2

The United States' Approach to "Platform" Regulation

Eric Goldman[*]

2.1 INTRODUCTION

This chapter summarizes the United States' legal framework governing internet "platforms" that publish third-party content. It highlights three key features of US law: the constitutional protections for free speech and press, the statutory immunity provided by 47 U.S.C. § 230 ("Section 230"), and the limits on state regulation of the internet. It also discusses US efforts to impose mandatory transparency obligations on internet "platforms."

2.2 WHAT IS A "PLATFORM"?

The term "platform" has emerged as a standard descriptor for internet services and has been incorporated into US legislation. Nevertheless, this term is problematic.

First, the term "platform" often refers to internet services that facilitate user-to-user communications – with Facebook viewed as the archetypical platform and the primary target for regulatory intervention. Yet user-to-user online communications take place in a wide range of services, including consumer review services, wikis, message boards, private messaging services (such as email services and private chat tools), online marketplaces, online dating services, livestreaming video services, video hosting services, "social media," and much more. There is no consensus about which services constitute platforms. Sometimes platforms refer to all of these services and others;[1] sometimes the term narrowly describes only "social media"

[*] This chapter addresses developments through December 1, 2022.

[1] For example, a proposed bill in Minnesota defined "social media platforms" as any "electronic medium … that allows users to create, share, and view user-generated content, " UNLAWFUL SOCIAL MEDIA ACTIVITIES (May 4, 2022) 325F.6945, https://www.house.leg.state.mn.us/cco/journals/202122/J050402.htm?fbclid=IwAR00geZn77rqZ2VX7NiuaX8iOnY8U-sWwV2zToKe7dN2E6ODpZoaNqepfE0#12992.

(another term without a precise definition); and sometimes it is used in other ways. Furthermore, numerous synonyms to the platform term are used in legislation and common parlance. The lack of standardized terminology creates scope problems for a chapter like this.

Second, the term "platform" can obscure or trivialize a service's editorial and publication functions. The nomenclature implies that the entities do not qualify for stringent constitutional protections applicable to "publishers." For example, platforms are sometimes analogized to common carriers or utilities because those entities get diminished constitutional protections. Alternatively, sometimes platforms are analogized to "public squares" or other government-provided functions that must comply with the constitution – a different way of curtailing services' editorial discretion, but no less censorial in intent. Because the term "platform" subverts internet services' editorial, curatorial, and publishing functions, it has significant political valence and consequences.

To sidestep the semantic and substantive problems created by the "platform" term, this chapter instead uses the term "internet services"[2] to cover all online services that publish third-party content.

2.3 CONSTITUTIONAL PROTECTION FOR FREE SPEECH

The First Amendment of the United States Constitution says, "Congress shall make no law . . . abridging the freedom of speech, or of the press."[3] This provision provides strong and wide-ranging protections against government censorship of speech.

2.3.1 *Content Protected by the First Amendment*

The First Amendment generally requires heightened scrutiny of speech restrictions, though the level of scrutiny varies. For example, government restrictions based on the speaker's viewpoint generally get the most demanding level of scrutiny (called "strict" scrutiny); government restrictions on commercial speech get a less rigorous, but still meaningful, level of scrutiny (called "intermediate" scrutiny). Government regulations rarely survive strict scrutiny, and they usually survive the lowest level of scrutiny (called "rational basis" scrutiny). The outcomes are less predictable when intermediate scrutiny applies.

Some types of content are characterized as receiving no First Amendment protection at all, including child sexual abuse material (CSAM), obscenity, incitements to violence, and defamation. However, each of those exclusions is defined

[2] Sometimes these services are called "user-generated content services" or "UGC services." The term "internet service provider" typically refers only to internet access providers.

[3] Elsewhere, the Constitution makes clear that these obligations apply to all government actors, not just Congress.

narrowly. For example, incitements to violence may be punished only when the speech is likely to lead to imminent unlawful violence.

