reducing the availability and diversity of content online. Site owners should remain responsible and potentially liable for the content on their websites, while entities providing intermediary functions such as web hosting, search engines, and caching should not be liable.

I. **Protect intermediary functions that host and display user-generated content**: Entities providing intermediary functions to host user-generated content should be protected from liability for that content. Without this protection, those intermediaries would not be able to continue to carry the content. This would dramatically and negatively impact the ability of individuals to post content and to engage in conversation and debate with other Internet users. Intermediary functions are a fundamental requirement for individuals to communicate their words, opinions, artistic creations, and conversations with others. Intermediary protections should be available to the entities that host user-generated content to ensure that users can continue to speak and share content online.

J. **Protect the intermediary functions of curating and moderating user-generated content**: An entity that hosts user-generated content *should* be able to set "rules of the road" for the types of discussions, creative works, or other content that it wishes to host. For example, if an entity hosting user-generated content chooses not to host "adult" content or chooses to set rules for users' behavior, the entity should be free to do so. These entities—performing intermediary functions of hosting user content—should also be protected from liability for removing irrelevant or objectionable content. Given the vast amount of user-generated content uploaded and shared every minute, curation is often critically important in helping users find a particular piece or type of content. Curation typically involves using one or more algorithms, from a simple algorithm that presents content in the order it is received to more sophisticated algorithms that present content based on a user's profile and interactions with the service. Filtering and "rules of the road" allow hosted content services and their users to avoid being overwhelmed with irrelevant, nuisance, and malicious material that drowns out legitimate content and drives away individual participation on the Internet. Intermediary protection regimes should protect entities from legal liability for enforcing their own rules of the road or removing objectionable content.

4.3 Specific Legal and Policy Principles that Can Be Applied to Intermediary Functions Without Undermining Internet Communications

Intermediary functions are essential for any content transmitted, hosted, or otherwise handled, and such functions require protection from liability for handling that content. But this does not mean that entities that provide these functions cannot be regulated. There is a broad range of policies, regulations, and laws that already apply, or can apply, to entities that provide intermediary functions, including, for example, competition and consumer protection laws. Below are some policy principles that could help address some of the policy concerns that have arisen about intermediary functions on the Internet:

User Privacy and Security

- Privacy and security are critical for protecting the confidentiality, integrity, and privacy of individuals' communications.
- Policies should apply strong rules to protect privacy and enhance the security of Internet communications.
- Entities providing Internet intermediary functions should also strive to incorporate "security-by-design" and "privacy-by-design," adopting industry best practices and innovating to enhance the privacy and security features of their functions.

User Control and Choice

- Providing users with the ability to choose and control the content they consume enables users to protect themselves by filter out irrelevant and unwanted content and sources.
- Policies should strive to enhance user choice and control over what online services they use and what content they choose to view.

User Accessibility

- The Internet should be available to all.
- Policies that promote robust accessibility can helpfully guide the design and implementation of intermediary functions to enable individuals with different accessibility needs to engage in online communication.[42]

42 See W3C Web Content Accessibility Guidelines 2.2 Understanding Documents at https://www.w3.org/WAI/WCAG22/Understanding/intro.

- Entities providing Internet intermediary functions should also strive to provide online content and controls that interact predictably and successfully with assistive technology.

User rights

- The Internet enables users to exercise their human rights online. Internet intermediary functions play a vital role in facilitating rights, including freedom of expression, freedom of association, and freedom to access information online. Government interference with the operation of intermediary functions risks preventing or hindering individuals from exercising their rights.
- Policymakers should assess, and avoid or minimize, the potential impact that any proposed policy concerning intermediary functions has on individuals' exercise of their human rights.

User digital skills

- Digital skills (also known as digital literacy) empower users to be more selective in the content they consume, to recognize content that may be misinformation, to manage privacy and security settings to protect their personal data, and to report unwanted content.
- Policies should promote digital skills for all users of all ages and needs, for example, by supporting digital education through schools, public libraries, government-funded programs, and community-led initiatives.

User non-discrimination

- Individuals have a right to be treated equally, regardless of categories such as race, color, sex, nationality, language, religion or ethnicity, national or social origin.[43]
- Policies should prevent discrimination against individual users or groups of users based on legally protected classes and characteristics in the provision of Internet services.

User knowledge

- Access to information about terms of service associated with hosting, curation, and moderating user-generated content empowers users to make informed choices about the services they use.

43 The list of protected classes and characteristics may vary depending on country and/or legal jurisdiction. Those listed here are drawn from Article 1 of the United Nations Convention on the Elimination of All Forms of Racial Discrimination, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial.

- Policies should encourage meaningful transparency about how content will be hosted, curated, and moderated.

User access to competitive services

- The Internet has historically been a tremendous place for small innovators and entrepreneurs to start and build businesses.
- Policymakers applying competition policy should be careful not to diminish intermediary protections.

User risks

- New intermediary functions or the application of known functions to new situations can have unintended consequences for users. This can include risks to users' safety, security, and privacy as well as the Internet itself.
- Policies should encourage a risk-based approach to the exercise of intermediary functions, rewarding mitigation of adverse effects while recognizing that there is no such thing as zero risk.

User reporting

- With the vast amount of content uploaded and shared every second, users may be the first to spot problematic content.
- Policies should encourage entities providing intermediate functions that display user-generated content to provide an easy means for users to report problematic content.

5 Spotlights — Policy Considerations for Specific Intermediary Functions

In this section, we build on the policy considerations listed above. The "Spotlights" identify specific scenarios that warrant deeper discussion. More details about the full range of intermediary functions are described in the Annex to this document.

5.1 Spotlight: Policy Considerations for "Social Media" Platforms that Host, Curate, and Moderate User-Generated Content

Much of the global public policy attention on entities that host user-generated content has focused on a small number of very large "platforms," particularly social media sites that are used by many users all over the world. Many of these concerns are *not* directly related to the intermediary protections that cover user-generated content. Instead, policymakers are concerned about issues such as an entity's collection and use of users' personal data, advertising practices, discrimination, lack of transparency and user control, and techniques for retaining users' continuing engagement on the platform, to mention a few current hot topics. None of these concerns have anything to do with the overarching objective of intermediary protections: protecting and encouraging individual participation on the Internet. It is not appropriate to address these concerns by removing or placing conditions on intermediary protections.

From the perspective of intermediary protections, a large social media platform hosting user-generated content is essentially no different than a small website that hosts user-generated content. Neither could operate if they were liable for defamatory, harassing, or illegal content posted by their users. There are more effective ways to address problematic

content that avoid exposing intermediaries to liability for user-generated content (outlined in section 4.3 above). Both types of intermediaries need strong protections for the intermediary functions involved in hosting user-generated content. A small website does not have the resources to pre-review all user-generated content and cannot operate with the risk of huge liability threats. A very large platform has similar constraints even if it has more resources because of the vast quantity of user-generated content—in multiple languages—that is uploaded by millions of users every minute.

However, intermediary protections from liability for user-generated content do not mean that policymakers are powerless to address important public policy concerns. For example, if the concern is that a platform is curating content so that it systematically presents a discriminatory selection of content to users, then existing or new non-discrimination laws could be applied to the platform. If the concern is that a platform is designing its user interface to seek to get users "addicted" to the platform, then health or consumer protection laws could be used to protect users from being exposed to an interface that is detrimental to their health, or one that subjects them to manipulation. If the concern is that a platform is misusing its users' personal data, then privacy and data protection laws could be applied to punish and deter those practices. If the concern is that a platform is misleading its users about its service, anti-fraud laws may be applied.

There are risks in *all* gathering places for social interaction—whether offline or online. Despite best intentions, social engagement by children on a playground can sometimes involve bullying and other unwanted behaviors. In-person social engagement among work colleagues can sometimes involve harassment. The online ecosystem may simultaneously exacerbate and mitigate some of the problems—the lack of direct physical interaction may increase the amount of harassment or bullying but may open opportunities for peer support. Further, the online space contains a vast number of venues for social interaction, so people may leave an overly toxic online space and join a more collegial one.

One major area of concern is the use of algorithms by platforms to choose and display content to users. Policymakers have identified the risk that algorithms could be used to manipulate users' behavior with adverse effects, discriminate against them, or spread unlawful or harmful content. However, algorithms have always been used by—and are essential to the operations of—social media platforms and an increasing number of other websites as well. The sheer volume of content shared on the Internet has

prompted an increasing reliance on algorithms that automatically sort and display content. Algorithms search for erroneous or malicious content. Algorithms improve e-commerce websites and manage the displayed content on social media platforms. Algorithms are also vital for increasing accessibility and converting voice into text captions for hard-of-hearing and deaf individuals.[44]

Our advice to policymakers is to remember that algorithms are not problematic *per se,* but how they are used might be. For example, an algorithm that systematically produces discriminatory outcomes against members of protected classes such as race or religion is a legitimate target for policymaking. The goal should be to craft policy that addresses the issue directly while allowing for appropriate use of algorithmic moderation and curation.

5.2 Spotlight: Policy Considerations for "Federated Networks" Enable New Approaches to Facilitate User Engagement.

"Federated networks" have garnered increasing attention over the past few years. We spotlight them because they apply a more decentralized approach to user-generated content hosting, sharing, curation, and moderation than more traditional social media platforms. Rather than having a single entity control a social media community, for example, federated technologies can enable many smaller communities to connect and share content throughout the federated ecosystem. This creates a similar social experience but with a more local approach to moderation.

"Federated" services have been in the news recently because some are now more directly competing with some of the very large social media companies and platforms. One example is Mastodon, based on the World Wide Web Consortium's ActivityPub standard.[45] Mastodon's functions are directly analogous with the Twitter/X type of global discussion capability. A major difference, though, is that Mastodon is a collection of servers operated by different entities that have chosen to participate in the federated network, rather than a set of servers controlled by one company. Significantly, each individual server participating in the

44 For a more detailed discussion of the issues, please refer to the Internet Society's Amicus Curie brief in Gonzalez v. Google LLC, 598 US 617 (2023), available at https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf.

45 https://www.w3.org/TR/activitypub/.

Mastodon federated network can set and control its own content moderation rules.[46]

Although federated social media has been a hot topic recently, federated services are not a new Internet phenomenon. For example, Internet email uses a federated model: millions of entities operate their own separate mail servers for their company, organization, university, or even households. Behind the scenes, these federated servers use email protocols to seamlessly send and receive emails from each other, without any prior arrangement.

In the area of social media, these nascent federated networks have the potential to democratize social media hosting. They offer the potential for much finer-grained content curation and moderation closer to the participating end user. The distributed model requires many Mastodon servers and has given rise to a new intermediary function, hosting a Mastodon server—the Mastodon equivalent of a web host or email service provider.[47] Significantly, the current success of federated social media networks prompted Meta to explore allowing its Threads users to share their posts to other ActivityPub-compliant servers, thereby reaching Mastodon users.[48]

Our concern is that federated networks could unintentionally be harmed by regulations or laws that are not crafted with an understanding of how modern federated networks fit into the "social media" landscape. As one possible example, if a country were to enact a law to apply to "social media services" with the intent to reach the largest platforms, that terminology could well apply to the entire federated network of the Mastodon system and its thousands of cooperating servers. A law aimed at the largest technology companies could end up affecting—and harming—an entirely different set of entities.

