A Policy Framework for Internet Intermediaries

September 2024

Executive Summary

This paper provides a framework to understand Internet intermediary functions and to develop policy concerning responsibility for online content, without harming the Internet and the ability of individuals 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. 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 how critical protections from liability are for 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 and the EU's E-Commerce Directive and Digital Services Act. We explain why they 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 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, "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 conclude this paper with several "Spotlights:" policy considerations for specific online sectors including social media, federated networks, on-line gaming, augmented reality/virtual reality, advertising, as well as pay-for-content business models, and managing protected speech.

Table of Contents

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 e-mail services are all examples of entities providing intermediary functions. Our goal here 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, tax incentives, rebates, certification schemes, procurement requirements, and even decisions **not** to legislate or regulate.

Policy challenges concerning intermediaries

A broad range of intermediary functions are essential for the operation of the Internet. Consequently, policies 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

[1] Under the intermediary liability protection regimes applicable to the internet, the focus is on intermediary functions that are involved in 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.

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 white 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 are not arguing that entities performing intermediary functions "cannot" or "should not" be subject to policy in some manner. Our goal is to explain 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.

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 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.

ISOC'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)

The Internet has clearly created economic opportunity and benefits for nations and organizations around the world.[2]

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: 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 needs in their communities. Governments can interact with their citizens far more robustly, quickly, and at less cost. Communications facilitated by the Internet enhance global knowledge and economic opportunity.

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 responsibility for such content. **User-generated content** may be an original work 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

[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)

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. And some may be harmful, defamatory, deceptive, threatening, or even illegal.

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. 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.

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 to 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 of these entities are effectively 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 it all. The postal services controls how mail is delivered from the point it is received; on the Internet there is no entity who controls how content is delivered or who is responsible for each step in the process. The open interoperable Internet technical protocols are what enable communications to flow without a central controller.

Nonetheless, in both cases, postal service and its agents, as well as the various intermediaries involved in an Internet communication, are communicating user-generated content.

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 the ability to its members 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.

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." For other entities, their 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 is typically only providing 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 which 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* with regard to 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 in liability.
- For the independent web hosting company that operates the servers and infrastructure used by the car manufacturer, the function is pure intermediary: *all* of 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 web sites 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, community networks—to connect to the Internet. Once connected to the Internet, *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 to not negatively affect the operation of the Internet.

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.

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. Thus, for a phone call sixty years ago 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 be used to carry 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 maintenance and extension of the network.

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 Years Eve. And 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.

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 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, common 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 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. 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, e-mail services, domain services, identity services, and security providers—that provide critical services that support and facilitate communications across the Internet. There is no centralized control or coordination of the networks or supporting entities.[5]

---

[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://en.wikipedia.org/wiki/Packet_switching

[5] An ISOC white 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 white 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/

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, and 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 of distributed operation and decentralized design are critical for the continued health and growth of the Internet.

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 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

[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.

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 —especially some that are closer to user content—are commercial, some Internet intermediary functions are provided by non-profit or volunteer communities. Entities may be located 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 Internet 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 the Internet (sometimes loosely termed "infrastructure intermediaries") generally are not aware 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]

Graphic of various intermediaries involved in a fairly simple Internet communication

[insert box to illustrate multiple intermediaries involved in sending traffic, providing an example (*e.g.*, the intermediaries involved in a user viewing the website of the Internet Society). NOTE: this example could be in a pop-out box, with a visual illustration of the intermediaries involved – we should consider working to make a pop out box work well in printed form, but possibly work much more robustly in an online version]

Liability Protections for intermediary functions

This section discusses liability protections, beginning with a brief history of the origins and key elements of the US Section 230. We also describe 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.

[7] Infrastructure intermediaries not only don't care about the specific content that is 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 that they are transmitting opaque and unknown.

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.

The initial development of intermediary protection laws: Setting the Context

The early Internet was developed in the 1970s based on funding provided by the U.S. 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 U.S. Government formally transferred the network to the private sector, which began to bring ordinary people onto the Internet.

As more and more individuals were able to speak publicly on the Internet, there quickly arose questions of 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 be legally liable for the words that those people had posted. In the 1990s, two seminal U.S. 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*.[9]

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

[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.

[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.

Internet would have lost 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.

