Journal of Law and Policy

Volume 30 | Issue 1 Article 2

12-1-2021

Section 230 and the Problem of Social Cost

Stanley M. Besen

Philip L. Verveer

SECTION 230 AND THE PROBLEM OF SOCIAL COST

Stanley M. Besen[*] *and Philip L. Verveer*[**]

This Article employs, with certain modifications, the framework developed in Ronald Coase's classic article, "The Problem of Social Cost," to analyze the current debate over Section 230 of the Communications Decency Act. This provision absolves interactive computer services, also known as platforms, from liability when they disseminate materials that cause "harm" to third parties, "harm" that can take the form of compensable damage of a sort found in ordinary tort cases but also can include broader injuries to social order and cohesion in the form of such things as hate speech and misinformation. The Article begins by pointing out that, as Coase observes, the ability of private markets to deal with such externalities is limited when the harmful effects are widely distributed, so that many of the entities that are harmed do not have incentives to bring private actions against their sources. It also notes that this problem is compounded in the case of information that is distributed over the internet because of the difficulties involved in identifying, and obtaining jurisdiction over, the ultimate sources of such information. For that reason, it concludes that private actions to limit the dissemination of harmful materials are likely to be more effective if interactive computer services, in addition to information sources, can be held liable by their victims both because the services will often be easier to identify and because they have greater ability to engage in content moderation. However, it also observes that this is likely to be of limited effectiveness, in part because of the difficulties of bringing private actions against these services both because of the cost,

---

[*] Senior Consultant, Charles River Associates. The views in this Article do not represent those of Charles River Associates or any of its clients.

[**] Fellow, Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School. The views in this Article are personal and do not reflect those of the Center or Harvard Kennedy School.

delay, and uncertainty of litigation and because some services may obtain substantial economic benefits when they disseminate harmful information. For these reasons, the Article concludes that policy makers should consider expanding the range of carve outs, provisions that eliminate the immunity from liability that interactive computer services currently enjoy when they are involved in the dissemination of certain types of harmful materials, and that empowering the government to bring civil actions against interactive computer services for disseminating specific types of harmful information should also be considered.

INTRODUCTION

> [I]n choosing between social arrangements within the context of which individual decisions are made, we have to bear in mind that a change in the existing system which will lead to an improvement in some decisions may well lead to a worsening of others. Furthermore, we have to take into account the costs involved in operating the various social arrangements (whether it be the working of a market or of a government department), as well as the costs involved in moving to a new system. In devising and choosing between social arrangements we should have regard for the total effect.[1]

> [T]he rights which individuals possess, with their duties and privileges, will be, to a large extent what the law determines. As a result the legal system will have a profound effect on the working of the economic system and may in certain respects be said to control it. It is obviously desirable that these rights should be assigned to those who can use them most productively and with incentives that lead them to do so and that, to discover and maintain such a distribution of rights, the costs of their transference

---

[1] R.H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1, 44 (1960) [hereinafter Coase].

> should be low, through clarity in the law and by making the legal requirements for such transfers less onerous.[2]

The work of Ronald Coase, the 1991 Nobel Laureate in economics, has had an exceptional influence on antitrust and regulatory policies over the last sixty years. Much of that influence flows from his two scholarly articles: "The Nature of the Firm," published in 1937,[3] and, more prominently, "The Problem of Social Cost," published in 1960.[4] The latter article posits that, assuming no transaction costs, private negotiations between and among interested parties will produce efficient outcomes regardless of how property rights are initially distributed among them.[5] Specifically, Professor Coase showed that costless private transactions would serve to eliminate or reduce negative externalities.[6] However, he was also careful to note that the conditions required to achieve this result often will not be met, so achieving economic efficiency and reducing negative externalities could depend upon the initial assignment of property rights and, in certain circumstances, government intervention in the form of direct regulation might be required to achieve this result.[7] In fact, he observes that "instead of instituting a legal system of rights which can be modified by transactions on the market, the government may impose regulations which state what people must or must not do and which have to be obeyed."[8] Nevertheless, Coase's analysis, with its emphasis on the role of private negotiations in achieving economically efficient outcomes and, more broadly, the efficacy of individual as contrasted with governmental action, has contributed materially to the

---

[2] R.H. Coase, Nobel Prize Lecture on *The Institutional Structure of Production* (1991), https://www.nobelprize.org/prizes/economic-sciences/1991/coase/lecture/ (last visited Oct. 28, 2021) [hereinafter *The Institutional Structure of Production*].