Our advice to policymakers seeking to regulate social media platforms is to be careful and cognizant of the likely impact of a proposed rule or regulation on federated networks. Without such care, there may

46 Mastodon rapidly gained popularity after X dramatically changed its content moderation policies. Mastodon allows users greater control over the content they see and the other users they engage with. It is a distributed approach to social media that empowers smaller entities and even individuals to host user-generated social media and make decisions about what content to allow or not allow on their own server and which other Mastodon servers to connect with.

47 For example, the SaaS provider Cloudflare offers a product: "Welcome to Wildebeest: The Fediverse on Cloudflare," The Cloudflare Blog, 2 August 2023, https://blog.cloudflare.com/welcome-to-wildebeest-the-fediverse-on-cloudflare.

48 Threads has entered the fediverse, Engineering at Meta Blog, 21 March 2024, https://engineering.fb.com/2024/03/21/networking-traffic/threads-has-entered-the-fediverse/.

be unintended harmful impacts on federated networks that offer an alternative to the larger social media platforms.

5.3 Spotlight: Policy Considerations for the Online Interactive Gaming Ecosystem

Online gaming has received particular public policy attention because many of its users are children and teenagers. For example, in 2011, South Korea passed (but later repealed) the Youth Protection Revision Act, restricting the hours in which children under the age of 16 could play online video games, blocking access between midnight and 6 a.m.[49] In 2019, China restricted minors to 90 minutes per weekday and banned them from playing online games between 10 p.m. and 8 a.m., imposing further restrictions in 2021.[50] Concerns range from addiction to gambling-like behavior, being exposed to inappropriate content, contact with strangers, and privacy violations.

Online gaming is often interactive with other users and frequently has features that enable users to communicate with each other in real time. The most common gaming communication tools are audio and messaging capabilities, but there are many more subtle methods of communicating: choosing and modifying avatars, particular behaviors during play, and sharing of scores, ratings, and other achievements. Some online games also permit users to upload and share modifications to the game. Online gaming has also inspired new genres of engagement on other platforms, such as YouTube and Twitch, and the field of esports.[51]

Our advice to policymakers is to be mindful of the intermediary functions being performed by online interactive gaming platforms. Today, most Internet-connected interactive gaming systems, with or without a hardware console allow a broad spectrum of "user-generated content," ranging from simple player-to-player conversations all the way to player-developed add-on modules that supplement and expand the gaming environment. Interactive gaming platforms perform intermediary functions, and major intermediary protection regimes apply equally to the gaming ecosystem.

49 The law was subsequently abolished in 2021. See https://en.wikipedia.org/wiki/Shutdown_law.

50 China keeping 1-hour daily limit on kid's online games, Associated Press, Zen Soo, 19 January 2023, https://apnews.com/article/gaming-business-children-00db669defcc8e0ca1fc2dc54120a0b8.

51 For more information about Esports, see Wikipedia at https://en.wikipedia.org/wiki/Esports.

However, as noted in our spotlight above on social media platforms, policymakers are not powerless to address harmful practices. For example, if the concern is that some so-called "loot boxes" in a game constitute deceptive practices or illegal gambling, consumer protection or illegal gambling laws should be directly applicable to such behaviors.

5.4 Spotlight: Policy Considerations for Internet-Connected Virtual Reality and Augmented Reality Systems

Virtual reality (VR) and augmented reality (AR) products are rapidly being added to the Internet's ecosystem. The purposes of VR and AR are diverse, but often they are used as part of an interactive communications system.[52] Some of these systems require a specialized device such as glasses, gloves, or headset, but others are accessible with a smartphone.

As with the gaming ecosystem, VR and AR systems connected to the Internet typically support "user-generated content," including a broad range of user-to-user communications.[53] Thus, like gaming, most major intermediary protection regimes could apply to VR and AR systems.

From a policy perspective, VR and AR systems overlap considerably with social media and other one-to-one or one-to-many communication services. However, VR and AR pose additional policy challenges, such as:

- The setting and use of representative avatars could create, at least in perception, a closer connection between the individual's real identity and their identity in virtual reality.
- Some AR systems can be used anywhere in physical space, superimposing virtual elements in the physical environment. These systems theoretically could lead to direct harm in the physical world, such as traffic accidents or personal injuries.[54]
- AR systems may be able to pull people who are not online and who haven't given consent into the augmented environment.

52 One vision of how VR might be used is the "metaverse," first described in the 1992 science fiction novel "Snowcrash" by Neal Stephenson. In his vision, the metaverse is a virtual reality space in which users can interact with each other using an avatar in a three-dimensional computer-managed environment.

53 By their nature, VR and AR systems can support a rich set of communication tools: written, spoken, and nonverbal such as head and hand motions, facial expressions, body orientation, proximity, and posture.

54 See, for example, the Pokémon Go Death Tracker at https://pokemongodeathtracker.com/.

As with social media and online gaming, our advice to policymakers is that policy concerns about issues such as privacy, user addiction, and personal safety are better resolved using existing laws in those areas rather than modifying intermediary protections or trying to construct a new set of policies specific to VR and AR.

5.5 Spotlight: Policy Considerations for Intermediary Functions that Enable Advertising on The Internet

Advertising content is a special kind of online content. While it often appears alongside user-generated content, it is not typically contributed by individuals. Some advertising may be considered original site content, such as an advertisement for a New Year's Day dinner special on a restaurant's website. However, the vast majority of advertising content that is displayed on the Internet is content created by entities other than the website owners for the specific purpose of advertising and is placed to obtain advertising revenues. Such content is usually embedded and dynamic.

The ability to display advertising content on the Internet has enabled companies to offer their services for little or no monetary charge, and for individuals to make money through user-generated content-sharing sites. Some argue that the advertising system should be protected from liability because without advertising "paying the bills," the Internet would have far fewer services and features and reduced individual participation. Without advertising revenue, more services would impose a fee for use, thereby increasing the digital divide.

Others believe that the advertising system—especially the behavioral advertisement system—is very problematic and should be significantly restricted. They say that targeted advertising exploits insufficient privacy protections, enabling online services and the industry to financially profit from user-generated content and online interactions.

Because of the Internet's global nature, the reach and impact of online advertising can be much greater than newspaper, television, and radio advertising. Online advertisements can be tailored and targeted to an individual user or very small groups of people in time, physical location, and context. Advertisers and the ecosystem of companies supporting online advertising track users across devices and even in the real world.

Beyond debates about the existing advertising system, the ad system unquestionably relies on intermediary liability protections in some contexts.[55] At the visible end of the ad systems—the websites and services where advertisements are displayed—intermediary protections may well come into play. In most services, the substance of advertisements displayed adjacent to user-generated content is out of the control of the user and usually not even controlled by the owner of the website. Technically, the advertising content displayed through a website is usually *not* hosted on the service's infrastructure but is hosted on a server managed by the advertising network.

Our advice to policymakers is to tread carefully in crafting regulation of the advertising ecosystem due to the difficult balancing of hoped-for benefits and potential harms. The online advertising ecosystem plays an important role in supporting broad access to speech, but at the same time, it raises policy concerns about privacy, inappropriate targeting, and misinformation. But, as with any other intermediary function, that does not mean that a government cannot regulate the ad systems directly. For example, in the European Union, the early eCommerce Directive directly imposed some specific transparency requirements on online advertisements, and the more recent Digital Services Act significantly expanded those transparency requirements and prohibited certain design techniques that sought to manipulate or deceive users.

5.6 Spotlight: Policy Considerations for Payments and Other Economic Compensation for "User-Generated Content" Covered by Internet Intermediary Principles

The Internet advertising system points to a much broader question—whether intermediary protections are appropriate to cover content for which money or another form of economic value changed hands as part of content placement on a website. The question can play out in a range of different scenarios:

- If a website carries articles written by users but only does so if a user pays the website to carry the article, should the website be protected from responsibility for the content it was paid to carry? What if the payment is very small? What if it is large?

55 The inner workings of online advertising systems are fairly opaque, with multiple interconnected and independent entities working together, both explicitly and implicitly. Untangling these systems to understand how intermediary liability protections might apply is far beyond the scope of this paper.

- If a website pays a content provider (such as a well-known "influencer" or other figure) to post content on the website, should the website have any legal responsibility for the content that it paid for and then hosted? Would the size of the payments make a difference to the analysis?
- If a website shares advertising revenue with the content provider, does this change the relationship and liability of the website?[56]
- If the commercial relationship between advertisers and websites removes protections and makes the website operator liable for the content of ads, how would this affect the advertising system? Would it harm websites that receive a modest amount of income from a low level of advertising?
- If liability protections were removed for intermediary functions for hosting user-generated content that was produced for economic compensation, would that cause economic, social, or technical impacts in the market for content? Would companies create artificial or less accountable alternatives to avoid liability?[57]
- If the market for paid content is dominated by a few entities that are heavily horizontally and vertically integrated across online services, how does this harm the competitive landscape for content?

In the context of the United States, payments for content in either direction generally do not impact the intermediary protections.[58] The questions we raise above help show the complexities, advantages, and disadvantages that come from focusing on economic compensation.

5.7 Spotlight: The Impact of Varying National Levels of Speech Protections

In understanding and creating policies related to protections from liability for intermediary functions, it is important to recognize the influence that national legal protections for speech and free expression will have

56 For example, YouTube has a system that is broadly open to all of its users who post videos to the site. In exchange for permission to post advertisements next to a user's videos, YouTube will share a portion of the advertising revenue that flows from the placed ads. If the user's videos are very popular, they would receive income from the ads—sometimes a substantial sum. Some content creators now make or significantly supplement their living from payments from YouTube. If YouTube were liable for the videos for which users were paid, would YouTube be able to continue offering the payments?

57 For example, would they seek to avoid liability by compensating select content creators for "having an account" rather than the content they produce, or would they offer other services and subscriptions for free?

58 Proposals to remove protections from US law for certain types of paid advertisements have not been successful.

on policies that could affect individuals' ability to communicate online, whether by sharing their own or others' content.

There are significantly differing protections for speech and free expression in different countries of the world, and those differences affect available policy choices within a country. Some countries establish a right to freedom of expression in their constitutions, including Brazil,[59] Ecuador,[60] Japan,[61] Peru,[62] and the United States.[63] Other countries and jurisdictions have fewer constraints on the ability of the government to, for example, mandate that private companies take actions to restrict or prevent certain types of speech. Other countries may prioritize other policy objectives, such as privacy over free speech or social cohesion over individual rights. Differing national regimes may go some way to explain the different national approaches to protections from intermediary liability. One example of different approaches being driven by constitutional or national laws are "notice and takedown" regimes, which are used by the European Union and some other countries to require the removal of online content. This type of mandate would face serious constitutional challenges if implemented in countries with strong rights to freedom of expression or speech, such as the United States.[64]

Our advice to policymakers is to carefully understand any constraints on regulations of speech imposed by national constitutional and statutory laws, as well as applicable international conventions and agreements on the freedom of expression.

Beyond these questions, if a country wants to support its citizens being able to participate in online conversations and start entrepreneurial efforts to create new online services, it must adopt protection for intermediary functions to ensure that Internet services can carry user speech without significant liability risks.

59 See Article 5 of the Constituição da República Federativa do Brasil, available at https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

60 See Article 66 section 6 of the Constitución del Ecuador, available at https://www.gob.ec/sites/default/files/regulations/2018-11/constitucion_de_bolsillo.pdf.

61 See Article 21 of the Constitution of Japan, available at https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

62 See Article 2 section 4 of the Constitución Política del Perú, available at https://www.congreso.gob.pe/constitucionyreglamento/.

63 See the First Amendment of the United States Constitution, available at https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say.

