The Computer & Internet Lawyer

Volume 39 ▲ Number 9 ▲ October 2022

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Section 230 of the Communications Decency Act of 1996: An Overview and Recent Developments

By Scott Feira, Tom Fox, Axel Gutermuth, Nicholas O'Keefe, Oscar Ramallo, Peter Schildkraut and Isaac Chao

Section 230 of the Communications Decency Act of 1996 ("Section 230")[1] is touted by its supporters as the bedrock for freedom of online expression without which the meteoric growth of the internet would not have been possible. The statute's detractors view it as an enabler of disinformation that is undermining democracy, public health, and other aspects of society. The following provides a brief overview of Section 230, a brief comparison of the liability standards and regulatory oversight for online content, television and print, and a brief description of the regulatory approaches for online content in the European Union ("EU") and United Kingdom ("UK"). The following also provides some of the criticisms levelled at Section 230, and some of the recent reform initiatives.

The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at *scott.feira@arnoldporter.com, tom.fox@arnoldporter.com, axel.gutermuth@arnoldporter.com, nicholas.okeefe@arnoldporter.com, oscar.ramallo@arnoldporter.com, peter.schildkraut@arnoldporter.com* and *isaac.chao@arnoldporter.com*, respectively.

BACKGROUND ON SECTION 230

What Is Section 230?

Section 230 was enacted in order to provide legal certainty in the wake of two conflicting judicial decisions.

Cubby, Inc. v. CompuServe, Inc.[2] involved a defamation claim against CompuServe, a company that ran a subscription-based electronic information service, which included a journalism forum in which a third-party published a daily newsletter. Plaintiffs ran a competing online service, and brought a claim in the U.S. District Court for the Southern District of New York against CompuServe and others for alleged defamatory statements made in the newsletter. In ruling on a motion for summary judgment, the Southern District considered whether to apply: (1) the general "publisher" rule that one who repeats or republishes defamatory statements is subject to the same liability as the original publisher of the statements, or (2) the more difficult to satisfy (i.e., less onerous) liability standard applicable to "distributors" like bookstores and libraries, which requires proof that the distributor knew or had reason to know

of the defamatory statements. In granting CompuServe's motion, the court viewed CompuServe's service as a type of electronic library, and thus held CompuServe to the less onerous liability standard applicable to distributors.

Four years later, in 1995, the New York Supreme Court in *Stratton Oakmont, Inc. v. Prodigy Services Co*.[3] came out the other way, holding that Prodigy, which hosted electronic bulletin boards, should be treated as a "publisher" for purposes of defamatory statements a third-party made on one of the bulletin boards. The *Stratton Oakmont* court held that the differentiating factor from the *Cubby* case was the degree of control that Prodigy exercised over bulletin board content. The message to electronic information service providers that rely on third-party content was that engaging in content moderation is risky because it opens the door to you being found liable for defamatory statements in third-party content – with such exposure extending to all third-party content on your site, not just third-party content you have moderated.

Section 230 was enacted in 1996 in order to address concerns that the two decisions created a legal environment that favored leaving up illegal and objectionable content over removing it, and so disincentivized the development and utilization of content moderating technologies. Section 230 has two key provisions: Subsection (c)(1) and Subsection (c)(2).

Subsection (c)(1), which is sometimes referred to as the "publisher" safe harbor, can be thought of as providing online service providers with protection from claims for publishing content posted by third parties. It provides:

> 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.

An "interactive computer service" is "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." Social media companies are the quintessential interactive computer service, although the definition applies more broadly. An "information content provider" is, as the phrase suggests, "any person or entity that is responsible, in whole or in part, for the creation or development of information provided though the Internet or any other interactive computer."

Subsection (c)(2), which is sometimes referred to as a "Good Samaritan" safe harbor, can be thought of as providing online service providers with protection from their actions taken in good faith to block certain types of objectionable third-party content. It provides:

> 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).

Subsection (e) provides that Section 230 has no effect on certain laws, including federal criminal laws, intellectual property laws, communications privacy laws or sex trafficking laws.

How Have Courts Interpreted Section 230?