[3] R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937).

[4] Coase, *supra* note 1.

[5] *Id.* at 43–44.

[6] *Id.* at 15–16.

[7] *Id.* at 17.

[8] *Id.*

deregulatory and noninterventionist policies that have prevailed in the United States for more than forty years.[9]

As Coase noted in his Nobel Prize Lecture, his aim in writing "The Problem of Social Cost" was to challenge

> [Arthur] Pigou's conclusion and that of most economists using standard economic theory[, which] was, and perhaps still is, that some kind of government action (usually the imposition of taxes) was required to restrain those whose actions had harmful effects on others, often termed negative externalities. What I showed in that article, as I thought, was that in a regime of zero transaction costs, an assumption of standard economic theory, negotiations between the parties would lead to those arrangements being made which would maximise wealth and this irrespective of the initial assignment of rights.[10]

Pigou's and Coase's respective approaches to the problem of externalities reflect the differences in the European and United States milieus in which each was writing. Pigou recommended direct government intervention in the form of taxes to suppress unwanted externalities, whereas Coase recommended individual initiatives to deal with the same problem, although possibly supplemented with some form of government regulation.[11] These differences in approach can be observed in a large variety of legal and regulatory policies in the respective areas. Specifically, the European Union continues to follow Pigou in relying on action by executive organs in Brussels and European capitals to control negative externalities.[12] By contrast, the United States continues to take an approach that is consistent with Coase's recommendation and relies on individual citizen efforts, in the form of actions in tort, to diminish and deter unwanted externalities.

---

[9] *See* Steven G. Medema, *The Coase Theorem at Sixty*, 58 J. ECON. LIT. 1045, 1046, 1050 (2020).

[10] *The Institutional Structure of Production*, *supra* note 2.

[11] *See id.*

[12] *See* Ottmar Edenhofer et al., *Pigou in the 21st Century: A Tribute on the Occasion of the 100th Anniversary of the Publication of* The Economics of Welfare, 28 INT'L TAX & PUB. FIN. 1090, 1100–01 (2021).

This Article draws on Coase's insights to examine the current debate over possible amendments to Section 230 of the Communications Decency Act, the provision that affords digital platforms such as Facebook, Twitter, and YouTube very substantial immunity from liability for the harmful effects of the content that they provide to their users.[13] Given current concerns about the costs and benefits of Section 230, we believe that an "economic" approach can shed new light on the kinds of revisions to the Section that might improve its operation.[14] We consider whether applying Coase's insights could produce adjustments to Section 230 that would lead to reductions in the negative externalities that result from harmful materials that are distributed over "interactive communications services." We conclude, consistent with Coase, that some expansion of platform liability would likely improve deterrence based on individual effort, but that enabling government civil prosecution of claims based on expanded liability would usefully supplement individual initiative.

---

[13] Telecommunications Act of 1996, Pub. L. No. 104-104, § 230, 110 Stat. 56, 137–39 (codified as amended at 47 U.S.C. § 230(c) (2018)).

[14] Alexandre de Streel, et al., *Liability of Online Hosting Platforms: Should Exceptionalism End?*, CTR. ON REGUL. IN EUR. (Sept. 2018) [hereinafter CERRE Report]. The CERRE Report also takes an economic approach to the issue of platform liability. The CERRE Report, intended as a contribution to the formulation of the European Community's Digital Services Act proposal, covers only "hosting services, which is defined as the storage of information provided by the users of the platform" by Article 14 of the eCommerce Directive, 2000/31/EC. The policy choice to immunize hosting services has been retained in the Digital Services Act proposal. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market for Digital Services (Digital Services Act) and amending the e-Commerce Directive, 2000/31/EC COM/2020/825 final. At various points below we briefly discuss overlaps in our respective analyses. By its own terms, the CERRE Report does not deal with material "that is harmful but legal." *Id.* at 10. By contrast, we intend for the analysis in this article to apply to any service that plays a role in the dissemination of harmful material and that may be able to play a role in limiting that dissemination, even if the material is not illegal.