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, in 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.
- 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 completed 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.

A new approach to liability was needed.

It is against this backdrop that the U.S. Congress considered and enacted the "Internet Freedom and Family Empowerment Act", which became 47 U.S.C. 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." 47 U.S.C. § 230(b)(1)[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.

[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] https://www.congress.gov/104/statute/STATUTE-110/STATUTE-110-Pg56.pdf

The U.S. 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." *Id.* § 230(a)(3). 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.

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 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.[14] At the same time, the U.S. 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.

Intermediary protections in Europe

In 2000, the **European Union** adopted the Electronic Commerce Directive (2000/31/EC),[15] or "E-Commerce Directive" to address intermediary protections. As a practical matter the E-Commerce Direct 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).
- And most importantly, the EU directive requires that intermediaries that obtain knowledge of content alleged to be illegal take steps to remove the content reasonably promptly.[16]

[14] 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.

[15] See https://eur-lex.europa.eu/eli/dir/2000/31/oj as well as Wikipedia analysis at https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000 and [[/jms insert other references here if appropriate.//jms]]

[16] 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 U.S. Constitution generally (outside of the copyright context) prohibits legal mandates to remove content without a specific judicial determination that the content is illegal.

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.

In 2022 the European Union (EU), 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 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)[17] 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.

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":[18]

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; and
3. a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service.

[17] See https://eur-lex.europa.eu/eli/reg/2022/2065/oj as well as 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.]

[18] Ibid., Article 3, "Definitions" of Digital Services Act

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), including:

- a point of contact for EU authorities and users;
- user-friendly terms and conditions;
- transparency regarding advertising, recommender systems and content moderations 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; and
- an obligation to provide a recommender system option not based on user profiling.[19]

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 offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such offence or contravention.[20]

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.[21]

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

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

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

[21] 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

member of a representative body and bound by the representative body's code of conduct recognized by the Minister.[22]

In **Brazil**'s "Internet Bill of Rights," Section III of Chapter III of *the Marco Civil da Internet* provides liability protections for Internet service providers such as ISPs and other infrastructure providers for third-party content. It also provides Internet application providers with protection from liability for third party content on the condition that they comply with court orders to make the specified content unavailable.[23]

Australia is actively moving forward in 2024 to adopt an intermediary liability protection regime focused on legal claims for defamation.[24] 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 services and for search engine providers.[25] 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 particular 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, a number of multilateral or multistakeholder organizations have issued statements of support for intermediary liability protections. These international agreements and statements reflect a growing consensus of the value of such protections.

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

[23] 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/

[24] 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)

[25] 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

Multilateral and multistakeholder principles 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[26] issued a joint declaration calling for protections of "mere conduit" intermediaries, and for other intermediary functions, expressing the view that they should 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,[27] 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."[28]
2014	The Organisation for Economic Co-operation and Development (OECD) released broad guidance on limiting intermediary liability:[29] **12. 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 and responsibilities of internet intermediaries (CM/Rec(2018)2)[30], applying a human rights-based approach to States and Internet intermediaries' responsibilities, leaving aside questions of liability.

[26] https://www.osce.org/representative-on-freedom-of-media/78309

[27] https://africaninternetrights.org/en

[28] https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf

[29] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387

[30] https://rm.coe.int/1680790e14

Recent intermediary liability trends

Protections for intermediaries are viewed as having been instrumental for 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 giving protection to intermediaries may lead to court-crafted protections or more problematic treatment of intermediary functions.

In this section, we identify five 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;
- over-blocking of lawful content; and
- 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 white 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 take down" approach, which requires an intermediary to remove content on receipt of a legally authorized notice, which in some jurisdictions may be an administrative order or a notice from a private entity.

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".

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[31].

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.

Content Moderation: In other countries, including a number in the MENA region including the Kingdom of Saudia Arabia, the policy approach to intermediaries that host user-generated content is to require intermediaries to actively monitor and remove illegal content posted by users, with penalties such as fines and imprisonment for non-compliance. This could be referred to as a "mandatory content moderation" approach is often coupled with giving government authorities the power to directly order that content be blocked by ISPs. However, Jordan, for instance, provides intermediaries with protection for liability provided that take down any illegal content when notified.

Age-Specific Requirements: In some countries, there is also a push 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.