As a result, many categories of speech that are regulated internationally may be constitutionally protected in the United States and thus subject to little or no government restriction. Some examples are as follows:

- "Hate speech": Unless the speech fits into one of the content categories that do not get First Amendment protection, it is not constitutionally permitted to restrict odious views about other people. As just one example, the First Amendment protects distribution of Nazi images and paraphernalia and public support for the Nazi party and its ideals (including declarations of Nazi affiliation).
- "Cyberbullying": Cyberbullying activities are often protected by the First Amendment, including typical online bullying behavior like name-calling, dehumanizing references, brigading, doxing, and uncivil behavior. Cyberbullying behavior becomes actionable only in extreme cases, such as when it constitutes criminal stalking, criminal harassment, or imminent threats of violence.
- "Terroristic" content: In general, the First Amendment protects content published by or about terrorist organizations that does not fit into one of its exclusions.
- "Pornography": With limited exceptions, the First Amendment protects nonobscene and non-CSAM depictions of sexual activity, no matter how "hardcore."
- "Misinformation": The First Amendment protects many categories of "false" information.[4] False political statements are routinely permitted unless they are defamatory, and the First Amendment imposes heightened standards for defamation claims in those circumstances.[5] The First Amendment also protects health misinformation provided by nonexperts, such as scientifically unsupported statements against vaccines or downplaying concerns about the COVID pandemic.

The First Amendment limits speech restrictions in any government-operated online speech venue. In other words, government-operated social media accounts may be unable to moderate constituents' comments that contain hate speech, misinformation, or pornography without violating the First Amendment.[6]

[4] For example, false public claims of military honors are protected. United States v. Alvarez, 567 U.S. 709 (2012).

[5] Usually, plaintiffs must show that the defendant made the statement with "actual malice" of the falsity, a very difficult standard for plaintiffs to satisfy. *See* New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

[6] Knight First Amendment Inst. v. Trump, 928 F.3d 226 (2d Cir. 2019), *vacated as moot*, Biden v. Knight First Amendment Inst., 141 S.Ct. 1220 (2021).

In practice, this means the government largely cannot manage users' antisocial behavior in any online speech venue it operates.

2.3.2 *Protection for Internet Services as "Publishers"*

The First Amendment protects the freedoms of speech and press, though the "press" freedom rarely gets invoked. For disseminators of third-party content, their editorial decisions are usually treated as their "speech" and are subject to the highest level of First Amendment protection. As a concurring justice explained in *Miami Herald v. Tornillo*, the "government may not force a newspaper to print copy which, in its journalistic discretion, it chooses to leave on the newsroom floor."[7]

Nevertheless, because of their unique structural dynamics, several types of communication providers get reduced First Amendment protection, including telephony/telegraphy providers and broadcasters. These diminished First Amendment principles do not extend to internet services, however. In 1997, the Supreme Court said that its prior telephony and broadcasting rulings "provide no basis for qualifying the level of First Amendment scrutiny that should be applied to the Internet."[8]

Instead, when internet services perform editorial or curatorial functions, the First Amendment protects those functions to the same degree it would protect offline content publishers. As one court explained, "Like a newspaper or a news network, Twitter makes decisions about what content to include, exclude, moderate, filter, label, restrict, or promote, and those decisions are protected by the First Amendment."[9]

The First Amendment should negate all attempts to impose strict liability for disseminating third-party content.[10] However, it permits the imposition of liability based on higher levels of scienter, such as intent, knowledge, and recklessness, and perhaps a "should have known"/negligence standard as well. As a practical matter, Section 230 (discussed momentarily) typically moots the need for courts to explore the interplay between the First Amendment and internet service scienter. Thus, it is not clear what level of internet service scienter regarding third-party tortious or criminal content is required to impose online publisher liability under the First Amendment.

2.4 STATUTORY PROTECTION FOR FREE SPEECH (SECTION 230)

2.4.1 *Overview*

In 1996, Congress enacted 47 U.S.C. § 230 as part of the Communications Decency Act, which says the following:

[7] Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241 (1974) (concurrence of Justice White).
[8] Reno v. ACLU, 521 U.S. 844 (1997).
[9] O'Handley v. Padilla, 2022 WL 93625 (N.D. Cal. Jan. 10, 2022).
[10] Smith v. Cal., 361 U.S. 147 (1959).