64 "Notice and takedown" regimes have also been notoriously subject to abuse and misuse. See, e.g., "Warning: repressive regimes are using DMCA takedown demands to censor activists," Jan. 13, 2023, available at https://www.accessnow.org/dmca-takedown-demands-censor-activists/; "Notice and Takedown Mechanisms: Risks for Freedom of Expression Online," Sep. 7, 2020, available at https://www.eff.org/files/2020/09/04/mcsherry_statement_re_copyright_9.7.2020-final.pdf; "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech," Sep. 2010, available at https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf.

5.8 Spotlight: Differentiating Intermediary Liability Protection from Copyright Law and Policy

In many countries and regions—including the United States[65] and the European Union[66]—there are distinct legal approaches that cover intermediary protections from liability for "user-generated content" differently from "third-party use of copyrighted content." In the case of user-generated content, the legal question is whether the content itself is illegal or caused harm. In the case of copyright, the pertinent legal questions are whether the poster of the content (a) owns the copyright, (b) has a license to post the content, or (c) is otherwise protected by "fair use" or other limitations on copyright law. This paper is focused on the first scenario, not on copyright-infringing content.

Many copyright-specific laws contain notice-and-takedown requirements under which a copyright owner can notify a hosting company about content asserted to be covered by copyright. Following notice, the host has a certain time to remove the specified content. The copyright-focused approach, which generally does not require a court order, has sometimes led to abuse, with persons using copyright takedown notices to prevent lawful speech.[67] By contrast, as noted in Section 3.5, the few countries that have adopted a notice-and-takedown approach for problematic user-generated content have typically required a court order.

5.9 Spotlight: Artificial Intelligence

Following the launch of consumer-focused generative AI services[68], a common question that has arisen among policymakers is whether and to what extent intermediary protections apply to services that utilize "artificial intelligence" (AI). AI is a very broad term that encompasses everything from fairly simple algorithms to artificial neural networks. AI

65 See Digital Millennium Copyright Act, 17 U.S. Code § 512, available at https://www.law.cornell.edu/uscode/text/17/512.

66 See Article 17 of the EU Copyright Directive (the Directive on Copyright in the Digital Single Market), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ:L:2019:130:TOC.

67 Sometimes referred to as "censorship by copyright." For some examples, see Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Speech (2010), Center for Democracy & Technology, available at https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf; Copyright shouldn't be a tool of censorship (2017) by Daniel Nazer and Mitch Stoltz, Electronic Frontier Foundation, available at: https://www.eff.org/deeplinks/2017/01/copyright-shouldnt-be-tool-censorship.

68 For an explanation of generative AI, see Wikipedia at https://en.wikipedia.org/wiki/Generative_artificial_intelligence.

tools can perform specific tasks (e.g., recognize images), react to specific situations (e.g., filter spam filter, increase routing efficiency), and learn and adapt responses (e.g., interact with users as chatbots). AI is already found across the Internet ecosystem, from Internet traffic routing to searching and locating web pages to managing literally billions of pieces of content.

In the context of online content, there are at least three aspects of AI worth spotlighting. The first concerns the use of AI in providing online services. Various kinds of AI have been used to provide online services for many years. For example, the technology used to select and curate content to be displayed to users has included aspects of AI since at least 2006.[69] The use of AI in online search dates back even further.[70] As discussed above in this paper and the Annex, intermediary protection laws generally protect activities that include curation, filtering, screening, choosing, and searching for content. These protections likely apply regardless of whether the technology includes an AI component.

A second and newer aspect relates to AI-generated responses to users' searches for information: whether the output of AI that was trained on vast amounts of user-generated content should themselves be viewed as "user-generated content." Views differ as to when AI-generated content should be characterized as "content created by others" and, therefore, covered by intermediary protections from liability. Although some output of such AI services might contain specific content that was user-generated, the totality of the output could be viewed as new content created by the service.

A third aspect of AI being actively discussed is whether AI services that produce text, images, sound, or videos in response to requests from users should be liable for producing illegal or unlawful content. These types of AI services clearly can enable individual user creativity, but it is also arguable that the AI service is a co-creator of the output content.

We do not seek to resolve these questions in this paper or to provide detailed policy recommendations on the treatment of AI-based services. These are not easy questions to answer, and it will likely take some time and careful analysis to develop appropriate policy approaches. AI offers tremendous potential for advances in medical, scientific, and even creative fields, and protections for AI-based services may be appropriate.

69 See Cait McNamara, "The Evolution of AI on Social Media," May 2024, available at https://favola.co.uk/the-evolution-of-ai-on-social-media/.

70 See Dan Katcher, "The Evolution of AI Search: Past, Present, Future," Feb 12, 2024, available at https://www.rocketfarmstudios.com/blog/the-evolution-of-ai-search-past-present-future/.

But some AI services can create significant risks for society, and they may warrant regulatory consideration.

As with all other types of policymaking discussed in this paper, the Internet Society recommends that policy interventions to address AI be carefully scoped and targeted. Without such caution, overbroad regulations or restrictions on AI could adversely impact other uses in intermediary functions that facilitate individuals' communication on the Internet.

6 Conclusion

This paper provides a framework for understanding Internet intermediary functions and developing policy concerning responsibility for online content. Our goal is to provide information to policymakers so that they can build policies that preserve what the Internet Society believes are the most important characteristics of the Internet: being open, globally connected, secure, and trustworthy. The Internet is increasingly important to peoples' lives and economic and social prosperity. As policymakers grapple with legitimate societal concerns about online content, it is critical that policies ensure that the Internet can continue to be a positive resource for global communication, education, and discourse.

Responsibility for user-generated content is an issue that has grown as the Internet has grown, becoming an essential communication medium for modern societies. Building policy approaches that provide liability protection for many different types of intermediary functions that enable Internet communication remains necessary for a healthy Internet. At the same time, there is a range of policy tools to address online concerns without harming individual participation on the Internet.

We believe that there are five key strategies that policymakers should follow when looking at building Internet-focused policies:

1. Carefully scope policymaking to achieve objectives. Use the narrowest set of policies possible to directly control and mitigate the concern.
2. Where possible, use existing policy tools to address specific concerns. Privacy, anti-discrimination, consumer protection, and other laws already offer ways to protect users and enhance online accountability.
3. Maintain, or where they do yet not exist, build liability protections for the functions that enable Internet communications. This is especially important for those functions that make the Internet work, but also those that most directly interact with users' communications, such as hosting and displaying content. Without these protections, the Internet cannot continue to be a medium for communication.
4. Protect the entities that provide the functions of curating and moderating user-generated content from liability. The scale of the Internet requires curation and moderation. With appropriate transparency, an entity that hosts user-generated content should be able to apply both automated and manual

curation and moderation without fear of attracting liability.

5. Work with Internet stakeholders (including civil society, academic and technical communities, businesses, and citizens) to conduct an "Internet Impact Assessment" of any proposed policy to help understand possible unintended consequences or effects on the Internet or its users.

The Internet Society strives to engage and work with governments worldwide to help develop policies that address societal concerns while still supporting the Internet. We work to support the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. We welcome discussions of opportunities, challenges, and concerns facing policymakers in the Internet ecosystem and ways to address them.

Annex – Intermediary Functions

This Annex to "A Policy Framework for Internet Intermediaries" ("Policy Framework") describes in detail the range of intermediary functions needed for communications to flow over the Internet. For each of these functions, we provide recommended policy approaches.

Our main focus is on intermediary liability protection. However, as noted in section 4.3 of the Policy Framework,[1] there are also other policy approaches that can be applied to address policy concerns regarding intermediary functions, such as privacy and consumer protection laws.

To help in organizing these recommended policy approaches, we have grouped related intermediary functions into eight separate sections (as set out in the table of contents).

1 Policy Framework Section 4.3, Specific Legal and Policy Principles that Can be Applied to Intermediary Functions Without Undermining Internet Communications.

1 Transmission of Data Packets

This section describes the most basic and foundational intermediary functions involved in the transmission of Internet communications – the transmission of data over wires or wirelessly.

- **Section 1.1** describes the function of providing a communication medium for Internet communications.
- **Section 1.2** describes the function of providing a communication path over a communication medium.
- **Section 1.3** describes the function of providing backbone or transit services that allow Internet access providers (also known as Internet service providers) with the ability to send and receive traffic across the Internet.
- **Section 1.4** describes the function of providing Internet access providers with the ability to exchange their traffic locally rather than using backbone or transit providers.
- **Section 1.5** describes the function of providing Internet access to an endpoint (a user's device).

1.1 Communications Medium (Wired and Wireless)

Description of function: providing the communications media to support the transmission of Internet Protocol network (IP) packets. Communications media are used in every part of the Internet, from the connection to a home or mobile device to "backbone" network providers to under the oceans. This intermediary function is essential for even the most basic of Internet communications.

Technical and practical considerations: IP packets can be transmitted over a "wire," over air, and even through space using various networking protocols that are specific to the medium. Communications media can be owned by or leased to a provider of an Internet Protocol communications path (see 1.2 below) and may carry other traffic than just IP packets. For example, capacity on an undersea fiber optic cable may be partly used for IP traffic and partly used for other proprietary data transmission protocols.

Examples of communications media include undersea cables, copper, coaxial, fiber to the home, and wireless over licensed or unlicensed radio spectrum.

Recommended policy approaches	Reasons for this approach
Providers of communications media should not be liable for the content that passes through their media.	Without liability protections, providers of communications media would be concerned about being liable for the content passing through their communications media. They may restrict access to their media to content from only a small number of pre-vetted sources. This would greatly reduce the sources and type of content transmitted via the communications media and would hinder individuals' ability to participate online. It would also fragment the Internet into different content networks.

1.2 Internet Protocol Communications Path

Description of function: sending and receiving Internet Protocol (IP) network packets via a network packet-switching system through one or more communications media. This function includes last-mile access (discussed below in section 1.5). On the Internet, endpoint-to-endpoint communications are achieved by traversing interconnecting communications paths (moving from network to network). Like communications media (described above), IP communications paths are used in every part of the Internet. An IP network delivers IP traffic without its customer necessarily knowing which communications paths will be or are used. This intermediary function of providing the IP communications path is essential for even the most basic of Internet communication.

Technical and practical considerations: The principal IP communications paths between large, strategically interconnected computer networks and core routers on the Internet are collectively known as the Internet backbone (described in section 1.3 below). These paths (otherwise known as routes) mostly use fiber-optic cables for large bandwidth, speed,

and limited signal attenuation. Networks that participate in the Internet backbone often have settlement-free peering agreements with neighbor networks to interconnect and carry traffic. Some networks, particularly those that are closer to the end-user, may have to pay for transit to have their traffic carried to the Internet.

Recommended policy approaches	Reasons for this approach
Providers of IP communications paths (IP network services) should not be liable for the content that passes through their networks.	Without liability protections, providers of IP network services would be concerned about being liable for the content passing through their networks. As a result, they may restrict access to their communications paths to content from only a small number of pre-vetted sources. At its extreme, a lack of liability protection could restrict Internet use to broadcasted content from a small number of companies and prevent individuals from being able to share their own content. It would greatly undermine the open and globally connected nature of the Internet.
Providers of IP communications paths should not be required to monitor and intercept the content of user traffic.	Monitoring or intercepting the content of traffic across IP communications paths (IP networks) is likely to severely degrade the speed and reliability of communications over such paths. It will also violate users' expectations of confidentiality, security, and privacy. The Internet Engineering Task Force considers pervasive monitoring[2] of IP networks to be an attack, regardless of the motivation.