Section 230(c)(1) has been described as protecting from liability "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider."[4] Courts have held that it not only protects against claims premised on treatment as a publisher or speaker, but also those premised on treatment as a distributor.[5] Thus, an interactive computer service provider ("ICSP") would not be liable as a publisher or speaker of third-party content, even for third-party content that the ICSP knew or should have known was defamatory or otherwise unlawful.

On the other hand, Section 230(c)(1) does not apply with respect to claims invoking liability on other bases, such as promissory estoppel claims or FTC claims for unfair or deceptive acts or practices based on misrepresentations in published policies, or claims that are expressly excluded under Section 230(e), such as intellectual property or federal criminal law matters.

Courts have held that Section 230(c)(1) can protect users of an ICSP who repost content created by others. Liability protection can apply even if users or ICSPs make minor edits to the third-party content. But liability protection is lost if the users or ICSPs are deemed to be "responsible, in whole or in part, for the creation or development" of the content at issue, and thus are the "information content provider" as defined in Section 230(f)(3). An ICSP may provide neutral tools that are then used for illicit searches without being deemed an information content provider. However, if the ICSP

materially contributes to the creation or development of the content, it may be treated as an information content provider, resulting in loss of liability protection under Section 230(c)(1).[6]

Unlike Section 230(c)(1), Section 230(c)(2), which provides a liability shield for actions taken by an ICSP to restrict access to content, includes a good faith requirement. Accordingly, if an ICSP restricts access to content for reasons other than the content being obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable – e.g., censoring motivated by anticompetitive reasons – the protections of Section 230(c)(2) would not be available.

What Businesses Benefit From Section 230?

Section 230 benefits a wide range of businesses. It benefits not only the large social media companies, but also other companies that rely on user-generated online content, such as blogs, forums, distributors of newsletters, sites where users post reviews, classified ad sites, online auction sites, and sites that rely on user generated profiles, such as dating sites or apartment rental sites. Section 230 can also benefit others, such as adtech companies, and internet infrastructure companies, such as internet service providers. Proponents of Section 230 often defend it as being particularly useful for smaller companies, who do not have the financial means to engage in protracted litigation, because it both acts as a deterrent to litigation and enables them to get litigation dismissed at an earlier stage of the proceeding.

WHAT ARE SOME OF THE CRITICISMS OF SECTION 230?

Section 230 has been criticized as overly broad in various ways. Some critics charge that while Section 230 may have been appropriate when the internet was nascent, it now tips the field too far in ways that are harmful. Subsection (c)(1) has been criticized as providing ICSPs with overly broad immunity for published content, enabling them to profit from the spread of false and harmful information, or from content that involves violations of law. These criticisms invoke several aspects of Section 230, such as the judicial interpretation noted above that Subsection (c)(1) extends to distributor liability and not just publisher liability. Subsection (c)(1) is also faulted for not including a "good faith" requirement, similar to that in Subsection (c)(2), which would remove immunity if ICSPs knew or should have known of the harmful or illicit nature of the content. A "good faith" requirement for Subsection (c)(1) was proposed by the U.S. Department of Justice ("DOJ") in its proposed amendment to Section 230, as discussed below. Another fault attributed to Subsection (c)(1) is that while there is an exclusion for federal criminal law, there is no exclusion for state criminal law. Thus, ICSPs are not legally incentivized to prevent harm caused by activities such as revenge pornography, which is not a federal crime, even though it is a crime in most states.

Section 230 has also been criticized for bestowing on ICSPs a very powerful, and potentially politically harmful, role as censors of public speech. This criticism is particularly levelled at large social media companies. One aspect of this criticism is that content moderation, as interpreted by the courts, appears to fall within both Subsections (c)(1) and (c)(2) of Section 230, which creates a potentially overly broad and ill-defined swath of protection for ICSPs. Content moderation expressly falls within Subsection (c)(2), because a central purpose of Section 230 was to override the incentive not to remove harmful content that was created by the *Stratton Oakmont* decision. But courts have also interpreted Subsection (c)(1) in a way that permits traditional editorial functions without the ICSP being deemed to be a publisher.[7] For critics, this risks Subsection (c)(1), which does not contain a good faith requirement, swallowing Subsection (c)(2), which does. It also introduces the concept of traditional editorial functions, which is not only undefined, but not even included in the language of Section 230. This overlap between Subsections (c)(1) and (c)(2) was one of the main areas of criticism in the rulemaking petition of the National Telecommunications and Information Administration ("NTIA Petition") in July 2020, described below, and in the Executive Order of May 28, 2020 ("Executive Order") that preceded it. Another criticism in the NTIA Petition, and cited in some of the proposals to amend Section 230, is the inclusion of the words "or otherwise objectionable" in Subsection (c)(2). Critics maintain that this language needs to be either removed or narrowly defined to prevent it from being interpreted in a way that leaves ICSPs free to censor content for any reason.