(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.
(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 (1).

Translating these provisions into simpler language:[11]

- Section 230(c)(1) says that websites and other online services are not liable for third-party content.
- Section 230(c)(2)(A) says that websites and other online services are not liable for the content filtering decisions they make, even if they are partially responsible for the content.
- Section 230(c)(2)(B) says that vendors of anti-threat software filters, such as anti-spam, anti-spyware, anti-virus, and parental choice vendors, are not liable for their blocking decisions.

These provisions are subject to statutory exceptions discussed below.

Defendants need Section 230(c)(1)'s immunity only when the law would otherwise impose liability. This immunization is not a technical loophole or a "get-out-of-jail-free" card. It is a critical policy choice that Congress made to get the benefits provided by internet services that otherwise would be foreclosed by liability concerns.

Section 230(c)(1) is a globally unique policy. No other country has adopted a legal rule like it. The United States has entered into trade agreements with Mexico and Canada,[12] as well as Japan,[13] that nominally require those countries to adopt Section 230–like protection, but those countries have not taken steps to honor those commitments.[14]

[11] For a more comprehensive description of Section 230, *see* Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, The Oxford Handbook of Online Intermediary Liability 155 (Giancarlo Frosio, ed. 2020).
[12] United States-Mexico-Canada Agreement (USMCA) Article 19.17.
[13] Agreement Between the United States of America and Japan Concerning Digital Trade (US-Japan Digital Trade Agreement) Article 18.
[14] US-Japan Digital Trade Agreement: Side Letter on Interactive Computer Services, October 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Letter_Exchange_on_Interactive_Computer_Services.pdf (saying that "Japan need not change its existing legal system").

2.4.2 *Elements of a Section 230(c)(1) Defense*

A defendant qualifies for a Section 230(c)(1) defense[15] when it satisfies the following three elements:

1. *Interactive Computer Service Provider/User*. The definition of "interactive computer service" includes internet access providers (IAP). By definition, anyone online necessarily uses an IAP to connect to the internet, so Section 230(c)(1) protects all services, and users of those services, from liability for third-party content. Sometimes Section 230(c)(1) is mistakenly characterized as a "gift" or privilege to "Big Tech," but it equally benefits "Small Tech" and individual internet users.
2. *Publisher or Speaker Claims*. Section 230(c)(1) says that defendants "shall not be treated as the publisher or speaker" of third-party content, but this phrase is not limited to causes of action that expressly reference "publisher" or "speaker" in the claim elements. Instead, this phrase applies to any cause of action where the imposition of liability would treat the defendant as the publisher or speaker of third-party content.

However, Congress has enumerated four statutory exceptions to Section 230:

- Federal criminal prosecutions: If the US government brings a criminal prosecution of federal law, Section 230 does not apply.[16] However, Section 230(c)(1) does apply to civil claims based on federal crimes[17] and to state criminal prosecutions (with the exception of FOSTA discussed below), when based on third-party content. To reinforce the point: with respect to third-party content, internet services only need to comply with the single national standard of federal criminal law, not the cacophony of state criminal laws with diverse standards.
- Intellectual property claims: Federal intellectual property claims (except for claims under the Defend Trade Secrets Act) are excluded from Section 230(c)(1). For example, federal copyright claims are not covered by Section 230(c)(1), though Congress has enacted a separate safe harbor, 17 U.S.C. §512 (the DMCA Online Safe Harbor), for claims over third-party copyright infringement. State IP claims are also excluded from

[15] This part will focus on Section 230(c)(1). *See A Review of Section 230's Meaning & Application Based on More Than 500 Cases*, Internet Assoc., July 27, 2020, https://archiveia.org/publications/a-review-of-section-230s-meaning-application-based-on-more-than-500-cases/ (discussing the relative infrequency of Section 230(c)(2) litigation).

[16] Sometimes critics of Section 230, including judges, claim that Section 230 creates a lawless zone for third-party content. This is plainly erroneous because federal criminal law always governs internet services (plus, content originators are always liable for their own content).