INTERNET PLATFORMS AS THE SOURCES OF NEGATIVE EXTERNALITIES

The harmful effects that result from the operations of major internet platform companies adversely affect the American population every day, resulting in offsets to the undeniable value that the companies' services also provide.[15] These harms take the form of defamation of individuals, groups, and institutions; dissemination of hate speech; incitements to violence; spreading of misinformation; promotion of fraudulent schemes; and foreign interference in our democratic processes.[16] Significantly, the services provided by platforms convey both the valuable and the destructive, the benign and the malign, with equal efficiency.

By their nature, the harms enabled by the operation of platform services can extend well beyond their immediate sphere of shareholders, creditors, vendors, customers, and employees. As a result, the "victims" can include those that have no *a priori* ability to protect themselves from the resulting damage. What is potentially much worse, the damage could occur to the country's underlying economic and social fabric, with losses both material and immaterial spreading in ways that threaten the social stability and cohesion on which democratic societies depend.

---

[15] *See* Robert H. Frank, *The Economic Case for Regulating Social Media*, N.Y. TIMES (Feb. 11, 2021), https://www.nytimes.com/2021/02/11/business/social-media-facebook-regulation.html (noting that the harms caused by social media platforms offsets the benefits of the services these platforms provide).

[16] There is a wide range of views concerning the significance of this problem. *See, e.g.*, Matt Perault, Section 230: A Reform Agenda for the Next Administration 4 (Oct. 26, 2020) (Day One Project Working Paper), https://9381c384-0c59-41d7-bbdf-62bbf54449a6.filesusr.com/ugd/14d834_16adf8519cc64ab5a6bc5e6a700126da.pdf ("[r]esearch has found that the impact of problematic online content may be relatively small"). Perault is a professor of practice at the University of North Carolina School of Information and Library Science and a former Facebook director of public policy. *But see, e.g.*, Julie E. Cohen, *Tailoring Election Regulation: The Platform is the Frame*, 4 GEO. L. TECH. REV. 641, 647 (2020) (arguing that "[i]n a networked media ecosystem designed for content targeting, optimization for engagement, and amplification of information flows, polarized and polarizing content spreads rapidly from one platform to another and between online and traditional media, gaining in volume as it travels").

A critical consideration is whether information that is disseminated causes harm only to the recipients of the information or whether those who do not receive the information may also be harmed. Consider, for example, a platform that disseminates false information in which the efficacy of a vaccine is questioned.[17] A user who is aware that the original provider of the information is a poor source can elect to ignore the source and, if the platform allows, can even choose to block all information from that source. Suppose, however, that others believe the source and act on it by not getting vaccinated. If a person's health is affected not only by whether he is vaccinated but also by whether others are as well, ignoring or blocking the source will provide him with only limited benefits. Where that is the case, individuals, acting alone, will be unable to avoid the harm caused by the dissemination of the information. As Baker and Robinson observe, "vaccines reduce the probability of getting infected, which reduces the probability of a vaccinated person infecting someone else." [18] Of course, the potential for such third-party effects is not limited to cases of false health information.[19]

It is also important to observe that the legal domain in which these externalities arise is affected by the existence of the First

---

[17] The Centers for Disease Control and Prevention have noted that "[t]he spread of misinformation on social media and through other channels can affect COVID-19 vaccine confidence." *How to Address COVID-19 Vaccine Misinformation*, CDC, https://www.cdc.gov/vaccines/covid-19/health-departments/addressing-vaccine-misinformation.html (last updated Nov. 3, 2021).

[18] Christopher Baker & Andrew Robinson, *Your Unvaccinated Friend is Roughly 20 Times More Likely to Give You COVID*, CONVERSATION (Oct. 27, 2021, 3:13 PM), https://theconversation.com/your-unvaccinated-friend-is-roughly-20-times-more-likely-to-give-you-covid-170448. Baker is Research Fellow in Statistics for Biosecurity Risk, The University of Melbourne and Robinson is CEO of the Centre of Excellence for Biosecurity Risk Analysis, The University of Melbourne.

[19] *See also* Tarleton Gillespie, *Platforms are Not Intermediaries*, 2 GEO. L. TECH. REV. 198, 203 (2018) ("[e]ven if I never saw, clicked on, or liked a fraudulent news post, I still worry others may have done so. I am troubled by the very fact of it and concerned for the sanctity of the political process as a result. Protecting users is no longer enough. The offense and harm in question is not just to individuals but also to the public itself and to the institutions on which it depends.").