HOW DOES THE LIABILITY STANDARD FOR DEFAMATION AND REGULATORY OVERSIGHT FOR ONLINE CONTENT COMPARE TO THAT FOR TRADITIONAL TV AND PRINT?

Common Law

Print publishers are subject to the common law standard for defamation, as modified by the First Amendment. Generally stated, the elements for a

defamation claim are (i) a false statement of purported fact about a defamed party; (ii) unprivileged publication to a third party; (iii) some level of fault, such as negligence, recklessness or intent; and (iv) harm to the defamed person's reputation. If the defamed person is a public figure, then the defaming statement must be made with "actual malice."[8] One who repeats or republishes defamatory statements is subject to the same liability as the original publisher. Distributors, such as bookstores and libraries, are only liable if they knew or had reason to know of the defamatory statements. Statements made on TV are subject to the same liability standards as applies to print. For online statements, there is a difference in liability standard between an ICSP publishing its own statements, and an ICSP publishing a third party's statement. In the former case, the liability standard is the same as for print and TV. But for publishers of third-party statements, Section 230 creates a different standard. Under Section 230, ICSPs are not treated as publishers or distributors of statements made by third parties, and so have effective immunity from defamation for third-party statements that they disseminate, as long as they do not modify the statements in a way that the statements become their own statements.[9]

The FTC

The Federal Trade Commission ("FTC") does not have general regulatory oversight over print publishers, TV or online communications. The FTC administers laws to which companies in those industries are subject, through its investigatory and enforcement powers in the areas of antitrust and consumer protection. The latter includes regulation of "unfair or deceptive acts or practices" ("UDAP") under Section 5(a) of the Federal Trade Commission Act, for which the FTC can seek civil remedies, such as cease and desist orders, corrective disclosures, obligations to notify harmed individuals, fines and civil penalties, and also bring criminal enforcement actions. Civil actions by the FTC under Section 5(a) are not among the excluded laws under Subsection (e) of Section 230, and so Section 230 could, in theory, shield companies from UDAP claims based on online communications. But the FTC has successfully argued in such actions that Section 230 immunity was unavailable either because the company, through its involvement in the challenged action, was itself the information content provider,[10] or because UDAP liability was premised not on the online content (for which Section 230 may have been available), but on the company's conduct (for which it was not).[11] Section 230 is also unavailable to online companies in UDAP actions brought for representations they make about their services, such as the nature of the tracking they employ, the ability of users to control the privacy of their personal information, and how the companies use algorithms.

As discussed below, the Executive Order and several bills pending in Congress have sought to expand the FTC's role with respect to some ICSPs, such as through treating violations of proposed rules relating to content moderation policies or the use of algorithms as UDAP violations and, for one bill, creating a role for the FTC in overseeing risk assessment and mitigation for large online platform companies and creating a bureau within the FTC to undertake studies and investigations of ICSPs.

The FCC

Broadcast TV and radio are subject to licensing by the Federal Communications Commission ("FCC"), and historically the FCC exerted considerable oversight over these industries. Most notably, the FCC's fairness doctrine required that broadcasters present controversial issues of public importance in a manner that fairly reflected differing viewpoints. Broadcasters also have been subject to restrictions on indecent programming. The FCC, however, abandoned the fairness doctrine in 1987, and indecency enforcement actions have slowed dramatically in the last 15 years, as concerns about chilling free speech have grown and the FCC's outlook has become increasingly deregulatory.

Unlike broadcast TV and radio, no FCC license is required to print something or make content available online. The FCC thus lacks a clear regulatory mandate over these activities, although the FCC on occasion has tried to exercise authority over them when an FCC licensee engages in them.[12]

The Executive Order and NTIA Petition, discussed below, arguably call for a turnabout for the FCC. The FCC would become more active in policing online content, and the FCC would become more involved in regulating an industry that is not subject to FCC licensing.