[17] Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016); Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021).

Section 230 in most of the country, but the Ninth Circuit Court of Appeals (covering the western United States) has applied Section 230(c)(1) to state IP claims (such as trade secrets, publicity rights, and state trademark claims) based on third-party content.[18]

- The Electronic Communications Privacy Act (ECPA) and state law equivalents. This exception is largely irrelevant in practice.
- FOSTA. In 2018, Congress enacted FOSTA, a complex bill that targeted online promotions of sex trafficking victims and commercial sex more generally.[19] Among other consequences, FOSTA amended Section 230(c)(1) to exclude state criminal prosecutions related to the promotion of sex trafficking and commercial sex, as well as private claims related to the promotion of sex trafficking.

3. *Information Provided by Another Information Content Provider*. Conceptually, this provision says Section 230(c)(1) only applies to third-party content, not first-party content. Thus, content originators remain liable for their content, but no one else online is liable alongside them. Of course, works are often prepared jointly or collaboratively, and internet services could potentially contribute to the development of users' content. However, courts applying Section 230(c)(1) typically reject plaintiffs' arguments to characterize user content as first-party content based on standard editing practices by services, such as reformatting content or engaging in content moderation.

To get around this first/third-party distinction, plaintiffs can claim that they are enforcing the services' contract or marketing promises made by the service. However, perhaps surprisingly, some courts have used Section 230(c)(1) to reject private lawsuits alleging services breached their public promises when courts think those lawsuits seek to hold the services liable for third-party content.[20]

In addition to Section 230(c)(1)'s statutory exclusions, courts have developed common-law exceptions for the following claims: promissory estoppel,[21] civil conspiracy,[22] failure to warn,[23] and defective software design (so long as the defect does not result in the publication of third-party content).[24] Additional common-law exceptions may apply when defendants allegedly moderated content with anti-competitive animus,[25] consummates an online marketplace

[18] Perfect 10, Inc. v. Ccbill LLC, 488 F.3d 1102 (9th Cir. 2007).
[19] For a fuller explanation of FOSTA, *see* Eric Goldman, *The Complicated Story of FOSTA and Section 230*, 17 First Amendment L. Rev. 279 (2019).
[20] *See, e.g.*, Murphy v. Twitter, Inc., 60 Cal. App. 5th 12 (Cal. App. Ct. 2021).
[21] Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).
[22] Tanisha Systems, Inc. v. Chandra, 2015 WL 10550967 (N.D. Ga. 2015).
[23] Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016).
[24] Lemmon v. Snap, Inc., 995 F.3d 1085 (9th Cir. 2021).
[25] Enigma Software Group USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040 (9th Cir. 2019).

transaction,[26] or encourages illegal content or designs its service to require users to input illegal content.[27]

2.4.3 *Implications of Section 230*

Some things that are not relevant to a Section 230(c)(1) defense:

First, Section 230(c)(1) has no prerequisites or formalities to qualify for the defense. A provider or user of an interactive computer service automatically gets Section 230(c)(1)'s immunity from liability for third-party content. In contrast, the DMCA Online Safe Harbor requires internet services to undertake numerous preparatory steps before they can qualify for the safe harbor – and any skipped step automatically disqualifies the service from the safe harbor's coverage.

Second, defendant scienter is irrelevant to a Section 230(c)(1) defense. An internet service may "know" about problematic third-party content or actions and still benefit from Section 230(c)(1)'s immunity. Thus, "takedown notices" or other legal demands for content removal do not affect an internet service's eligibility for Section 230(c)(1).[28] If the service otherwise qualifies for Section 230(c)(1), the service can ignore the takedown notice with no legal consequence. (In contrast, failure to remove allegedly infringing content in response to a takedown notice disqualifies the service from claiming the DMCA Online Safe Harbor).

Due to the irrelevance of scienter to Section 230(c)(1), the jurisprudence lacks the normal kinds of inquiries into the defendants' conduct or state of mind that one typically finds in US tort law cases. It does not matter to Section 230(c)(1) if plaintiffs allege that the service's employees reviewed the material at issue, or that the service had demonstrable evidence that it knew it had other instances of harmful content, or that the service had previously removed the same or similar content.