Amendment, which significantly limits the potential responses of the United States government to them. Although some negative externalities—those associated with child pornography and imminent incitement to violence, for example—plainly fall outside of First Amendment protection,[20] there obviously are First Amendment values that must be respected in dealing with others.

Excluding the clearly illegal, the ability or inability to address most of the perceived problems in this area is a function of Section 230 of the Communications Decency Act. This 1996 statutory provision, which shelters a platform's editorial judgments from liability to an extent otherwise unknown in our jurisprudence,[21] was intended, among other things, to promote the growth of the then-nascent internet by effectively holding platforms harmless for third-party content that they host or decline to host.[22] It did not affect the potential liability of those who provide content through platform facilities,[23] the ultimate sources of the information that is disseminated over the internet. They remain where the law found them in 1996.[24]

At its most fundamental level, the origin of Section 230 involved competing views about the role of platforms in moderating the content to which they provide access and the limitations imposed by the First Amendment.[25] It did not concern itself with the question of the economic efficiency consequences of granting liability protection to platforms whose business models depend on

---

[20] *See, e.g.*, Robert A. Sedler, *An Essay on Freedom of Speech: The United States versus the Rest of the World*, 2006 MICH. ST. L. REV. 377, 379 (2006); Brett M. Frischmann, *Speech, Spillovers, and the First Amendment*, 2008 U. OF CHI. LEGAL F. 301, 304, 317 (2008) (observing that "the First Amendment is not absolute; the government can and does regulate speech in some limited cases, often with the aim of internalizing negative externalities. [F]or certain types of speech, the costs and benefits of speech are distributed unevenly across groups so that speech that is beneficial to some is harmful to others.") (citations omitted).

[21] Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 203, 212 (2018) ("[t]his was and remains an idiosyncratic and exceptional treatment under law.").

[22] *Id.*

[23] *Id.* at 213.

[24] The Communications Decency Act's legislative history is complicated. *See infra* notes 35–39 and accompanying text.

[25] *See infra* note 49.

transmitting content for which others are the sources. That is the issue we seek to address in this Article, approaching it through the perspective of the famous Coase Theorem.[26] Specifically, we address whether the fact that Section 230 absolves interactive computer services from liability even if the information that they transmit is "harmful" is the most efficient initial assignment of legal rights and, if it is not, whether an efficient rearrangement of those rights can be effected either through private voluntary transactions or through private litigation, enabled by adjustments to the immunity from liability that shields platforms for the carriage of "harmful" content. Our objective is to analyze whether the manner that legal rights are assigned creates a situation in which entities that are involved in the dissemination of information have incentives to limit the dissemination of harmful information whenever the cost of doing so is less than the harm to those who would otherwise be victimized or, in other words, whether the efforts that are undertaken to limit harm will be at efficient levels.[27]

In our analysis, we consider two important factors not explicitly considered by Coase. First, we analyze the implications of the fact that *both* interactive computer services and information originators can limit the amount of harm caused as well as how the responsibility for doing so might be most effectively divided between them. Second, we analyze the implications of the fact that the dissemination of content that may harm some people can increase the profits of the sources of, and the conduits for, that content. With respect to the latter, Gill notes that "platforms use content moderation to promote their economic goals" and that "profits [are] at the forefront of moderation decisions."[28] In

---

[26] *See* Medema, *supra* note 9 for an extensive study of the history and significance of the Coase Theorem.

[27] As will be clear from the discussion below, in the case of the internet, making this determination is likely to be extremely difficult, whether undertaken by a court or a government agency. This is so both because, in many cases, the number of victims will be very large and because quantifying the economic value of the resulting harms will be far from straightforward.

[28] Karanjot Gill, *Regulating Platforms' Invisible Hand: Content Moderation Policies and Processes*, 21 WAKE FOREST J. BUS. & INTELL. PROP. L. 171, 201 (2021). The process by which an entity may prevent the dissemination through its facilities of materials that are provided by others is referred to as *content*

particular, she notes that Facebook initially banned breastfeeding photos despite demands from some users to include them, behavior that she attributes to the fact that "Facebook did not want to alienate potential advertisers and users, whose data they mine."[29] The counterpart, of course, is that platforms may be willing to provide access to harmful content if that *attracts* "potential advertisers and users."[30]

Although Coase notes that his article "is concerned with those actions of business firms which have harmful effects on others,"[31] the analysis is equally applicable to situations in which individuals and firms pursue non-economic objectives and where the "harmful effects" take non-economic form and large numbers of "others" are harmed. Our analysis results in three main findings.