2 "Pervasive Monitoring Is an Attack," Internet Engineering Task Force, Best Current Practice 188, RFC 7258, May 2024, available at https://datatracker.ietf.org/doc/html/rfc7258.

1.3 Backbone and Transit Networks

Description of function: providing a specific type of IP communications path known as backbone or transit networks. These networks interconnect and aggregate traffic from other IP networks, such as last-mile access providers. By doing so, they enable the flow of IP traffic to connect with all other parts of the Internet. This intermediary function is essential for facilitating even the most basic Internet communications.

Technical and practical considerations: Providers of backbone or transit network services are typically located in geographic areas where the demand is greatest, and it is most efficient to aggregate traffic. These networks are essential to carry Internet traffic to and from originating ISPs and other endpoints to destination ISPs and endpoints.

Recommended policy approaches	Reasons for this approach
Providers of backbone or transit network services should not be liable for the content that passes through their networks.	Without liability protections, these providers would be concerned about being liable for the content passing through their networks. As a result, they may restrict access to only a small number of networks. This would hinder global reachability and reduce the ability of individuals to communicate online.
Backbone and transit providers should not be required to monitor or intercept the content of user traffic.	The function of providing backbone or transit network services moves large volumes of Internet traffic through the Internet as efficiently as possible. The Internet would not be trustworthy or secure if providers of these services monitored or intercepted the content of the traffic they carry.

1.4 Traffic Exchange

Description of function: providing a physical location where multiple IP networks and content delivery networks can interchange packets. This intermediary function is critical for an efficient, robust, reliable, and secure Internet. With an Internet Exchange point, ISPs can exchange traffic locally rather than sending traffic to each other over a backbone or transit provider.

Technical and practical considerations: IXPs are the physical and usually neutral locations where different local networks connect to exchange traffic with each other, as well as backbone or transit providers participating in the IXP, as needed. IXPs create shorter, faster, and more direct routes for Internet traffic. They provide a more affordable and lower latency alternative to having to route local traffic through international networks. Traffic exchange at IXPs shortens and optimizes the transit path, reducing latency and cost.

Recommended policy approaches	Reasons for this approach
IXPs should not be liable for the content that passes through the exchange.	Without liability protections, there would likely be no one willing to operate or participate in an Internet traffic exchange point. Traffic would take inefficient and slower paths, costs would go up, and the Internet would be less affordable, resilient and sustainable.
Other than for effective traffic management purposes, exchanges should be discouraged from monitoring the content of, or intercepting, traffic that passes through the exchange.	The function of providing an Internet exchange is often shared by multiple IP communications path providers or IP network service providers. It is crucial that networks that use an IXP can be confident that the content of their traffic is not being monitored or intercepted. Otherwise, they may be reluctant to use the exchange because their customers do not want their communications surveilled.

Recommended policy approaches	Reasons for this approach
Internet Exchange Points should not be required to intercept, filter, or monitor the traffic passing through the exchange.	Requiring IXPs to inspect or scan for specific content would discourage ISPs from participating and harm the security of users' communications and privacy. Such an approach would undermine trust in the Internet, and hinder efficient exchange of Internet traffic.

1.5 Last Mile Access to the Internet

Description of function: providing end-users (and their devices) with access to the Internet, often referred to as "last mile access." This is a specific type of IP communications path (described in section 1.2 above). This function, which includes carrying IP traffic to and from the end-user, is essential for even the most basic of Internet communications.

Technical and practical considerations: Internet access can be provided to end-users through one or more means, including DSL, cable, wireless, mobile, fiber-optic connections, and satellite. Internet access is often supplied by a commercial Internet Service Provider (ISP), but some end-users access the Internet through a community network. From a technical point of view, last-mile access is no different from other IP communications paths, but it is often treated differently in some jurisdictions because of historical regulation of providers of communications services to end users.

Recommended policy approaches	Reasons for this approach
Providers of Internet access to end-users should not be liable for the content that passes through their networks.	Without liability protections, these providers would be concerned about being liable for the content their customers send and receive. As a result, they may restrict the content that end-users can access via, or transmit to, the Internet. They may try to impose download and upload filters which would undermine the security and privacy of their customers' use of the Internet. Further, to reduce the risk of liability, providers would likely over-block content, preventing end-users from sharing legal content online. Without these protections, the open globally connected secure and trustworthy Internet would be undermined.
Other than for security and effective traffic management purposes, providers of Internet access to end-users should be discouraged from monitoring or intercepting the content of users' traffic.	A fundamental principle of Internet access (often described as "net neutrality") is that Internet access providers should provide Internet access without regard to the content being carried on their networks. If providers of Internet access to end-users do not follow this principle, and apply different access depending on content, this would violate a critical property of the Internet, that it is a general-purpose network (see the Internet Way of Networking, Defining the critical properties of the Internet[3]). End-users may also restrict how they communicate online, fearful that their communications are being monitored.

3 Internet Society, "Internet Way of Networking, Defining the critical properties of the Internet," Sept. 2020, available at https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf.

2 Routing and Ancillary Functions that Facilitate Internet Communications

This section describes the various intermediary functions involved in addressing and routing, which are essential for an efficient, robust, reliable, and secure Internet.

2.1 IP Address Allocation

Description of function: allocating unique IP addresses to networks and users. This intermediary function is essential for even the most basic of Internet communications because every Internet communications path needs a starting point and a destination, as well as intermediary "hops," each identified by a unique IP address.

Technical and practical considerations: IPv4 and IPv6 addresses (otherwise known as Internet number resources) are delegated from the Internet Assigned Numbers Authority (IANA) to regional Internet registries (RIRs[4]) for fair allocation in the RIRs' regions. Within a region, the RIRs allocate IP addresses to IP network providers and end-user organizations. In some countries, RIRs also allocate IP addresses to national Internet registries. IANA and the RIRs are non-profit organizations governed by multistakeholder processes for networks and users all over the world. The five RIRs include AfriNIC[5] in Africa, the Asia Pacific Network Information Centre (APNIC[6]), the American Registry for Internet Numbers (ARIN[7]), the Latin American and Caribbean Internet Addresses Registry (LACNIC[8]), and the RIPE Network Coordination Centre (RIPE NCC[9]).

4 https://www.nro.net/about/rirs/.

5 https://www.afrinic.net/.

6 https://www.apnic.net/.

7 https://www.arin.net/.

8 https://www.lacnic.net/.

9 https://www.ripe.net/.

Recommended policy approaches	Reasons for this approach
Providers of IP address allocation services should not be liable for the content that is communicated using IP addresses they have allocated.	Without liability protections, providers of IP address allocation services, concerned about being liable for the content communicated using the IP addresses they allocated, may vastly restrict to whom they allocate IP addresses and under what conditions. This would shrink the Internet and prevent many users from being able to communicate online.
IP address allocation services should not be required to control illegal or unwanted content on the Internet.	IP addresses are often shared by more than one end-user and can be re-assigned to other users in the same or another country. Similarly, IP addresses are often shared by more than one content host. Interference with IP address allocation or IP address use to control content risks directly preventing users from sharing lawful content, as well as preventing content hosts from making lawful content available on the Internet.

2.2 Autonomous System Number Allocation

Description of function: allocating unique numbers to a group of IP networks operated by one or more network operators (providers of IP communication paths, described in section 1.2 above) that have a single and clearly defined external routing policy. Such a group of networks is referred to as an Autonomous System (AS), and the unique number that identifies it is its Autonomous System Number (ASN). This function is similar to the IP address allocation function (described above). It is a critical piece of the Internet traffic routing system that is used to help identify which communication paths are used to route Internet traffic.

Technical and practical considerations: ASNs are delegated from the Internet Assigned Numbers Authority (IANA) to regional Internet registries (RIRs) for allocation in their regions. RIRs allocate ASNs both to IP network providers and to end-user organizations. See section 2.1 above, "Technical and Practical considerations," for more information on IANA and the RIRs. There is a lot of diversity in ASNs. Some are very complex, comprised of multiple independent networks and users, and some are simpler.

Recommended policy approaches	Reasons for this approach
Providers of ASN allocation services should not be liable for the content that is communicated using ASNs they have allocated.	Without liability protections, providers of ASN allocation services may only be willing to allocate ASNs to a very small number of large established providers of network services, limiting the growth and diversity of networks on the Internet. This would likely have severe, negative, and unpredictable effects on the Internet and Internet access.
ASN allocation services should not be required to control illegal or unwanted content on the Internet.	Interfering with the allocation of an ASN is likely to prevent reliable and efficient routing of Internet traffic, may prevent networks from participating on the Internet and risks preventing broad range of users from sharing and accessing lawful content.

2.3 DNS Registration and Management

Description of function: facilitating the registration, renewal, and management of domain names for publication in the Domain Name System (DNS). This intermediary function is essential for Internet communications involving the use of domain names. Domain names are the "human readable" addresses of networks, servers, websites, and other endpoints on the Internet.

Technical and practical considerations: Domain names are important because they allow humans to navigate the Internet, instead of

remembering IP addresses such as "192.0.2.1". DNS registration and management includes the registration of domain names through accredited registrars, ensuring DNS zone integrity, and maintaining Registration Data Directory Service (RDDS, historically called WHOIS) information. Effective management includes ensuring compliance with policies, including consensus policies set by the community working through the Internet Corporation for Assigned Names and Numbers (ICANN) for "gTLDs" ("generic top-level domains"), and policies set by national bodies for "ccTLDs" ("country code top level domains") which are controlled by each country.[10] This function is performed by multiple organizations working collaboratively. This includes DNS registries (which manage gTLD and ccTLD top-level domains) and registrars (which handle the registration of domain names for individuals or entities so they can use the domain name on the Internet).

Recommended policy approaches	Reasons for this approach
Providers of DNS registration and management services should not be liable for the content that is communicated using domain names that they register or manage.	Failing to provide protections from liability for DNS registration and management service providers for content hosted under particular domain names would likely have a chilling effect on the ability of people to speak online. Without liability protections, providers would likely significantly restrict who can register domain names and how domain names can be used. It may even drive smaller competitors from the DNS market, decreasing competition and increasing the cost of domain name registration.

10 Countries can set their own policy for ccTLDs. The operation of some ccTLDs has been delegated by the country to an external entity that allocates domains on a commercial basis.

Recommended policy approaches	Reasons for this approach
DNS registration and management services should not be required to control illegal or unwanted content on the Internet.	Domain names are a critical part of how people interact with the Internet. Burdening the DNS registration system by requiring it to be part of content controls would lead to limits on who can register domain names and for what purpose, greatly reducing the ability of people to use the Internet.

2.4 DNS Publication

Description of function: making available the registered DNS data on authoritative DNS servers so that the information is available for DNS lookup (discussed in section 2.5 below) by everyone on the Internet. This intermediary function is essential for Internet communications involving the use of domain names. This function also covers (a) the operation of "root servers" that provide information about how to reach the authoritative DNS server for each top-level gTLD or ccTLD domain, and (b) the provision of copies of the authoritative DNS server information for resiliency, reliability and more efficient DNS lookup responses.

Technical and practical considerations: The DNS is a hierarchical system. For each top-level domain (such as .com), there is an intermediary that publishes the authoritative information about the domain on a DNS server known as a "root-server."[11] These intermediaries are often called "root-server operators." They are usually the DNS registry to which ICANN has delegated the management of that top-level domain. Virtually every Internet communication relies on the proper operation of the DNS publication function to ensure traffic is routed to the correct location on the Internet. The integrity and reliability of the DNS server system is crucial for the Internet's operations. Copies of authoritative DNS information can be used to improve the efficiency and speed of the DNS system.