Third, Section 230(c)(1) does not depend on the internet service's lack of financial interest in the third-party content. Section 230(c)(1) applies to third-party content that the service pays to obtain.[29] Section 230(c)(1) also applies when the internet service shares revenue with the content supplier and when the internet service is paid to disseminate third-party

[26] HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676 (9th Cir. 2019).
[27] Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).
[28] *E.g.*, Marshall's Locksmith Service Inc. v. Google LLC, 925 F.3d 1263 (D.C. Cir. 2019) ("it is 'well established that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech'").
[29] *E.g.*, Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

content, such as advertisements,[30] in either case even though the internet service derives financial benefit from the illegal content.

Fourth, Section 230(c)(1)'s immunity applies regardless of how vigorously the service moderates content. It protects services that do zero content moderation at all (an unsustainable model given the exceptions to Section 230), services that have humans fully pre-screen all third-party content and select only some of that content for publication, and every option or configuration between those two extremes. As a result, internet services do not have an obligation to pre-screen third-party content either manually or using automated filters, though they are free to deploy such techniques without risking their eligibility for Section 230(c)(1) immunity.

Fifth, if a US court has jurisdiction over the matter and is applying US law, Section 230 will apply to foreign plaintiffs[31] and claims over foreign activities, such as a Canadian deindexing court order[32] and foreign terrorist attacks.[33]

2.4.4 *The Interplay Between Section 230(c)(1) and the First Amendment*

Internet services can always assert a First Amendment defense, but Section 230 supplements the First Amendment defense in important ways. If Section 230 and the First Amendment would both lead to the same substantive outcomes with respect to the publication of third-party content online,[34] Section 230(c)(1) acts like a "procedural fast lane" to resolve litigation more quickly and cheaply than would be possible

[30] *E.g.*, Ramey v. Darkside Productions, Inc., 2004 WL 5550485 (D.D.C. 2004); Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009); Calise v. Meta Platforms, Inc., 2022 WL 1240860 (N.D. Cal. 2022).

[31] *E.g.*, Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019); Igbonwa v. Facebook, Inc., 786 F. App'x 104 (9th Cir. 2019). For more on this topic, see Anupam Chander, *Section 230 and the International Law of Facebook*, 24 YALE J.L. & TECH. 393 (2022) ("in all of the cases that I have been able to discover involving foreign parties or events, with one exception, defendants successfully invoked Section 230, except in cases where the courts did not reach that issue because the defendant won on other grounds"). Prof. Chander says he "could not locate cases where Section 230 was asserted by a foreign defendant." *Id.*

[32] Google LLC v. Equustek Solutions Inc., 2017 WL 11573727 (N.D. Cal. 2017).

[33] Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019); Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021) ("because § 230(c)(1) focuses on limiting liability, the relevant conduct occurs where immunity is imposed, which is where Congress intended the limitation of liability to have an effect, rather than the place where the claims principally arose. As such, the conduct relevant to § 230's focus is entirely within the United States – i.e., at the situs of this litigation"). Also, the SPEECH Act prevents the enforcement of defamation-related foreign court orders by US courts if the order would violate Section 230. 28 U.S.C. §§4101–4104.

[34] This is not the case. For example, the First Amendment provides less protection to commercial speech than non-commercial speech, but Section 230 treats both equally and thus provides greater protection for commercial speech than the First Amendment requires.

with a constitutional defense.[35] Among other reasons, Section 230(c)(1) empowers courts to dismiss claims at the earliest litigation stages (e.g., a motion to dismiss) when courts may be otherwise reluctant to make constitutional determinations, saving the internet services from incurring high litigation costs and getting dragged into discovery. These procedural benefits have substantive effects by encouraging internet services to moderate content without fearing the price tag of each decision.