WHAT IS THE CORRESPONDING LEGAL APPROACH TAKEN IN THE EU AND THE UK?

The EU

Within the EU, there is no uniform set of rules governing criminal or civil liability of service providers for defamation or other types of unlawful content. Instead, liability is governed by Member State law. In part to address market inefficiencies caused by disparities among Member State laws, in 2000, the EU adopted Directive

2000/31/EC, commonly referred to as the e-Commerce Directive.[13] Articles 12-14 of the e-Commerce Directive introduce limited exemptions from liability of providers of information society services established in the EU. Liability continues to be governed by Member States' law, but Articles 12-14 restrict the ability of Member States to hold providers of information society services liable under specified conditions.

An "information society service" is defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service."[14] Information society services span a wide range of economic activities that take place on-line, including services giving rise to online contracting and, in so far as they represent an economic activity, services which are not remunerated by those who receive them, such as those offering online information or commercial communications, or those providing tools allowing for search, access and retrieval of data. Information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service.Video-on-demand or the provision of commercial communications by electronic mail also constitute information society services.[15]

Articles 12-14 of the e-Commerce Directive include safe harbors that provide for limited liability exemptions of service providers for third-party content. To benefit from these safe harbors, an information society service provider must be acting as a "mere conduit," "caching" or "hosting." The safe harbors cover all types of unlawful content (e.g., infringements of copyright or defamation), and both civil and criminal liability.

Mere conduit (Article 12): An information society service provider functions as a "mere conduit" if its service consists 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. The service provider is not liable for the information transmitted if it: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.[16]

Caching (Article 13): Where the service consists of the transmission in a communication network of information provided by a recipient of the service, the information society service provider is not liable for the automatic, intermediate and temporary storage of that information, for the sole purpose of making the transmission more efficient, if: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information, (c) the provider complies with industry accepted rules regarding the updating of the information, (d) the provider does not interfere with the lawful use of technology, consistent with industry standards, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon learning that the information at the initial source of transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[17]

Hosting (Article 14): Where the service consists of the storage of information provided by a recipient of the service, the information society service provider is not liable for the information stored at the request of a recipient of the service, if: (a) the provider does not have actual knowledge of unlawful activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the unlawful activity or information would be apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[18] Thus, Article 14 sets forth the functional equivalent of "notice and take down" procedures, but without the procedural and substantive details. The exemption in Article 14 is not available if the recipient of the service is acting under the authority or the control of the provider.[19]

Article 15 clarifies that Member States cannot impose on service providers a general obligation to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating unlawful activity. The exemptions therefore cannot be made conditional upon the service provider observing such general monitoring or supervision practices.

The safe harbors described above do not apply directly. As is generally the case with provisions of EU directives, Member States have to transpose them into national law. This has led to divergence between Member States in the transposition and application of the safe harbor rules. Moreover, after more than 20 years of application, the safe harbors have been subject to numerous judgments by EU and Member State courts. As a result, the wording of Articles 12-14 no longer fully reflects the current state of the law.

For these reasons, the liability exemption regime is being updated and removed from e-Commerce Directive Articles 12-15. A largely similar, but further refined liability regime will soon be introduced as part of the Digital Services Act,[20] which currently is expected to be formally adopted in September 2022.

If adopted, Chapter II of the Digital Services Act will include a more detailed liability exemption regime, which, however, continues to be based on the principles of the e-Commerce Directive and the approach of providing for conditional liability exemptions for the activities of "mere conduit," "caching" and "hosting." Different from the e-Commerce Directive, the Digital Services Act will be a regulation and, as such, directly applicable throughout the EU without the need for Member States to transpose the new safe harbors into national law.

The UK

Defamation is a specialist area of English law under which claimants can bring actions regarding published statements which defame a named or identifiable individual in a manner which causes them loss in their trade or profession, or damages their reputation, subject to a threshold of "serious harm." Secondary publishers of defamatory material that is communicated to a third party can also be held liable. Therefore, defamation claims present a significant risk to intermediaries, including online service providers such as internet service providers, content hosts, operators of online bulletin boards and forums, network operators, and intermediaries who merely cache information.