First, the current arrangement in which information content providers but not interactive computer services are liable for the dissemination of harmful content is almost certainly not the most efficient mechanism for suppressing negative externalities. Instead, it is likely that, in many instances, it would be more efficient for victims to bring legal actions against interactive computer services than against content providers. Stated differently, it would often be more efficient for interactive computer services to invest additional resources in content moderation—that is, preventing the dissemination of harmful information—than is currently the case.

It is, of course, an empirical question whether it is more efficient for services or information providers to be the liable entities, but we know of no evidence that suggests that the current assignment of legal rights is the efficient one. On the contrary, plaintiffs have continued to bring actions against entities that were frequently found by the courts to be interactive computer services in the hope that they would, instead, be found to be information providers (or

---

moderation. SARAH T. ROBERTS, CONTENT MODERATION 1 (2017) (defining content moderation as "the organized practice of screening user-generated content (UGC) posted to Internet sites, social media, and other online outlets, in order to determine the appropriateness of the content for a given site, locality, or jurisdiction." Content can be moderated either through the use of artificial intelligence or by humans.).

[29] Gill, *supra* note 28, at 200.

[30] *See id.*

[31] Coase, *supra* note 1, at 1.

otherwise not immune), and thus liable for the harm to the plaintiffs.[32] This may indicate that they do not believe that actions brought against entities which are more clearly information providers are practical or effective ways to obtain redress for the harms that they have experienced.

Second, even if interactive computer services were made liable for the dissemination of harmful content over the internet, it is unlikely that more than a very small proportion of the large number of potential victims would choose to bring legal actions seeking compensation for the harm that they suffered because the amount of harm experienced by any individual will often be too slight, the cost of litigation too great, and the prospect for meaningful recovery too remote to justify taking legal action.[33] Although there may be specific instances in which such actions may be feasible—for example where the information defames a specific individual[34]—and in other situations actions may be brought by an organization or a government instead of by a single individual,[35] this will not likely

---

[32] *See infra* notes 50–54 and accompanying text.

[33] *See* Ronen Perry, *The Law and Economics of Online Republication*, 106 IOWA L. REV. 721, 768 (2020) ("Although the judgment-proof defendant is a general problem in tort law, it is particularly common in cases of online speech torts. Almost everyone in the developed world uses the internet. The ease of access and the veil of anonymity encourage everyone to participate. The typical user is essentially the average citizen with average assets and average income. Consequently, online speakers are often judgment-proof individuals. Typical internet users may not have sufficient assets to pay for the harms caused by their offensive statements. Thus, exclusive originator liability for online publication might result in under-deterrence. Obviously, a wrongdoer's inability to fully pay for the harm caused results not only in under-deterrence, but also in under-compensation. Exclusive originator liability might thus leave the victim with partly compensated harm.") (citations omitted).

[34] *See, e.g.*, Bollea v. Gawker Media, LLC, No. 522012CA012447, 2016 WL 4073660 (Fla. Cir. Ct. June 8, 2016).

[35] *See, e.g.*, Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F. 3d 1157 (9th Cir. 2008) (successfully alleging that housing advertisements carried by Roommates were discriminatory); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill.2009) (county sheriff unsuccessfully claimed that the carriage of "erotic services" by Craigslist constituted a public nuisance). Notably, these were both brought against entities that were found by the court to be internet communications services and thus to be immune from liability under the terms of Section 230.

be an effective solution in many situations. Because of the complex way in which information is distributed over the internet and the large number of service providers, it may not always be possible for victims to identity the specific conduit or conduits through which the harmful information was initially disseminated, let alone to locate the original source of the content[36]—a matter vastly complicated by the practice of reposting by "users" who enjoy the same immunity as the service providers.[37] In such cases, given the costs and uncertainties involved, bringing legal action against a specific interactive computer service for the harm done by the dissemination of a particular piece of information may not be feasible.