When "lawful-but-awful" content is protected by the First Amendment, internet services never can be liable for that content – with or without Section 230(c)(1)'s immunity. In those circumstances, many regulatory and public complaints about the content's availability online are more appropriately directed to the First Amendment, not Section 230. In other words, Section 230(c)(1) revisions will not create any new legal incentives for the services to redress lawful-but-awful content. Instead, Section 230's immunity provides extra-legal comfort to internet services to do the socially valuable work of cleaning up harmful speech – work that the First Amendment would not permit the government to do itself.

2.4.5 *Liability for Account Terminations and Content Removals*

Internet services usually have the unrestricted editorial discretion to terminate or suspend user accounts or remove or downgrade user content without incurring liability. Users have lost dozens of cases over these decisions, and no plaintiff has gotten a courtroom victory over terminations/removals.[36] Those defense wins are based on a variety of theories (depending on the plaintiff's precise claims), including:

- Private internet services aren't state actors or sufficiently linked to the government to be obligated to comply with constitutional requirements.
- Internet services typically defeat contract claims because their terms of service expressly reserve their right to terminate accounts and remove content as they see fit.
- Section 230 protects the services' decisions. In particular, courts often treat the plaintiffs' content as third-party content,[37] thus evaluating the case using Section 230(c)(1) rather than Section 230(c)(2)(A) (which would require the service to show good faith decision-making). Though Section 230 plays an important part in this jurisprudence, it has been in play in less than half of the termination/removal cases.[38]
- The plaintiffs cannot satisfy the prima facie elements of the claim.

[35] *See* Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 Notre Dame L. Rev. Reflection 34 (2019).
[36] Eric Goldman & Jess Miers, *Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules*, 1 J. Free Speech L. 191 (2021).
[37] *E.g.*, Federal Agency of News LLC v. Facebook, Inc., 432 F. Supp. 3d 1107 (N.D. Cal. 2020).
[38] Goldman & Miers, *supra* note 36.

2.4.6 *What Happens When Section 230 Does Not Apply to Claims over Third-Party Content?*

Section 230(c)(1) applies to an essentially infinite number of state law claims predicated on third-party content. However, when a case fits into Section 230's statutory and common law exclusions, what rules apply then?

Every plaintiff must establish the prima facie elements of their claim. Sometimes, those elements do not apply to internet services for third-party content. For example, there have been numerous lawsuits against social media services for allegedly providing illegal "material support to terrorists." Many of those lawsuits have failed because the applicable statute simply does not reach the provision of content publishing tools. (Those lawsuits have also failed on Section 230, First Amendment, and other grounds).

As another example, some plaintiffs overcome a Section 230 defense by alleging that the defendant service failed to warn them that other users could harm them. Nevertheless, those lawsuits cannot establish the prima facie elements of negligence.[39]

If a plaintiff establishes a prima facie case, the defendant can assert a First Amendment defense. As discussed above, the First Amendment should negate strict liability for third-party content, plus services can interpose any defenses available to the content originator (such as the First Amendment limits on defamation liability).

The IP exception to Section 230 includes federal copyright, federal trademark, and (in some parts of the country) state IP claims. First Amendment defenses are not usually tenable for federal copyright or trademark claims, though they apply to some state IP claims.

With respect to federal copyright claims based on third-party content, internet services routinely qualify for the DMCA Online Safe Harbor.[40] Upon receipt of a takedown notice, the service makes a choice: it can expeditiously remove the targeted item or waive the DMCA Online Safe Harbor and accept whatever default liability may apply. If a service does not qualify for the DMCA Online Safe Harbor, a successful plaintiff must show that either (a) the service knew of the infringing content and materially contributed to the infringement or (b) the service had the right and ability to control the infringing conduct and directly profited from it.

With respect to federal trademark claims, no federal statute parallels the DMCA Online Safe Harbor.[41] Nevertheless, the courts have generally followed the same legal principles: a service is not liable if it expeditiously stopped third-party trademark infringements after receiving takedown notices.[42]

[39] Beckman v. Match.com, LLC, 743 Fed. Appx. 142 (9th Cir. 2018); Doe No. 14 v. Internet Brands, Inc., 2016 U.S. Dist. LEXIS 192144 (C.D. Cal. 2016).