11 https://root-servers.org/.

Recommended policy approaches	Reasons for this approach
Providers of DNS publication services should not be liable for the content that is communicated using domain names they publish.	Disruption of DNS registration and management services would directly harm the Internet's operations by disrupting users' ability to locate the servers where content and other resources are hosted. If DNS publication service providers could be held liable for content hosted under domain names they publish, they may cease providing the DNS publication function or to only provide it to pre-vetted domains. This would have severe, negative, and unpredictable effects on Internet communications.
DNS publication services should not be required to control illegal or unwanted content on the Internet.	Reliable and fast access to reliable and trusted published DNS data is critical for efficient Internet operations. Preventing DNS publication or specifying which domains in what circumstances can be published would fragment the Internet and make the Internet untrustworthy.

2.5 DNS Lookup

Description of function: translating domain names to their currently correct numeric IPv4 or IPv6 addresses (as well as some other information). Typically, users use domain names to locate websites and other resources on the Internet that they wish to access. Domain names need to be converted to the correct IP address to enable networks, servers, and end-users (devices) to connect with each other. This function is provided by specialized servers called recursive domain name servers (recursive DNS servers), which obtain their DNS information from authoritative DNS servers (see section 2.4 above). They store the mapping between domain names and IP addresses and respond to requests to lookup domain names and return IP addresses (or other requested information).

Technical and practical considerations: Recursive DNS servers are located in many different parts of the Internet. To speed up the Domain Name System, most end-user computers do not talk to authoritative DNS servers. They request DNS information from recursive DNS servers. Some recursive servers are offered to the entire world (often called "open DNS servers"). Others are operated by Internet Service Providers (ISPs), other network operators, and private enterprises primarily for the use of their users. Occasionally, individuals operate their own recursive servers for personal use. They are operated by individuals on their own computers, generally for their own personal use. Although the primary function, DNS lookup, might be the same, many users choose a particular DNS provider for security and privacy reasons.

Recommended policy approaches	Reasons for this approach
Providers of DNS lookup services should not be liable for the content that is communicated using responses they provide to DNS lookup queries.	Without liability protections, providers of DNS lookup services would likely limit the ability of users to use the DNS system to access Internet content. Content would be unreachable without knowledge of the specific IP address of the website or other Internet resource. This would have a severe and negative impact on Internet communications.
DNS lookup services should not be required to control illegal or unwanted content on the Internet.	Blocking access to domain names through DNS lookup services (recursive DNS servers) creates significant risks of over-blocking content, preventing access, and fragmenting the Internet. Attempts to require content filtering via recursive DNS servers breaks the integrity of the DNS and will make it untrustworthy.

2.6 DNSSEC Services

Description of function: providing authentication for domain name records stored on authoritative DNS servers. This function is fulfilled by providing public key cryptographic signatures for those records. The purpose of this function is to protect the integrity of domain name records, and to provide a mechanism for validating that the IP address (or other information) returned from a DNS query is what the operator of the domain intended to provide. DNSSEC is a crucial intermediary function that ensures that there is no tampering with the domain name record.

Technical and practical considerations: DNSSEC—a security protocol developed by the Internet Engineering Task Force (IETF)—helps to prevent a range of cybersecurity attacks on Internet communications. Without DNSSEC, an attacker could, for example, corrupt DNS data in transit by changing the IP address that corresponds to the website a user wants to access, thereby directing them to the attacker's website. When deployed correctly, DNSSEC secures all the DNS records relating to a domain name. These records can be used to locate services such as instant messaging and email, as well as to support antispam measures that depend on DNS.

Recommended policy approaches	Reasons for this approach
Providers of DNSSEC services should not be liable for content that is communicated using domains protected by DNSSEC.	DNSSEC protects the integrity of DNS results regardless of the underlying content. Without protections from liability, DNSSEC service providers would directly reduce the use of DNSSEC. This would have the effect greatly reducing the security of Internet communications.

2.7 TLS Certificate Services

Description of function: creating, storing, and issuing cryptographically signed Transport Layer Security (TLS) certificates for creating secure connections to a server on the Internet. TLS certificates are generally issued by a Certificate Authority ("CA"). A common use for TLS certificates is securing web traffic to prevent eavesdropping and tampering. Issuing TLS certificates is an essential intermediary function that is necessary for a reliable and secure Internet.

Technical and practical considerations: A TLS certificate is digitally signed and issued by a CA and contains information such as the domain name, the entity (person, organization, or device) that it was issued to, the issuing CA's name, and its period of validity. TLS certificates protect the integrity and authenticity of cryptographic public keys, which are used to establish encrypted HTTP (HTTPS) sessions to secure web traffic against eavesdropping and tampering. TLS is a vital tool to keep communications over the Web secure.

Recommended policy approaches	Reasons for this approach
Entities which provide TLS certificates should not be liable for the content that is secured using those TLS certificates.	TLS is intended to protect traffic on the Internet, regardless of its content. Imposing liability for content on providers of TLS certificates would undermine the security of communications on the Internet. If entities providing TLS certificates could be liable for the content that is transmitted using their certificates, they will be reluctant to issue TLS certificates, especially to individuals and smaller entities, rendering the Internet less secure for all Internet users.

3 Hosting and Caching Services

The first two groups of functions (outlined in the sections above) enable communications over the Internet. This third section describes functions that enable content to be made available on the Internet, including user-generated content created by individuals and smaller entities.

3.1 Web Hosting

Description of function: providing and operating servers and other resources needed to host websites or other web resources and applications, and make them accessible over the Internet. This intermediary function enables individuals and others to share content with other users via the World Wide Web.

Technical and practical considerations: Hosting a website involves operating servers that (a) store a website's or web application's files, databases, software, and code, and (b) receive and respond to requests from users to access the content on the site. Entities that provide hosting may also provide other related services, including technical support, backup solutions, and security. Many individuals, businesses, non-profits, and governments rely on third-party web hosting services rather than acting as their own web hosts. These web hosting services typically offer more secure, less expensive, and more reliable hosting of websites.

Recommended policy approaches	Reasons for this approach
Providers of web hosting services should not be liable for the content of their direct customers or the content provided by users of their customers' web sites.	If entities providing web hosting services could be liable for the content on their customers' websites, service providers would be reluctant or unable to provide web hosting services, especially to individuals and smaller organizations. Without liability protections, hosting service providers may severely restrict who can post content online and what content they can post, thereby significantly limiting the ability of individuals to communicate on the Internet.
Providers of web hosting services should not be required to inspect or remove content placed by their customers.	Making providers inspect and remove content would undermine their ability to operate as website hosts, especially smaller providers. They may restrict their services to pre-vetted content from a small number of websites and users would have limited options for making their content available on the Internet.
Providers of web hosting services should not be required to control illegal or unwanted content.	Responsibility for problematic content should be placed on the person or entity that posted the content, not on a service provider hosting the content.

3.2 Email Hosting

Description of function: providing and operating email servers to send, receive, store, forward, and otherwise manage email services on the Internet. This intermediary function is essential for email, a major tool for communications over the Internet.

Technical and practical considerations: Email hosting involves operating servers that send, receive, store, forward, and otherwise manage email. Email hosting providers may also provide other related services, such as technical support, archiving, spam filtering, and compliance support. Most Internet users, whether personal or organizational, now rely on third-party email hosting. Generally, third-party providers can offer more secure, less expensive, and more reliable email services than many individuals and businesses can provide for themselves.

Recommended policy approaches	Reasons for this approach
Providers of email services should not be liable for the content of email sent or received by their users.	If entities providing email services could be liable for the content of their customers' sent or received emails, service providers would be reluctant or unable to provide email services, especially to individuals and smaller entities. Without liability protections, providers of email services may be forced to seek to surveil and censor email messages. As a result, email would no longer be a useful tool for person-to-person communications.
Providers should not be required to remove content or block users' ability to use their services.	Responsibility for problematic content should be placed on the person or entity that transmitted the content, not on the email hosting provider or other providers facilitating the transmission of email. Placing a burden on the hosting provider would undermine the ability of small providers to operate in the market, and could harm the trust, integrity, and reliability of email.

3.3 Other Hosting

Description of function: providing and operating servers that host content, files, databases, software and code, and other resources that enable others to operate a vast array of apps, sites, and services to send and receive communications over the Internet. Because the vast majority of apps and offerings on the Internet—especially those offered by startups and small or medium enterprises—use hosting services, this intermediary function is essential for the availability of a diverse set of services and apps on the Internet.

Technical and practical considerations: Hosting involves operating servers that (a) store content, files, databases, software, and code that make up an online service or application and (b) enable users to interact with the service or app. Providers of the hosting function may also provide other related services, including technical support, backup solutions, security, and Internet access. Many users rely on third-party hosting services because such providers can offer more secure, less expensive, and more reliable hosting than many individuals and businesses could provide for themselves.

Recommended policy approaches	Reasons for this approach
Providers of hosting services should not be liable for the content of their customers or the customers' users.	If entities providing hosting services could be liable for the content sent or received by customers or the customers' users, service providers would be reluctant or unable to provide the function, especially to individuals and smaller entities. Without liability protections, innovation on the Internet would decrease and content hosting would be limited to a small number of large providers.

Recommended policy approaches	Reasons for this approach
Hosting service providers should not be used to control illegal or unwanted content on the Internet.	Responsibility for problematic content should be placed on the person or entity that transmitted the content, not on a provider hosting the content. Placing a burden on the hosting provider would undermine the ability of small providers to operate in the market and users would have more limited options for making their content available online.

3.4 Caching and Content Delivery Services

Description of function: temporarily storing copies of content closer to the end-user to reduce latency and costs for frequently accessed content. Caching services are a special type of hosting service, usually involving temporarily storing copies of other content closer to the end user. Content delivery networks (CDNs) use geographically dispersed data centers and networks to deliver their customers' content faster to end-users. Typically, their customers are large content distributors such as streaming services. These caching and content delivery services are crucial for the efficient operation of the Internet.

Technical and practical considerations: Some caching functions are provided by browsers (discussed below). However, on the Internet, the principal caching function is typically offered by a CDN, which operates a network of distributed servers. The caching function can also be offered by Internet Service Providers to help speed access to content for the ISP's customers. In both cases, caching servers store temporary copies of popular content, such as web pages, videos, or images. Since these servers are distributed in different networks across the Internet, this means that copies of desired content can be closer to users and more quickly accessed. This reduces the distance that the content must travel, which reduces load time and latency, and improves the user experience. Caching also lowers the cost of distributing content by avoiding retransmission of the same content over and over. Decisions about what content to cache, and for how long, are typically automated based on specific caching algorithms.

Recommended policy approaches	Reasons for this approach
Providers of caching and content delivery services should not be liable for the cached content.	If entities providing caching or content delivery services could be liable for content temporarily stored on their servers, the service providers would be reluctant or unable to provide the services, which would increase costs, directly reduce efficiency, and negatively affect the user experience.
Caching service providers should not be used as control points for illegal or unwanted content on the Internet.	If caching service providers were required to control content, they would only cache known and vetted content. This would effectively increase costs for smaller content providers and make them less attractive to Internet users because of the reduced quality of the user experience. Users will lose access to a rich diversity of content, with local content likely to suffer the most.

3.5 Application Programming Interface (API) Content Delivery

Description of function: hosting and delivering content via an API, or Application Programming Interface, which is a set of rules or protocols that allow computer servers to communicate information from one machine to another. APIs are very common tools used in a broad range of contexts to send and receive information over the Internet, and in some of those contexts, they are used to transmit user-generated content. In a common use case, for example, APIs can allow the display of blog or social media posts embedded within other web pages.