The Defamation Act 2013 reduced exposure for secondary publishers, including website operators, for defamation claims arising from third-party content. The 2013 Act introduced a statutory defense which applies where the website operator can show that it did not post the defamatory statement. Pursuant to regulations made under the Act (the Defamation (Operators of Websites) Regulations 2013) there are procedures requiring website operators to take certain actions in response to a complaint, including contacting the actual poster, providing the identity of the actual poster to the claimant, and potentially removing the defamatory post. These rules can therefore function as a "notice and take down" mechanism, with the website operator losing the benefit of the defense and risking liability if it fails to respond to a notice of complaint. This mechanism is consistent with a more broadly applicable, and still operative, defense under Section 1 of the Defamation Act 1996, pursuant to which a party may have a defense as an "intermediary" if it can show that it was not the author, editor or publisher of the allegedly defamatory statement; it took reasonable care in relation to its publication; and it did not know, and had no reason to believe, that its actions caused (or contributed to) the publication of a defamatory statement.

In addition, the UK implemented the E-Commerce Directive into its national law via the Electronic Commerce (EC Directive) Regulations 2002 SI 2002 No. 2013 (the "E-Commerce Regulations") prior to leaving the EU. As a result, the aspects of this legislation affecting the liability of information society service providers remain substantially the same: if such a party is acting as a "mere conduit," "cache" or "host," the party may be able to argue for protection under the E-Commerce Regulations.

While the E-Commerce Regulations derived from EU law remain part of UK law, any updates or revisions made to the EU's underlying E-Commerce Directive will not take effect in the UK, nor will any aspects of the EU's proposed Digital Services Act and Digital Markets Act. In the meantime, the UK Government is seeking to pass its own new legislation providing for additional internet regulation in the form of the Online Safety Bill. This is still in development but is intended to give the UK Office of Communications ("OFCOM") new powers to act as the online safety regulator. It will, among other things, impose new duties on providers of user-to-user and search services to assess their user base and the risks of harm to those users present on the service, and to take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) content and activity that is harmful to children. The draft legislation focuses on criminal liability and enforcement by OFCOM and makes no provision for civil liability. However, it introduces the concept of requiring the control of content that is legal, but "harmful" (i.e., typically prohibited under a website operator's terms of service), and imposes a number of duties of care. It seems possible that future civil actions may be based upon alleged breaches of some of these duties.

SECTION 230 REFORM INITIATIVES

Rulemaking Petition of the National Telecommunications and Information Administration

After President Trump issued an executive order[21] in May 2020 accusing social media platforms of politically motivated censorship, the National Telecommunications and Information Administration ("NTIA") petitioned the FCC to engage in rulemaking to "clarify" Section 230 in a manner that would narrow its protective scope in comparison to the prevailing interpretation in the courts.[22] The proposed clarifications include the following:

- Under prevailing law, a decision to restrict access to material is potentially protected under Section 230(c)(1) because deciding what content to publish has been considered part of the editorial discretion

that Section 230 was intended to protect. NTIA's proposal would limit protection for restricting access to material solely to the Good Samaritan (Subsection (c)(2)) safe harbor provision, which only protects "good faith" actions to restrict access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" content.

- NTIA's proposal would narrow the scope of the term "otherwise objectionable" in the Good Samaritan safe harbor to content that is similar in type to obscene, lewd, lascivious, filthy, excessively violent, or harassing content. This clarification serves to unify the interpretation of "otherwise objectionable," which has been read broadly by some courts to mean anything subjectively objectionable to the ICSP.

- NTIA's proposal would define "good faith" under the Good Samaritan safe harbor to require an action "consistent with publicly available terms of service or use that publicly state plainly and with particularity the criteria the interactive computer service employs in its content-moderation practice." Current law does not require ICSPs to create or follow any policies to benefit from the safe harbor.

- NTIA would strip Section 230(c)(1) immunity for ICSPs that modify or prioritize content in favor of a certain viewpoint. For example, if a social media platform's algorithm prioritized conservative viewpoints over liberal viewpoints, then the social media platform could be held liable for its users' content.

Finally, NTIA's proposal would impose a standalone requirement on any "mass-market retail offering to the public" to disclose its content moderation policies.