[40] 17 U.S.C. §512.

[41] 15 U.S.C. §1114(2)(A) provides a safe harbor for "innocent" printing of third-party materials, but this provision is rarely litigated because the "innocent" requirement is tautological.

[42] Tiffany Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).

With respect to state IP claims based on third-party content that are not preempted by Section 230, the laws are too diverse, and the cases are too infrequent, to summarize.

2.5 STATE REGULATION OF THE INTERNET (THE DORMANT COMMERCE CLAUSE)

The United States vests regulatory power both in the federal government and in subnational regulators, such as state legislatures. In practice, however, state legislatures have numerous limits on their authority over internet services, including the First Amendment, Section 230 (which expressly preempts most conflicting state laws regarding third-party content),[43] federal preemption, and constitutional limits on personal jurisdiction.

In addition, the US Constitution restricts the ability of states to regulate the internet through a doctrine called the "Dormant Commerce Clause." The Constitution gives Congress the authority to regulate interstate commerce, and by negative implication, that power is allocated exclusively to Congress and not to the state legislatures. State regulation of internet services often has Dormant Commerce Clause implications because of the services' global and national reach. Some reasons why a state law might violate the Dormant Commerce Clause:

- Two or more states enact conflicting laws that make it impossible for an internet service to simultaneously comply with each law.
- A state's law regulates activity wholly outside of the state, such as a law purporting to govern how a service outside the state facilitates an interaction between two residents of other states.
- A state's law erects barriers to an out-of-state service providing services in-state.

However, Dormant Commerce Clause challenges against state internet laws are infrequently advanced, and those challenges succeed only occasionally. More often, overreaching state internet laws are struck down on First Amendment grounds.

2.6 TRANSPARENCY AS REGULATION[44]

In addition to, or instead of, dictating content moderation decisions outright, legislatures are requiring internet services to provide greater "transparency" about their editorial practices and operations. These regulations can take many forms,

[43] 47 U.S.C. §230(e)(3). The non-preempted state laws are the ECPA-equivalents, state IP claims outside the Ninth Circuit, and FOSTA claims.

[44] For a fuller treatment of this subject, *see* Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, 73 HASTINGS L.J. 1203 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4005647.

including requiring internet services to publish their editorial policies, provide explanations to affected users about content moderation decisions, and publish aggregated statistics about their content moderation practices.

The constitutionality of mandatory editorial transparency requirements is actively being litigated, and the final resolution is uncertain. Much depends on how the courts frame the requirements. If the disclosure requirements are like standard compelled commercial disclosures, the requirements will get relatively relaxed constitutional scrutiny. If the requirements distort editorial decisions by publishers, then they are more likely to get stringent constitutional review.

Whether or not states create new transparency requirements for internet services, government enforcement agencies are demanding disclosures from Internet services by invoking consumer protection laws, such as state "UDAP" (unfair and deceptive acts or practices) laws and other restrictions on "false" advertising. These information demands are more likely to be upheld by a court than broad-based statutory disclosures, but not all of them would survive judicial scrutiny. For example, the government regulators sometimes choose their enforcement target on partisan grounds, which makes the investigation look like impermissible retaliation for constitutionally protected speech.

2.7 CONCLUSION

Online speech freedoms have become inextricably intertwined with partisan politics, which creates irreconcilable conflicts. Oversimplified, Democrats want internet services to remove more content, even if it is constitutionally protected; while Republicans want internet services to publish more content, even content that hurts society or the internet service's audience. Although both sides are unhappy with the current legal framework governing internet services and would favor censorial interventions, their solutions advance two radically different visions of the internet's future.

Given the partisan split on content moderation expectations, internet services are now routinely subject to partisan attacks on all sides. The services cannot satisfactorily navigate these attacks, because (as with any partisan topic) any accommodations to one team automatically anger the other team. As a result, the partisanship creates a dangerous ecosystem for terrible policy ideas, especially when one partisan party controls all of the applicable regulatory apparatus. This means the US legal framework described by this chapter could change dramatically – and almost certainly not for the better – imminently.