Finally, because the dissemination of potentially harmful material may directly enhance the profitability of information services and the utility—monetary and otherwise—of content providers, the amount of such material that appears on the internet is likely to be large. The benefits to purveyors of harmful information, together with the fact that victims are unlikely to be fully compensated for the harm that they experience, provide an additional reason why such harmful information is likely be offered. As a result, the legal system, taking the form of actions in tort, alone may be insufficient to limit the dissemination of harmful information and it may need to be complemented by more direct forms of intervention.

Our analysis leads us to the following policy conclusions about the efficiency-focused appropriateness of Section 230 as it is currently structured. First, making information providers but not interactive computer services liable for the dissemination of harmful information may not be the most efficient assignment of legal rights and, if that is the case, it is highly unlikely that these rights can be reassigned adequately through private transactions—either through contracts or litigation. For that reason, in some cases it may be

---

[36] *See* Michael R. Bartels, *Programmed Defamation: Applying § 230 of the Communications Decency Act to Recommendation Systems*, 89 FORDHAM L. REV. 651, 673 (2020) (describing the difficulty of identifying the origins of online material).

[37] *See* Batzel v. Smith, 333 F.3d 1018, 1030–31 (9th Cir. 2003). *See also* Barrett v. Rosenthal, 146 P.3d 510, 513 (Cal. 2006); *see also infra* note 78 and accompanying text.

desirable to impose liability on the interactive computer services as well as on the sources of the content that they disseminate in order to enable private actions by victims.

Second, even if interactive computer services are held liable for the dissemination of harmful information, because it will often be difficult or impossible for those harmed to bring legal actions against them and because, for at least some platforms, underinvestment in content moderation to limit the dissemination of harmful information may increase their profits, imposing legal liability may be insufficient to control such dissemination. For those reasons, it may be desirable, subject to the limitations posed by the First Amendment, for the government to expand the types of information for which dissemination is banned entirely or for which the government can engage in civil as well as criminal prosecution.

THE CURRENT CONTROVERSIES ABOUT SECTION 230

Section 230 of the Communications Decency Act contains two significant provisions. Subsection (c)(1) provides that "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*."[38] That is, if a computer service merely provides a mechanism through which others disseminate information, it *cannot* be held liable for any adverse effects of the dissemination of that information on others nor can users who simply repost content originated by others. Subsection (c)(2) provides:

---

[38] The statute defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions" and an information content provider as "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." Communications Decency Act, 47 U.S.C. § 230(c)(1) (emphasis added). "[P]ublication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." Barnes v. Yahoo, Inc., 570 F.3d 1096, 1102 (9th Cir. 2009).

> 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).[39]

That is, a service *can* restrict access to information that it finds "objectionable" without incurring liability for doing so. Importantly, subsection (e) carves out certain matters from the immunity protection: violations of federal criminal law, state laws, intellectual property law, certain communications privacy laws, and sex trafficking law.[40]

Overall, this would appear to be the best of both worlds for an interactive computer service. On the one hand, it cannot be held liable if it chooses to do nothing to limit access to the information that is available through its service and, on the other, it cannot be held liable if it chooses to limit such access if it finds the information to be "objectionable."[41] To the extent that there is liability for the dissemination of harmful information, it is to be imposed only on

---

[39] Communications Decency Act, 47 U.S.C. § 230(c)(1) (emphasis added).

[40] *Id.* § 230(e).

[41] Kathleen Ann Ruane, *How Broad a Shield? A Brief Overview of Section 230 of the Communications Decency Act*, CONG. RSCH. SERV. LEGAL SIDEBAR 1, 2 (Feb. 21, 2018), https://sgp.fas.org/crs/misc/LSB10082.pdf (listing Facebook, Twitter, and Google as among the entities that "are permitted to publish others' content without reviewing it for criminality or other potential legal issues." It is important to note, however, that the list of interactive computer services, the entities whose behavior is protected under Section 230, is far longer than this and, in fact, Ruane notes that "[r]eviewing courts have interpreted [the] definition [of interactive computer services] to cover many entities operating online, including broadband Internet access service providers (e.g., Verizon FIOS and Comcast Xfinity), Internet hosting companies (e.g., DreamHost and GoDaddy), search engines (e.g., Google and Yahoo!), online message boards and many varieties of online platforms.").

the source of the information, not, with limited exceptions, on the computer service through which it was disseminated.