Technical and practical considerations: This function is very similar to the general hosting of web-based content discussed above but sometimes uses different technical protocols or capabilities to request and send the content.

Recommended policy approaches	Reasons for this approach
Providers of API services should not be liable for user content delivered through their services.	If entities providing API services could be liable for user content delivered through their services, they would be reluctant or unable to provide such services, thereby reducing the ability of people to publish and receive lawful content over the Internet.
API services should not be used to control illegal or unwanted content on the Internet.	APIs are fundamental tools throughout the Internet ecosystem, and any attempt to use them as a means to control online content risks walling off content within services, greatly reducing interoperability and innovation.

3.6 Curation, Moderation, and Display of Content

Description of function: organizing and, in some cases, selecting content to display to users. We distinguish this from web hosting, described above in section 3.1, by the additional functions provided, such as curation or moderation. These are very commonly provided in user-generated content websites. This function may be provided both in an automated way using algorithms and automation and, at times, in a manual way by individuals.

Technical and practical considerations: The curation function is commonly provided by hosts of user-generated content, which needs to manage and organize a vast volume of submissions. There are many reasons to provide this function. For example, hosts may screen out content that violates their terms of service. They will likely also present the content to users based on their interests and preferences, viewing history, or other criteria. These functions enable the practical management of content on user-generated content sites. Curation and moderation decisions are likely to be more relevant to users and understood by them if they take into account cultural, linguistic, and other contextual factors.

Recommended policy approaches	Reasons for this approach
Organizations providing the functions of curation, moderation, and display of content to users should be able to do so without risk of liability for that content.	If entities providing curation and moderation functions could be liable for the content or those functions, they would be reluctant or unable to provide those functions. Without any curation and moderation, user-generated content would be unsorted and disorganized. It would be challenging for users to share content with their audiences and to locate the content they want.
The ability to curate and moderate should not be restricted.	Without curation and moderation—which are essential to block spam and irrelevant content and to provide content of interest to users—content hosting sites would likely become unmanageable for operators, and undesirable for site visitors.

4 Communications To and From People

This section includes a fourth group of functions that focus on different communication modes that allow people to engage in person-to-person communications over the Internet. These functions are essential for people—and small organizations and businesses—to interact over the Internet.

Some aspects of these functions overlap with other intermediary functions in this Annex. However, it is important to describe them independently because these are fundamental functions that have recurred over and over in new services delivered over the Internet. For example, messaging apps are a relatively recent innovation that combines the functions of one-to-one communications and one-to-many communications.

4.1 One-to-One Communications

Description of function: providing a reliable means of sending, receiving, displaying, routing, and otherwise supporting discrete communications—in real time (synchronously) or for later delivery (asynchronously) between a sender and receiver. This function may, in some cases, be coupled with a "discovery" function to search for other users of a particular service (for example, by name or phone number) to allow users to connect with other users.

Technical and practical considerations: This function defines a broad capability for people (and organizations) to communicate with one another. The function is part of a wide range of services, including what is often termed email, text messaging, chat, direct messaging, and other tools. It can include person-to-person communications in a wide range of environments, such as web-based sites, video conferencing, gaming, social media, and other contexts. Some environments may also include the ability of an individual speaker to direct the same content to more than one recipient at a time (which overlaps with the one-to-many function discussed in section 4.2). Some of these services offer enhanced

security and privacy as a distinguishing feature based on end-to-end encryption (E2EE), decentralization, or other technologies.

Recommended policy approaches	Reasons for this approach
Providers of one-to-one communications services should not be liable for the content sent or received by their users.	If entities providing one-to-one communications services could be liable for the content of their users' communications, they would be reluctant or unable to provide the services, especially to individuals and smaller entities. Without liability protections, providers may be forced to stop offering the service or over-censor messages—including lawful speech—to avoid liability. The result would be a reduction in the ability of people to communicate online.
Providers of one-to-one communications services should not be responsible for addressing problematic content sent or received by customers	Responsibility for problematic content should be placed on the person or entity that transmitted the content, not on a service provider hosting or delivering the content. Placing proactive content review burdens on providers of one-to-one communications could well drive providers (especially smaller providers) out of business and thereby reduce the ability of users to communicate one-to-one. It may also cause them to remove critical privacy and security protections such as end-to-end encryption.

4.2 One-to-Many Communications

Description of function: providing a reliable means of sending, receiving, displaying, routing, and otherwise supporting discrete communications—in real time (synchronously) or for later delivery (asynchronously) from a sender to a defined group of recipients (which may or may not be defined

or controlled by the sender). The recipients may or may not have the ability to respond and engage in conversation within the larger group.

Technical and practical considerations: This function defines a broad capability for people (and organizations) to communicate with groups of recipients. The function is part of a wide range of services, ranging from decades-old email mailing list services to more modern video webinar services. Some of these services may offer enhanced security and privacy as a distinguishing feature, such as end-to-end encryption (E2EE) or decentralization. Generally, participants in one-to-many communications have the option to leave or "unsubscribe" from the group or to block communications from particular senders.

Recommended policy approaches	Reasons for this approach
Providers of one-to-many communications services should not be liable for the content sent or received by their users.	If entities providing one-to-many communications services could be liable for the content of their users' communications, they would be reluctant or unable to provide the services. Without liability protections, the providers may be forced to stop providing the service or over-censor messages—including lawful speech—to avoid liability. The result would be the reduction in the ability of people to communicate online.

Recommended policy approaches	Reasons for this approach
Providers of one-to-many communications services should not be responsible for addressing problematic content sent or received by customers through content review and filtering.	Responsibility for problematic content should be placed on the person or entity that transmitted the content, not on a service provider hosting or delivering the content. If providers are required to proactively monitor the forum for undesired content, that burden would likely reduce the ability of providers (especially smaller ones) from hosting such a forum. Providers should be protected if they choose to remove or block a user who violates terms of service or the norms of the group.

4.3 Many-to-Many Communications

Description of function: providing a reliable means of sending, receiving, displaying, routing, and otherwise supporting communications—in real time (synchronously) or for later delivery (asynchronously) from senders/content creators to all users of a service or another broad, undefined group of recipients not controlled by the sender. Recipients or viewers may or may not have the ability to respond and engage in conversation within the larger group.

Technical and practical considerations: This function defines a broad capability for people (and organizations) to communicate to the public or other large groups of people (such as all users of a particular service). The function is part of a wide range of services, including, among other services, collaborative "wiki" sites, collaborative content/software development sites, image/pre-recorded video sharing sites, live video streaming services, and social media sites. Some of these services may offer users the ability to limit the distribution of their posts or content to a defined group of people (thus overlapping with the one-to-many function described in 4.2 above). Some providers of many-to-many communications offer users the ability to block communications from particular senders or to unsubscribe from the group.

Recommended policy approaches	Reasons for this approach
Providers of many-to-many communications services should not be liable for the content sent or received by their users.	If entities providing many-to-many communications services could be liable for the content of their users' communications, they would be reluctant or unable to provide the services. Without liability protections, they may be forced to stop providing the service or over-censor messages—including lawful speech—to avoid liability. The result would be the reduction in the ability of people to communicate online.
Providers of many-to-many communications services should not be responsible for addressing problematic content sent or received by customers through content monitoring and filtering.	Responsibility for problematic content should be placed on the person or entity that transmitted the content, not on a service provider hosting or delivering the content. If providers are required to proactively monitor the forum for undesired content, that burden would likely reduce the ability of providers (especially smaller ones) from hosting many-to-many communications. Providers should be protected from liability if they choose to remove or block a user who violates terms of service or the norms of the group.

5 Search

This section covers a fifth group of functions that include the primary methods used by people to locate content on the Internet. Search functions are used both because people want to access new information or content, and because they want to revisit previously viewed content.

Many search tools and techniques display a portion of the content for resource being suggested in response to a search query.[12] Therefore, the search function not only includes locating content, but display of user-generated content. Search functions are essential to enable users to discover and access content on the Internet.

5.1 Searching the Web

Description of function: responding to search requests with the means to connect the searcher to the content and, often, displaying a portion of the content. Search is most commonly performed by "search engines," which are third-party services allowing users to search for relevant resources on the World Wide Web by providing keywords, a question, or uploading or linking to an image.

Technical and practical considerations: Providing this search function typically involves (a) indexing content on the Internet using algorithms that evaluate and record information such as keyword relevance, content type, freshness of content, user engagement and page quality, and (b) identifying, providing an access link, and displaying suggested results (often with "snippets" of the content) in response to a user search query using algorithms that evaluate factors such as user location, user language, previous search history, and device type.

12 Although some search tools now provide AI-generated summaries of content in response to search queries. For a discussion of these issues, see Policy Framework Section 5.9, Spotlight: Artificial Intelligence.

Recommended policy approaches	Reasons for this approach
Providers of search services should not be liable for Internet content created by others that are displayed to users in response to search queries.	If search engines were liable for user-generated content, they would likely stop indexing most of the content on the Web. This would have the practical result of leaving huge swaths of the Internet effectively unavailable to users around the world.
Providers of search services should not be responsible for addressing problematic content displayed in search results.	Search is a vital intermediary function that enables Internet communication because it facilitates user access to *content created by others* by helping them find and locate "relevant" content on the Internet. Without search, users would need to know in advance the URL or IP address of every website or other online resource they want to access, which is impossible at Internet scale.

5.2 Embedded Search

Description of function: providing embedded site-specific search results as a service to websites and others that do not have the technical resources or financial means to develop their own site-specific search tools.

Technical and practical considerations: By outsourcing an on-site search function to a third-party search engine, a website can provide users with a direct search on its site. This function is often, but not exclusively, offered by search engines that themselves provide web-focused searches (as discussed above). The search results can be tailored to the needs of the specific website that uses the embedded search.

Recommended policy approaches	Reasons for this approach
Providers of embedded search services should not be liable for Internet content that is managed by the underlying website that is using the service for an embedded search capability.	If embedded search providers were liable for the content displayed in search results, they would likely stop offering that service, especially to smaller websites and less established businesses or organizations, which would directly impact the Internet user experience because sites would lack good search functions.
Providers of embedded search services should not be responsible for addressing problematic content displayed in embedded search results.	If embedded search engine providers were required to monitor content on the site, the service would likely become too costly for smaller websites and less established businesses or organizations. This would directly hamper the ability of small websites to compete with larger sites.

5.3 Specific Search

Description of function: providing search results focused on specific media or topics (such as, for example, reverse audio services or search tools for podcasts or images) from sites operated by someone other than the search provider. This function increases the ability of users to locate content of interest on the Internet, especially content that is not easily searchable using a general search engine.

Technical and practical considerations: General search tools are often too broad, and thus, a range of more focused search tools have arisen to allow Internet users to search particular types of content more effectively and efficiently. The search results can be tailored to the types of media or content.

Recommended policy approaches	Reasons for this approach
Providers of embedded search services should not be liable for Internet content that is managed by the underlying website that is using the service for an embedded search capability.	If embedded search providers were liable for the content displayed in search results, they would likely stop offering that service, especially to smaller websites and less established businesses or organizations, which would directly impact the Internet user experience because sites would lack good search functions.
Providers of embedded search services should not be responsible for addressing problematic content displayed in embedded search results.	If embedded search engine providers were required to monitor content on the site, the service would likely become too costly for smaller websites and less established businesses or organizations. This would directly hamper the ability of small websites to compete with larger sites.