As an 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 provide information on users that make prohibited uploads and respond to "take down notices".[32]

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.

Removal of Intermediary Liability Protections: Reactions to early experience with Internet-specific policies have inspired some sweeping proposals. For example, in the United States,

---

[31] 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.

[32] 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

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. Such proposals to amend or repeal Section 230 (and similar laws in other countries), 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. This would affect the ability of individuals to share opinions and other speech on the Internet.

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.

Policymaking principles for Internet intermediary functions

This section includes three set of principles the Internet Society believes will be useful to policymakers looking at the Internet. The Annex to this document complements these sets of principles by providing short descriptions of widely used intermediary functions, technical and practical considerations, and some policymaking guidance.

The three sets of principles include:

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.

Overarching principles for prudent policymaking concerning the Internet

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

A. **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 which seems narrowly tailored, to understand whether there could be any adverse effect 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.[33]

B. **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 web sites. 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.

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

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:

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

E. **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

[33] *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/.

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 web sites, while entities providing intermediary functions such as web hosting, search engines, and caching should not be liable.

F. **Protect intermediary functions that host and display user-generated content:** Entities providing intermediary functions to host user-generated content ~~s~~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.

G. **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 to not 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. At the same time, 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.

Specific general 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 protections from liability for handling that content. But this does *not* mean that entities that provide these functions cannot be regulated. There are a broad range of policies, regulations and laws that already apply, or can apply, to entities that provide

intermediary functions. Many of these policy principles could help address some of the policy concerns that have arisen about intermediary functions on the Internet:

H. **Privacy and security**: Privacy and security are critical values in the Internet ecosystem, and strong rules to protect privacy and enhance security of Internet communications should be adopted. Entities providing Internet intermediary functions should strive to incorporate "security-by-design" and "privacy-by-design", adopting industry best practices and innovating to enhance the privacy and security features of those functions.

I. **Non-discrimination**: The exercise of Internet intermediary functions must not discriminate against individual users or groups of users based on protected classes and characteristics. Individuals have a right to be to be treated equally, regardless of categories such as race, color, sex, nationality, language, religion or ethnic, national or social origin.[34] Rules should prevent illegal discrimination in the provision of Internet services, including intermediary functions.

J. **Accessibility:** The Internet should be available to all, and guidelines promoting robust accessibility can helpfully guide the design and implementation of intermediary functions to enable individuals with different accessibility needs for online communication.[35] Online content and controls should interact predictably and successfully with assistive technology.

K. **Human rights and values:** The Internet enables users to exercise their human rights online. Internet intermediary functions play a vital role in facilitating freedom of expression, freedom of association, and freedom to access information online. Any government interference with the operation of intermediary functions risks preventing or hindering individuals from exercising their rights. Therefore, policymakers should consider the potential impact that any proposed policy concerning intermediary functions has on individuals' exercise of their human rights.

L. **Competition policy:** Although the Internet has historically been a tremendous place for small innovators and entrepreneurs to start and build businesses, it has certainly not been immune from concerns about concentration of power and anti-competitive activity. Policymakers considering competition concerns on the Internet should be careful to not diminish other intermediary protections discussed here.

M. **Choice and control:** Providing users with the ability to control the content they consume enables users to filter out irrelevant and unwanted content and sources. Limited choice of services can put users at greater risk of unfair or discriminatory

[34] 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.

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

practices. Policymakers should strive to enhance user choice and control over what services they use and what content they choose to view.

N. **Transparency:** Access to information about terms of service governing intermediary functions that host, curate and moderate user-generated content empowers users to make informed choices about the services they use. Policies should encourage meaningful transparency about how content will be hosted, curated and moderated. For example, entities should be transparent about, among other things, their use of generative algorithms and the collection, sale and use of personal data. At the same time, mandated disclosure of algorithms and individualized explanations of moderation decisions can be very damaging to the ability of companies to operate, and these hyper-transparent types of policies should be avoided.

O. **Openness:** Access to the Internet, to 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.

P. **Innovation, interoperability and "switch-ability"**: The ability to add new or change intermediary functions at all "layers" of the Internet continues to enable a wide and growing range of diverse communication methods, styles and audiences. Policies should strive to encourage innovation in intermediary functions, remove barriers that prevent new entrants and avoid hindering interoperability. Users should not be "locked in" and unable to switch providers.