While the FCC took public comments on NTIA's petition, the FCC stopped moving forward on the proposal after the 2020 election.

DOJ Section 230 Amendment Proposal

In June 2020, the DOJ issued a set of reform proposals that it characterized as addressing the issues facing the modern internet that were not foreseen in 1996 when Section 230 was enacted.[23] Among its proposals, the DOJ would create a "Bad Samaritan" carve-out that would deny immunity from civil liability to platforms that purposefully facilitate or solicit third-party content that violates federal criminal law. The DOJ would also narrow the Good Samaritan safe harbor by replacing the catchall language allowing ICSPs to remove "otherwise objectionable" content and replacing it with the terms "unlawful" and "promotes terrorism."

Similar to NTIA's proposal to require content moderation policies, the DOJ would also require ICSPs to make content moderation decisions in accordance with published terms and conditions and accompanied with reasonable explanations for their decisions. Content moderation decisions not made in accordance with these requirements would not be considered in "good faith" for purposes of the Good Samaritan safe harbor.

Finally, the DOJ would add several categorical carve-outs to immunity for child exploitation and sexual abuse, terrorism, cyber-stalking, and federal antitrust claims.

Bills Pending in Congress

There have been dozens of bills introduced in Congress to modify or repeal Section 230. The bills generally take one or more of the following approaches:

- A small number seek to repeal Section 230, with one bill seeking to replace it with a narrower immunity scheme.

- Several bills create an expanded role for the FTC, with one bill seeking to create a role for the FTC in overseeing risk assessment and mitigation for large online platform companies, and seeking to create a Bureau of Digital Services Oversight and Safety within the FTC to undertake studies and investigations of ICSPs and perform other tasks as the FTC deems appropriate. Several pending bills seek to impose constraints on content moderation policies or the use of algorithms, and provide that violations of the applicable act are deemed to be UDAP violations enforceable by the FTC. Some bills require the FTC to engage in rulemaking.

- Some bills target specific types of content, such as illegal content, healthcare misinformation or content that causes or relates to other types of harm, and fall under either a new exception to Section 230 or an existing exception, such as the federal crime exception. Some bills provide for a cause of action for civil damages for harmed individuals. Some require that illegal content, or content that reveals illegality, be taken down or that an authority be notified of it.

- Several bills target content moderation generally, and include matters such as requiring disclosure of and compliance with a policy, prohibiting or providing for loss of Section 230 immunity in the event of selective enforcement of the policy, requiring the policy to be operated in good faith,

or requiring a system for handling content moderation complaints.

- Several bills target the use of algorithms, and provide for an exception to Section 230 for content promoted through the use of algorithms, or the use of algorithms in a discriminatory or harmful way.

- Some bills require large ICSPs to make information available to government bodies, academic researchers or other organizations.

- Some bills provide narrowly focused exceptions to Section 230, such as to remove immunity under Subsection (c)(1) for distributor liability, or to expand the list of exceptions to Section 230.

- Some of the bills only focus on ICSPs above a certain size, such as through the number of monthly users.

SELECT ISSUES

How Does Section 230 Impact Exposure for Content Moderation Decisions?

Section 230 gives service providers broad protection from liability for moderating content. "At its core, [Section] 230 bars lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content."[24] In *NetChoice, LLC v. Moody*, for example, a Florida statute imposed daily fines on social media platforms that deplatformed political candidates. The district court held the Florida statute was preempted by Section 230 and enjoined its enforcement.[25] Despite Section 230's broad protective scope, a service provider may lose its Section 230 immunity if it goes beyond content moderation to become responsible for what is objectionable about the content or if it unlawfully removes unobjectionable content (e.g., in violation of antitrust laws).

The influential *Roommates.com* decision illustrates the circumstances in which a court may consider a service provider responsible for unlawful content.[26] Roommates.com operated a website designed to match people renting out spare rooms with people looking for a place to live. Applicable law prohibited housing brokers from discriminating on the basis of sex, sexual orientation, and familial status. The website required users to include in their profiles their preferences with respect to the sex and sexual orientation of their roommates, as well as whether they preferred to live with children. The court ruled that by forcing users to violate anti-discrimination laws, the website was responsible for the unlawfulness of the content. On the other hand, the court held users, not the website, were responsible for content entered into a free-form "Additional Comments" box because the website did not force users to include any unlawful content in such responses.