5.4 Site-Provided Search

Description of function: providing within-site content search. Some major online services (especially those that host extensive user-generated content, such as social media services) offer their own internal search tools, tailored to their service, to allow users to discover content on their sites.

Technical and practical considerations: Providing tools for users to locate content is a basic function of sites that support user-generated content. Search results can be tailored to the particular types of content supported by the site and/or the individual user.

Recommended policy approaches	Reasons for this approach
Site operators that provide their own search tools to locate content on the site should not face liability for content created by others because they offer a within-site search tool to allow discovery of that content.	If these sites were not permitted to provide search tools on their sites, users would be deprived of efficient local tools to locate content.

6 Cybersecurity Protection, Privacy Protection, and User Content Controls

This section covers a sixth group of functions that:

- (a) seek to combat cyberattacks on the Internet, which are essential for a secure, robust, reliable, and efficient Internet,
- (b) allow individual users to take steps to protect the security and privacy of their own Internet communications and
- (c) allow users to exert control over the categories of content that they can receive.

Note: Some intermediary liability protection laws explicitly extend their protections to software and services that allow users to control the content they receive over the Internet. For example, providers of family-oriented user-controlled filtering software can be protected from lawsuits brought by sites that are blocked by the software. *See, e.g.,* US Statutory Code, 47 U.S.C. §§ 230(f)(2) & (4).

6.1 Network-Scale Traffic Protection

Description of function: protecting networks, online services, websites, and other Internet resources from a broad range of malicious traffic, including distributed denial of service (DDoS) attacks and other cybersecurity threats. This function is part of an overall collaborative cybersecurity effort[13] to secure communications over the Internet.

Technical and practical considerations: Network-scale protections involve the use of different and constantly evolving techniques (such as signature databases, anomaly detection, and artificial intelligence) and dedicated infrastructures to defend against cyberattacks and mitigate

13 Internet Society, "Collaborative Security: An approach to tackling Internet Security issues," April. 2015, available at https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf.

the impact of malicious traffic on the availability, accessibility, or reliability of networks, online services, websites, and other Internet resources. Some of these techniques require that communications must pass through a network operated by a cybersecurity provider before reaching the intended network. Thus, at times, cybersecurity service providers' networks carry "user-generated content" and other types of content "created by others" on the Internet.

6.2 User-Controlled Content Filters and Tools

Description of function: providing the user with tools to block or limit certain types of content from being delivered to their devices. A variety of types of tools are available. For example, user-controlled content filtering tools can be used to reduce spam email from being delivered, block malicious code from being delivered by a website, or seek to prevent unwanted web content such as pornography from being viewed by a household or user device.

Technical and practical considerations: User-controlled filters and tools offer important protections (such as from spam and malware on web pages) and family-protection options (such as from pornography or other content). These tools use various technical methods and are not always fully effective (but nevertheless can be very useful). They are sometimes provided as an additional service by an Internet Service Provider, but also commonly as software to be installed on users' computers and devices. The U.S. intermediary liability protection law, Section 230, recognizing the value of such tools to allow users to decide what content to block, specifically includes protections for entities providing these tools. See, e.g., US Statutory Code, 47 U.S.C. §§ 230(f)(2) & (4).

Recommended policy approaches	Reasons for this approach
Providers of user-controlled filters and tools should not be liable for the content that passes through their tools, and should not be liable because they block particular content.	Without liability protections, providers would likely be unable to operate, thereby depriving Internet users of important cybersecurity and spam protections, and content filtering tools.

Recommended policy approaches	Reasons for this approach
Providers of user-controlled filters and tools should not be responsible for addressing problematic content sent or received by their users.	The purpose of these filters and tools is to empower *users* to decide what content they want to access, and what content they would prefer to block. A mandate to providers to also *block* problematic content before it reaches users would both complicate the tool (and might not even be possible). Such a mandate would undermine users' autonomy to control the content they receive, and give them concerns that their Internet communications are being monitored. As a result, they are likely to avoid using such tools to protect their online interactions, leading to lower overall cybersecurity on the Internet.

6.3 User-Focused Traffic Protection

Description of function: enabling individual users to protect their Internet traffic from cyberattacks, surveillance (by private entities and governments), and censorship.

Technical and practical considerations: User-focused traffic protections are those that can be applied at the discretion of the user to direct their Internet traffic over trusted network paths and protocols. These protections can also help users obfuscate their identity or location and thereby enhance their privacy and security. These traffic protection services utilize various technical methods, including virtual private networks (VPNs), onion routing services (most commonly the Tor network), and other approaches. In most cases, the providers of such services do not—and often cannot—determine what content is flowing across their networks.

Recommended policy approaches	Reasons for this approach
Providers of user-focused traffic protection should not be liable for the content that passes through their networks.	Without liability protections, providers would likely be unable to operate, thereby depriving Internet users of an important cybersecurity tool protecting them from cyberattacks, identify-theft, surveillance, and censorship.
Providers of user-focused traffic protection should not be responsible for addressing problematic content sent or received by their users.	Inspecting and potentially blocking particular traffic would be directly contrary to the intent of the user-focused traffic protection service providers. This would undermine the effectiveness of these services, reducing privacy and increasing security risks for the users.

7 Applications, Software, and their Development and Distribution

The seventh group of intermediary functions includes the most common computer applications, programs, and software libraries that are used in sending, receiving, and displaying Internet communications. This section also discusses the intermediary functions of application and software distribution. The applications and software discussed in this section may also include capabilities that are unrelated to Internet communications.

Because of software's overarching role in facilitating, displaying, protecting, and filtering content on the Internet, some intermediary liability protection laws specifically include, within their protection, creators, and distributors of the software that is used in Internet communications. See, e.g., US Statutory Code, 47 U.S.C. §§ 230(f)(2) & (4).

The functions in this section (such as the development of web and email software) are closely linked to functions discussed in Sections 3 and 4 above (including for example web hosting and one-to-one communications). This section, however, focuses on the development and distribution of the underlying software used to offer the services addressed above, which can warrant intermediary protections independent from the provision of services.

7.1 Operating System Software

Description of function: providing device software that allows (1) the device to connect to the Internet and send or receive communications over the Internet, (2) users of the device to input content for transmittal to the Internet, and (3) users of the device to receive and view content transmitted over the Internet. These functions are among the many other activities and functions that an operating system performs on a device.

Technical and practical considerations: A device's operating system performs essential functions that allow the transmission, receipt, and display of communications to and from the Internet. Essentially all computing devices have an underlying operating system, from consumer devices like computers, mobile phones and TVs to the routers, switches, servers and other devices that are essential to the operation of the Internet.

Recommended policy approaches	Reasons for this approach
Entities which provide operating systems should not be liable for the Internet content that is transmitted, received, or displayed through the operating system.	Operating systems are essential for communications on the Internet, and for the Internet itself. Imposing liability for Internet content created or transmitted by users or others on providers of operating systems would greatly limit if not eliminate the ability of users to communicate over the Internet.
Operating systems should not be mandated to block or otherwise interfere with problematic content on the Internet.	The security, stability, reliability, and integrity of operating systems are critical to Internet access and all computing more broadly. Mandates that operating systems monitor or block access to content would undermine the speed, security, and reliability of the functions of operating systems.

7.2 Web Browsing and Serving Software

Description of function: providing software for requesting, sending, receiving, and displaying content using World Wide Web protocols. These actions are performed by two broad types of software: web "server" software (which receives and responds to requests from web clients for online content) and "client" software, most commonly web browsers, which allows users to request, receive, and view a broad array of web content. This intermediary function also includes "apps"—software running

on smartphones, computers, and other devices—that retrieve content using World Wide Web protocols. A vast amount of Internet content is delivered to users through the functions of web servers and web client software, which is a critical method for users to access content online.

Technical and practical considerations: The Web relies on the interoperability afforded by World Wide Web protocols, most commonly the Hypertext Markup Language, or HTML, for formatting content, and Hypertext Transfer Protocol Secure, or HTTPS, a protocol for securely requesting and delivering content. This interoperability provides one of the foundational benefits of the Internet—the ability of anyone to create, format, and link content that people elsewhere in the world can access. Many websites embed content from multiple sources (e.g., an embedded video from a streaming service or a photo from a photo-sharing service that appears in the middle of the web page). Web browsers are a common tool to access Internet content, and browsers offer the user a rich set of options to control the content presented to them and, to some extent, to protect their own privacy and security.

Recommended policy approaches	Reasons for this approach
Entities which provide web client and server software, should not be liable for the content that is transmitted, received, or displayed through the software.	Web browsing and web serving software programs are critical for enabling individuals to access content on the Internet. Without protections from liability, entities providing these vital intermediary functions would be concerned about being liable for the content handled by their software. They may restrict the use of their tools to limit liability, such as by limiting use to web resources that they have inspected or who have agreed to indemnify them in the event of any legal action. Modern websites and web resources typically contain dynamic content that can change frequently and without notice. This makes it practically impossible for anyone to assess whether the content users wish to send or receive could attract liability. The risk of liability would likely greatly restrict the content that is available on the Web and hinder individuals' ability to communicate online.
Web browsing software should not be mandated to block or otherwise interfere with problematic content on the Internet.	Mandates that web server or client software monitor or block access to content would likely undermine the speed, security, trust, and reliability of the Internet. For example, if browsers screen or block content in ways that are uncontrollable and unmanageable by the user, users will use alternative tools to modify or replace their browser (which could expose users to malware and identity theft).

Recommended policy approaches	Reasons for this approach
Web browsing software should not be mandated to reduce security to allow third-parties to examine and block problematic content on the Internet.	Policies have been proposed that require browsers to reduce overall security to allow third-parties to examine and block traffic that would otherwise be encrypted between web browser and web server. For example, a requirement to install government-controlled root certificates[14] would enable this type of blocking, but would also undermine security, trust, and reliability of the Internet.

7.3 Email Software

Description of function: providing software for sending, receiving, storing, and displaying emails. These actions are performed by two broad types of software: email server software and email client software. Server software performs the "back-end" functions of transmitting, receiving, and storing emails, while client software allows users to send, receive, forward, and view emails. Email is a widely used communications mechanism, based usually on an asynchronous, federated, store-and-forward model, with independent mail servers or systems transmitting and receiving email on behalf of senders and receivers.

Technical and practical considerations: The interoperability of mail servers and clients using globally accepted email protocols means that senders and receivers can exchange email regardless of what email software or service providers they use. Encryption technologies such as S/MIME and PGP are available to secure email on an end-to-end basis for users who choose to encrypt their email.

14 Internet Society, "Mauritius Must Not Fall into the 'Mass Surveillance' Trap," 28 May 2021, available at https://www.internetsociety.org/blog/2021/05/mauritius-must-not-fall-into-the-mass-surveillance-trap/.

Recommended policy approaches	Reasons for this approach
Entities which provide email client and server software should not be liable for the content that is transmitted, received, or displayed through the software.	Email client and server software is a critical tool for communication on the Internet. Without protections from liability, software developers are likely to stop providing email to large classes of users, limiting the ability of users to communicate by email over the Internet..
Email software should not be mandated to block or otherwise interfere with problematic content on the Internet.	Mandates that email software monitor or block access to content would undermine the security, privacy, and reliability of email. It would also discourage email providers from offering their customers the ability to secure their email communications with end-to-end encryption.