Q. **Risk assessment**: New intermediary functions or the application of known functions to new situations can have unintended consequences. 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.

R. **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.

Spotlights - Policy considerations for specific intermediary functions

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

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. Both need strong protections for the intermediary functions involved in hosting that 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 they have 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, for example, 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 the identified the risk that algorithms could be used to manipulate users' behavior with adverse effect, discriminate against them, or to 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 also are vital for increasing accessibility, converting voice into text captions for hard of hearing and deaf individuals.[36]

Our advice to policymakers is to remember that algorithms are not problematic *per se*. However, 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.

Spotlight: Policy considerations for "federated networks" enable new approaches to facilitate user-engagement.

"Federated networks" is a term that has garnered a growing amount of attention over the past few years. We turn a spotlight onto to 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

[36] For a more detailed discussion of the issues, please refer to the Internet Society's Amicus Curie brief in Reynaldo Gonzales et al. v Google LLC 598 U.S. 617 https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf

content throughout the federated ecosystem. This creates a similar social experience but with a more local approach to moderation.

"Federated" services are in the news recently because some federated services 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.[37] 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 Mastodon federated network can set and control their own content moderation rules.[38]

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 email 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.[39] 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.[40]

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

[37] https://www.w3.org/TR/activitypub/

[38] Mastodon rapidly gained in 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.

[39] 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

[40] 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/

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

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 am.[41] In 2019, China restricted minors to 90 minutes per weekday and banned them from playing online games between 10 pm and 8 am, imposing further restrictions in 2021.[42] 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 communications tools are audio and messaging capabilities, but there are many more subtle methods of communicating: choosing and modifying avatars, particular behaviors during play, 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.[43]

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. The interactive gaming platforms are performing intermediary functions, and major intermediary protection regimes apply equally to the gaming ecosystem.

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

[41] The law was subsequently abolished in 2021. See, https://en.wikipedia.org/wiki/Shutdown_law

[42] 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

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

boxes" in a game constitute deceptive practices or illegal gambling, consumer protection or illegal gambling laws should be directly applicable to such behaviors.

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.[44] 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.[45] Thus, like gaming, most major intermediary protection regimes could apply to VR and AR systems.

From a policy perspective, VR and AR systems do have considerable overlap 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 harms in the physical world, such as traffic accidents or personal injuries.[46]
- AR systems may be able to pull people who are not online, and who haven't given consent, into the augmented environment

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/AR.

[44] 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.

[45] 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, and body orientation, proximity, and posture.

[46] See, for example, the Pokèmon Go Death Tracker at https://pokemongodeathtracker.com/

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.

We are aware that the value the advertising industry brings to the Internet is subject to differing opinions. Some proponents say that the advertising system should be protected, 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 a 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 tracks user across devices and even in the real world. This means that users can be monitored, assessed according to their value to advertisers, influenced (or manipulated by bad practices), and discriminated against based on their location, spot demand for product, and estimated purchasing power.

Beyond debates about the existing advertising system, the ad system unquestionably relies on intermediary liability protections in some contexts.[47] 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-contributed 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

[47] The inner workings of the 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.

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 significant 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 expands those transparency requirements, and also prohibits certain design techniques that seek to manipulate or deceive users.

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 the placement of content 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?
- 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?[48]
- 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?

[48] 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?

- 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?[49]
- 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.[50] The questions we raise above help show the complexities, advantages, and disadvantages that come from focusing on economic compensation. We do not include this to offer policymakers specific advice, but to raise some of the challenges highlighted in this "Spotlight."

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 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. The First Amendment of the United States Constitution,[51] for example, provides very strong limitations on governmental regulation of speech, while 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.[52]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 challenge under the First Amendment if implemented in the United States.[53]

[49] 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?

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

[51] https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say

[53] "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

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.

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 communications medium for modern societies. Building policy approaches that provide liability protection to for many different types of intermediary functions that enable Internet communication remains a necessity for a healthy Internet. At the same time, there 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

Meritless Copyright Claims Threaten Online Political Speech," Sep. 2010, available at https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf.

Internet work, but also those that most directly interact with users' communications, such as hosting and display of content. Without these protections, the Internet cannot continue to be a medium for communications.

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 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. 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.