Since the *Roommates* decision, courts have held service providers may be responsible for content authored by the service provider's employees,[27] paying users to post unlawfully acquired confidential information,[28] and specifically encouraging false sexual harassment allegations.[29] Courts have found service providers not responsible for selecting for publication defamatory user posts about an individual,[30] creating algorithms that allegedly bolstered the reach of terrorists groups on social media,[31] failing to remove dangerous and impersonating profiles from a "hook-up" app,[32] or summarizing multiple user ratings of a business into a single metric.[33]

Enigma Software illustrates the potential for liability stemming from an improper takedown or restriction of access.[34] Malwarebytes offered consumers software that automatically blocked them from downloading malicious programs. Malwarebytes and Enigma Software were direct competitors. After Enigma Software's most popular programs were flagged and blocked by Malwarebytes, Enigma Software sued for unfair competition, alleging its programs were legitimate and posed no threat to consumers. The court rejected Malwarebytes' argument that Section 230's Good Samaritan safe harbor permitted it to restrict access to any software Malwarebytes' subjectively considered "objectionable." While the court did not delineate the full scope of "objectionable" content subject to the safe harbor, the court held it did not include content taken down on the basis of anti-competitive motivations.

Does the Use of Algorithms Impact the Availability of Section 230 Immunity?

Section 230 predates widespread use of content-recommendation algorithms and does not expressly reference them. But commentators have noted that use of an algorithm could result in an ICSP being deemed to be a "developer" of content and thus an "information content provider" for which immunity is unavailable under Section 230.[35] While the decision in *Roommates.com* did not turn on the use of an algorithm, one was used on the content entered by subscribers that was at issue there. As the court explained, the algorithm "decodes the input, transforms it into a profile page and notifies other subscribers of a new applicant or individual offering housing matching their preferences." This use of an algorithm contributed to the

company being deemed to be the "developer" of the content at issue there, and thus to the loss of Section 230 immunity.

Algorithms can also create legal issues based on the use of the ICSP's algorithm on third-party content, as opposed to the status of the ICSP as a publisher or speaker. This could arise, for example, in advertising based on the use of discriminatory ad targeting and delivery algorithms.[36] The FTC has made clear that the use of algorithms to "deny people employment, housing, credit, insurance, or other benefits" can result in a violation of the Fair Credit Reporting Act, and the algorithmic automation of employment decisions based on "race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance" can result in a violation of the Equal Credit Opportunity Act. The U.S. Equal Employment Opportunity Commission ("EEOC") has announced an initiative to ensure that artificial intelligence and other algorithmic decision-making tools used in hiring and other employment decisions comply with federal civil rights laws.[37] The EEOC and the DOJ have each issued guidance[38] on how to use AI-based employment tools consistent with the Americans with Disabilities Act.[39]

The FTC has also made clear that misrepresentations about the use of algorithms or associated data can lead to a violation of Section 5 of the FTCA.[40] State and local jurisdictions have also started enacting laws regulating the use of algorithms. As indicated above, several bills introduced in Congress provide that algorithmic bias, or the algorithmic spread of certain types of information, can lead to the loss of Section 230 immunity.