7.4 Messaging Software

Description of function: providing software for a broad range of tools to send, receive, store, and display messages. These actions are performed by two broad types of software: messaging "server" software (which performs "back-end" functions of routing messages and may also receive, transmit, and store messages) and "client" software (which allows users to send, receive, and view messages, and may also store them). Like email, messaging is a widely used communication mechanism.

Technical and practical considerations: There is a wide range of messaging systems, and many of them are not interoperable with each other (and the internal architecture of the various systems may be very different). Some messaging systems are based on broadly developed Internet standards, while others have developed both the client and the server software to support messaging. Some messaging systems support end-to-end encrypted messaging, which can provide critical protections to keep messages private and secure.

Recommended policy approaches	Reasons for this approach
Entities which provide messaging software, including client and server software, should not be liable for the content that is transmitted, received, or displayed through the software.	Messaging software is a critical communications tool on the Internet, especially for secure and private end-to-end communication. Without these protections, software providers would be concerned that they may be liable for the content their users share. As a result, they may stop providing the function or feel compelled to weaken the security and privacy of their users' communications by disabling end-to-end encryption or scanning their users' communications.
Messaging software should not be mandated to block or otherwise interfere with problematic content on the Internet.	Mandates that messaging software monitor or block access to content would undermine the speed, security, privacy, trust and reliability of messaging.

7.5 Other Software Used in Sending, Receiving, and Displaying of Internet Communications

Description of function: providing an application or program with a secondary function that offers the ability to send, receive, and display content and communications. For example, an app that provides information about hiking trails in a geographic area may also permit users to post comments about the trails that are delivered to other users.

Technical and practical considerations: There is a vast diversity of programs and apps that allow users to post or send content and receive content from others.

Recommended policy approaches	Reasons for this approach
Entities which provide applications that enable users to post, transmit, or receive content or communications should not be liable for the user-generated content that is transmitted, received, or displayed through the application.	Because a vast number of applications allow users to transmit content and communications, broadly phrased regulations could easily sweep in hundreds or even thousands of applications, many from start-ups and small providers. Without protections from liability for user-generated content, developers and providers of such applications would be unlikely to offer the added communications functionality as part of their service, undermining the ability of individuals to communicate via those apps and limiting innovation and new products on the Internet. It could also drive some providers, especially smaller ones, out of the market.
Applications should not be mandated to block or otherwise interfere with problematic user-generated content on the Internet.	Mandates that entities that provide communications functions as part of their program and application software monitor or block access to user-generated content would likely limit legitimate communications, and undermine the security, privacy, trust and reliability of the Internet.

7.6 Software/Application Development and Distribution

Description of function: developing and facilitating the distribution of software and applications that support the communication of content over the Internet. This function includes, for example, applications, software, software libraries, and software plug-ins that transmit, receive, display, forward, cache, search, subset, organize, reorganize, translate, filter, screen, allow, disallow, pick, choose, analyze, digest content, or

otherwise facilitate the communication of content over the Internet. This category of software and applications—and their distribution—may be provided for end-users, Internet infrastructure providers, or other participants in the Internet ecosystem. Because few people today have the technical knowledge to create their own Internet client and server applications, the ability to locate and retrieve software written by others is an essential function for the operation of the Internet.

Technical and practical considerations: The development and distribution of software tools that enable users to access the Internet and communicate over it are vital functions. The development and distribution function takes a wide range of forms, including open-source software repositories (that provide some of the most foundational software on which the Internet operates), collaborative software development workspaces (often used to develop open-source software), "app stores" available to users, "stores" in browsers and other software to allow users to add third-party add-ins (for example, to support the filtering of web traffic; updating and patching of installed software), and other approaches.

Recommended policy approaches	Reasons for this approach
Providers of software development and distribution services should not be liable for the content that users send and receive using the software developed or distributed.	Without these protections from liability, providers would likely be unable to provide these functions due to concerns about potential liability for content handled by the software that is developed or distributed. Liability would threaten the ability of the Internet to continue to operate, and would be particularly harmful to open-source software developers.[15]

15 Internet Society, "The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem," 24 October 2022, available at https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/.

Recommended policy approaches	Reasons for this approach
Developers and providers of software should not be mandated to block or otherwise interfere with problematic user-generated content on the Internet.	Such mandates would adversely affect global connectivity and individuals' access to the tools to communicate content online. Contributions to open-source software would likely decline and critical software would not be maintained, leading to much less secure and trustworthy Internet.

8 Complex Environments

This final section discusses sites and services that could be viewed as providing a single distinct function (such as a "social media" function) or providing a combination of the functions discussed in the sections above to create a more enriched environment for user interaction. Ultimately, the policy analysis is very similar—the entities are handling content created by other people, and thus, imposing liability on the entities raises significant concerns not only for this category of functions but also for other critical Internet intermediary functions.

8.1 Social Media

Description of function: providing a social networking environment that enables users to connect with other users, as well as create, share, exchange, receive, and interact with content created by others. Section 5.1 of the Policy Framework[16] discusses social media in more detail.

Technical and practical considerations: Social media sites facilitate communication, networking, and content discovery among users, often through a combination of text, images, videos, and links. Additional functions performed by social media sites include user account management, content hosting and delivery, algorithms for content recommendation and personalization, and tools for user interaction such as "likes," comments, and shares. The function of providing a social networking environment can be applied to a very broad range of sites—not just the large and well-known social media services. For example, many sites offer users an opportunity to engage with each other, exchange content and ideas, and develop direct relationships with other users. The "social media" functions could easily apply to small and niche-audience social media services and also to sites that focus on specific communities of interest—such as marathon runners, gardeners, fans of a particular sports team, or members of a political party or club.

16 Policy Framework Section 5.1, Spotlight: Policy Considerations for "Social Media" Platforms that Host, Curate, and Moderate User-Generated Content.

Recommended policy approaches	Reasons for this approach
Providers of social media services should not be liable for the content created, posted, sent, or received by their users.	If entities providing social media services could be liable for user-generated content (see section 1.5 of the Policy Framework[17] for a discussion of user-generated content), they may significantly reduce the opportunities for individuals to engage in online discourse, and may over-censor speech—including lawful speech—of their users. Without liability protections, providers may severely restrict who can place content online, thereby significantly limiting the ability of individuals to communicate content on the Internet.
Providers of social media services should not be responsible for problematic content created, posted, sent, or received by their users.	Responsibility for problematic content should be placed on the person or entity that posted the content, not on a service provider hosting the content. Placing responsibility on providers would undermine the ability of those providers to carry significant amounts of user-generated content.
Where policy concerns center on actions of the service provider (and not the content of users' postings), any policy response should not burden user speech.	As noted in Policy Framework Section 5.1, there is a broad range of laws and policies that can be applied to social media service providers *without* making them liable for the content created or communicated by their users.

17 Policy Framework Section 1.5, Comparing Liability for Site-Generated Content and User-Generated Content.

8.2 Federated Networks

Description of function: providing a decentralized approach to user-generated content hosting, sharing, curating, and moderation, including, for example, social networking environments. Multiple independently operated servers can choose to participate in a federated network, allowing users to interact across the federated network while each server maintains control over its own data and communities. For example, in contrast with a centrally controlled social media community, a federated social media system can enable many smaller independent communities to connect and share content throughout the federated ecosystem. This can create a similar social networking experience but with a more local approach to moderation. Section 5.2 of the Policy Framework[18] discusses federated networks in more detail.

Technical and practical considerations: Federated social networks of independently operated servers using standardized protocols such as ActivityPub have become more popular. In this type of network, each independent server sets its own rules and policies over, for example, moderation, data privacy, and other topics, while still participating in a broader network. The Internet's global email system is another example of a federated network because vast numbers of independently run mail servers exchange email with each other without prior arrangement. The email system allows each separate participating entity to set its only policies over, for example, spam management and message storage limits. Federated service providers—many of which are small companies or organizations—allow users to maintain broad connections across the Internet while still being able to select a service provider that offers privacy, moderation, and other policies that meet their preferences.

18 Policy Framework Section 5.2, Spotlight: Policy Considerations for "Federated Networks" Enable New Approaches to Facilitate User-Engagement.

Recommended policy approaches	Reasons for this approach
Providers of federated content services should not be liable for the content created, posted, sent, or received by their users.	If these providers could be liable for user-generated content, they may be unable—technically or financially—to continue to offer those services. Federated networks by their nature attract small companies and even individuals as service providers. If these entities are unable to operate, Internet users would lose valuable tools that provide alternative options to large social media companies and more granular content moderation.
Providers of federated content services should not be responsible for problematic content created, posted, sent, or received by their users.	Responsibility for problematic content should be placed on the person or entity that posted the content, not on a provider hosting the content. Placing responsibility on the federated provider would undermine the positive potential of federated networks and greatly restrict their availability.

8.3 Gaming Environments

Description of function: facilitating multiple players to connect and play video games together in real-time over the Internet, including facilitating a range of methods for players to interact and exchange communications and content with each other. Section 5.3 of the Policy Framework[19] discusses gaming environments in more detail.

Technical and practical considerations: Most, if not all, modern gaming environments are at least partially connected through the Internet, and some are fully Internet-based. Common communication components of gaming environments include in-game chat and direct person-to-person voice and video connections. Gaming ecosystems are not merely spaces

19 Policy Framework Section 5.3, Spotlight: Policy Considerations for the Online Interactive Gaming Ecosystem.

for users to participate in online games with other users around the world—they also provide a social media environment.

Recommended policy approaches	Reasons for this approach
Providers of gaming environments should not be liable for the content created, posted, sent, or received by their users.	If providers could be liable for the content of their customers' communications, they may significantly reduce the opportunities for individuals to engage with each other and may over-censor the speech—including lawful speech—that their users seek to communicate. Without liability protections, may severely restrict who can participate and what content can be posted, thereby significantly altering and limiting gaming ecosystems.
Providers of gaming environments should not be responsible for problematic content created, posted, sent, or received by their users.	Responsibility for problematic content should be placed on the person or entity that posted the content, not on a service provider hosting the content. Placing responsibility on a gaming provider would likely alter the dynamics of the games and undermine the viability of gaming systems.

8.4 Virtual and Augmented Reality Environments

Description of function: enabling multiple users to interact and collaborate in a shared virtual reality (VR) or augmented reality (AR) environment. Section 5.4 of the Policy Framework[20] discusses VR and AR environments in more detail.

20 Policy Framework Section 5.4, Spotlight: Policy Considerations for Internet-Connected Virtual Reality and Augmented Reality Systems.

Technical and practical considerations: Although virtual or augmented reality environments have emerged more recently as gaming systems, AR and VR systems are—like gaming systems—increasingly integrating with the Internet. Many VR and AR environments directly connect to the Internet and allow users to interact with each other in real-time. VR and AR environments may, in some cases, create direct impacts on the physical world and on people not intentionally participating in a virtual or augmented reality environment.

Recommended policy approaches	Reasons for this approach
Providers of virtual or augmented reality environments services should not be liable for the content created, posted, sent, or received by their users.	If VR and AR providers could be liable for the content of their user's communications, the service providers may significantly reduce the opportunities for individuals to engage in online discourse or may over-censor the speech—including lawful speech—that their users seek to communicate. Without liability protections, providers may severely restrict who can place content online and what content they can place, thereby significantly altering and limiting the ongoing development of VR and AR technologies and services.
Providers of virtual or augmented reality environments should not be responsible for problematic content created, posted, sent, or received by their users.	Responsibility for problematic content should be placed on the person or entity that posted the content, not on a service provider hosting the content. Placing responsibility on providers would likely negatively impact the developing virtual and augmented reality technologies.