It has been observed that the combination of this broad immunity and the business models, especially those of advertiser-supported internet services, has diminished the incentives of internet platforms to engage in content moderation. For example, as the Stigler Committee on Digital Platforms noted:

> [T]he goal of all these [digital platforms] is to maximize engagement, often through extreme or divisive content, as recognized by Facebook itself. Unlike other media, however, [digital platforms] do not have any legal liability for promoting this content, thanks to Section 230 of the Communications Decency Act. This immunity, combined with the limited competition these platforms face, means that [digital platforms] have very weak incentives to promote quality content or to limit the spread of false or divisive information.[42]

The effects of the Section 230 incentive structure on interactive computer services are reflected in the outcomes of numerous lawsuits claiming harm. In a number of cases, the services have been challenged on the grounds that their failure to control the information to which they provide access has injured third parties––that their actions produce negative externalities, harmful effects on others that are ignored by the parties undertaking those actions. In most cases, Section 230 has shielded them from liability for any adverse effects that the dissemination of information through their services may have had.[43] This has led to proposals to modify Section

---

[42] Stigler Committee on Digital Platforms: Final Report, CHI. BOOTH 1, 10 (Sept. 16, 2019), https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf.

[43] We discuss some of these cases below. *See* cases cited *infra* note 63. However, one study involving "a review [of] all Section 230-related court opinions published between July 1, 2015 and June 30, 2016 to determine the extent of immunity . . . [found] that in approximately half of the cases, courts refused to *fully* grant Section 230 immunity." Jeff Kosseff, *The Gradual Erosion of the Law That Shaped the Internet: Section 230's Evolution Over Two Decades*, 18 COLUM. SCI. & TECH L. REV. 1, 3 (2016) (emphasis added). "[S]ome plaintiffs, knowing of courts' relatively broad interpretation of Section 230, may be

230, most often to make interactive computer services liable if the information to which they provide access causes certain defined harms by increasing the subsection (e) immunity carveouts.[44] This Article applies an economic lens to these and other reform proposals to assess their prospects for reducing harms.

HOW SECTION 230 WORKS

The early, influential *Zeran v. America Online* decision addressed Congress' intent in adopting Section 230:

> Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech.

---

discouraged from ever bringing a lawsuit against online intermediaries." *Id.* at 36–37.

[44] *See, e.g.*, Letter from Attorney General, William P. Barr, to The Honorable Michael R. Pence, President, United States Senate (Sept. 23, 2020), https://www.justice.gov/file/1319346/download. The Attorney General proposes that platforms would be excluded from immunity if they: "(1) purposefully promote, facilitate, or solicit third party content that would violate federal criminal law; (2) have actual knowledge that specific content it is hosting violates federal law; and (3) fail to remove unlawful content after receiving notice by way of a final court judgment." More controversially, the letter also proposes that the definition of information content provider be broadened to include "situations in which a platform 'solicits, comments upon, funds, or affirmatively and substantively contributes to, modifies, or alters the content of another person or entity.'" The "comments upon" provision appears designed to address a contemporaneous controversy involving Twitter, Facebook, and others' warnings concerning posts that contained misinformation. *See also* Exec. Order No. 13,925, May 28, 2020, 85 Fed. Reg. 34,079 (June 2, 2020); revoked, Exec. Order No. 14, 029, May 14, 2021, 86 Fed. Reg. 27, 025 (May 19, 2021). Other suggested reforms recommend requiring that services increase transparency in their handling of content and content-related disputes and conditioning immunity on the adoption of "reasonable" content moderation practices. *See, e.g.*, Danielle Keates Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453, 455–56 (2018) (conditioning immunity on a service provider taking reasonable steps to prevent or address unlawful third-party content that it knows about).

> Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.[45]

The decision went on to note that "[b]y its plain language, Section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[46] Although it is indisputable that part of the motivation for the adoption of Section 230 was to enable freer exchange of information on the internet, the court also recognized that "[a]nother important purpose of Section 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services."[47] This observation points to an important part of the Communications Decency Act's origin. When the Act was adopted, there were conflicting congressional views about how best to discourage asserted harms, especially the availability of indecent and offensive material to children.[48] The important point is that there was some expectation of active content moderation despite the fact that subsection (c)(1) taken in isolation apparently affords service providers an opportunity to avoid liability through complete passivity.[49]

---

[45] Zeran v. Am. Online Inc, 129 F.3d 327, 330 (4th Cir. 1997).