Notes

1. 47 U.S.C. § 230.
2. 776 F. Supp. 135 (S.D.N.Y. 1991).
3. 23 Media L. Rep. (BNA) 1794, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished).
4. *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009) (footnote omitted).
5. *Zeran v. America Online, Inc.*, 129 F.3d 327, 332-34 (4th Cir. 1997).
6. For a good discussion of this issue, *see Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1162-72 (9th Cir. 2008). Different jurisdictions have applied standards different from the "material contribution" standard to determine when an ICSP becomes an information content provider.
7. *See Zeran*, 129 F.3d at 330.
8. *See New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
9. A print newspaper that also publishes online has been treated like an ICSP entitled to the protections of Section 230 with respect to third-party content on its website. *See Straw v. Streamwood Chamber of Commerce, Inc.*, 2015 IL App. (1st) 143094, ¶46.
10. *See FTC v. Accusearch Inc.*, 570 F.3d 1187, 1197-1201 (10th Cir. 2009).
11. *See FTC v. LeadClick Media, LLC*, 838 F.3d 158, 175-77 (2d Cir. 2016).
12. For example, in 2001, when AOL, an online content provider not subject to FCC licensing, sought to merge with Time Warner, which held FCC licenses related to its cable TV system, the FCC conditioned its approval of the merger on the combined company's compliance with various conditions on the online content business.
13. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1, 17 July 2000.
14. E-Commerce Directive, Article 2(a), referring to Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC.
15. *See* E-Commerce Directive, Recital (18).
16. E-Commerce Directive, Article 12(1). According to Article 12(2) e-Commerce Directive, the acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
17. E-Commerce Directive, Article 13(1).
18. E-Commerce Directive, Article 14(1).
19. E-Commerce Directive, Article 14(2).
20. Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final of 15 December 2020.
21. Exec. Order No. 13925, 85 Fed. Reg. 34,079 (May 28, 2020).
22. NTIA Petition for Rulemaking to Clarify Provisions of Section 230 of the Communications Act (FCC July 27, 2020), available at *https://www.ntia.gov/files/ntia/publications/ntia_petition_for_rulemaking_7.27.20.pdf*.
23. U.S. Dep't of Justice, Section 230 – Nurturing Innovation or Fostering Unaccountability?: Key Takeaways and Recommendations (June 2020), available at *https://www.justice.gov/file/1286331/download*.
24. *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 407 (6th Cir. 2014) (relying on *Zeran*; internal quotation marks omitted).
25. *NetChoice, LLC v. Moody*, 546 F. Supp. 3d 1082, 1089-90, 1096 (N.D. Fla. 2021). The Eleventh Circuit affirmed this portion of the district court judgment on First Amendment grounds without reaching Section 230. *See* 34 F.4th 196 (11th Cir. 2022).

26. *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1161, 1172-73 (9th Cir. 2008).
27. *Huon v. Denton*, 841 F.3d 733, 742 (7th Cir. 2016).
28. *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1200 (10th Cir. 2009).
29. *Elliott v. Donegan*, 469 F. Supp. 3d 40, 59 (E.D.N.Y. 2020).
30. *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 403 (6th Cir. 2014).
31. *Gonzalez v. Google LLC*, 2 F.4th 871, 896 (9th Cir. 2021); *Force v. Facebook, Inc.*, 934 F.3d 53, 66 (2d Cir. 2019).
32. *Herrick v. Grindr LLC*, 765 F. App'x 586, 588, 590 (2d Cir. 2019).
33. *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1270 (9th Cir. 2016).
34. *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1049-50 (9th Cir. 2019).
35. One of the co-authors of Section 230 made such a point in a panel discussion. *See* What's Missing, Misunderstood in Section 230 Debates, Government Technology (Apr. 13, 2022), available at *https://www.govtech.com/policy/whats-missing-misunderstood-in-section-230-debates*.
36. Facebook has faced multiple lawsuits, including one from the U.S. Department of Housing and Urban Development, alleging that its ad targeting and delivery algorithms discriminate against protected classes. *See, e.g.,* Charge of Discrimination, *HUD v. Facebook, Inc.* (Mar. 28, 2019), available at *https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf*; *see also* Ariana Tobin, HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse, ProPublica (Mar. 28, 2019), available at *https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms*. This lawsuit has now been settled. *See United States v. Meta Platforms, Inc. (f/k/a Facebook, Inc.)*, No. 1:22-cv-05187 (SDNY filed June 21, 2022).
37. The EEOC announced its initiative in 2021. *See* EEOC Press Release, EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness (Oct. 28, 2021), available at *https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness*.
38. *See* EEOC, The Americans with Disabilities Act and the Use of Software Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees (May 12, 2022), available at *https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence*; U.S. Dep't of Justice Civil Rights Division, Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring, available at *https://beta.ada.gov/assets/_pdfs/ai-guidance.pdf*.
39. In addition, the Consumer Financial Protection Bureau has issued guidance that under federal consumer protection law, creditors still need to notify credit applicants of the specific reasons for denying a credit application even if the decision is based on use of a complex algorithm. *See* Consumer Financial Protection Bureau, CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms (May 26, 2022), available at *https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/*.
40. *See, e.g.,* FTC, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI (Apr. 19, 2021), available at *https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai*.