[46] *Id.*

[47] *Id.* at 331.

[48] Force v. Facebook, Inc., 934 F.3d 53, 77–80 (2d Cir. 2019) (Katzmann, C.J., concurring in part and dissenting in part) (describing the way in which, with the aid of the Supreme Court, Section 230's approach to content moderation, won out over an alternative employing constitutionally suspect direct prohibition); *see also* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019) (offering an excellent history of Section 230 and the cases leading to its passage); ERIC GOLDMAN & JEFF KOSSEFF, ZERAN V. AM. ONLINE (2020) (ebook) (including essays describing additional history of Congress' deliberations over Section 230 and the history of the Zeran litigation); Danielle Keates Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 404–06 (2017); Sylvain, *supra* note 21, at 235–38.

[49] As former Representative Christopher Cox and Senator Ron Wyden, the authors of Section 230, recalled, "we began with these two propositions: let's make sure that every internet user has the opportunity to exercise their First Amendment rights; and let's deal with the slime and horrible material on the

Section 230 protects an interactive computer service from liability if "in good faith" it chooses to restrict access or availability of various types of material that it finds to be "objectionable."[50] This reduces, but does not completely eliminate, the risk that, in exercising its content moderation function, a service will be successfully sued by the *sources* of such materials. However, it is also important to note what it does *not* do. It does not encourage the service to restrict access to, or the availability of, materials that it finds it profitable to offer regardless of whether an outside observer would find them "objectionable."[51] That is, it provides no affirmative obligation on the part of the service to limit the dissemination of harmful content if it is not in its economic interest to do so. This would be irrelevant to a service whose business model is based on providing access only to materials of high quality, i.e.,

---

internet by giving both websites and their users the tools and the legal protection necessary to take it down." FCC Reply Comments of Co-authors of Section 230 of the Communications Act of 1934, 47 U.S.C. § 230(c)(2) (2018), 8 FCC RM-11862 (Sept. 17, 2020). For additional perspectives on the significance of content moderation, *see* Citron & Wittes, *supra* note 44, at 456; Stigler Committee, *supra* note 42, at 192 (observing that "[a]lthough sometimes viewed as a sweeping libertarian intervention, Section 230 actually began life as a smut-busting provision: an amendment for the 'Protection for Private Blocking and Screening of Offensive Material.' Its purpose was to allow and encourage Internet service providers to create safe spaces, free of pornography, for children."). The European Union's e-Commerce Directive, which was adopted four years after the Communications Decency Act, is similar to Section 230(c)(1). The Directive's Articles 12, 13, and 14 addressing conduit, caching, and hosting services afford providers immunity and do not require them "to monitor the information which they transmit or store, nor . . . to seek facts or circumstances indicating illegal activity." Article 15 of the proposed Digital Services Act retains this policy, which has been referred to as the "passivity paradox." Joris V.J. van Hoboken, *European Intermediary Liability in Historical Perspective*, CEPS BRUSSELS (Mar. 21, 2017), https://www.ceps.eu/wp-content/uploads/2017/03/CEPS%20-%20Limited%20liability%20for%20the%20Net%20-%20Joris%20van%20Hoboken.pdf.

[50] 47 U.S.C. § 230(c)(2). Although Section 230 identifies several specific types of objectionable materials, it also references a broader category of "otherwise objectionable" materials. We intend the analysis in this article to apply to all materials that may adversely affect third parties, not just those enumerated in subsection (c)(2)—"obscene, lewd, lascivious, filthy, excessively violent, [or] harassing."

[51] *See* sources cited *infra* note 102.

materials that are unlikely to be regarded as "objectionable," such as those provided by, say, the American Bar Association, the American Medical Association, or the American Economic Association. However, for services for which that is not the case, where the provision of access to materials of low quality or materials that are clearly "objectionable" is, in fact, their "stock in trade," the Act provides no obligation for them to limit access to such materials.

"Objectionable" materials may include, for example, the content of so-called "predatory journals," which appear to be unconcerned with the quality of the articles that they publish so long as doing so increases their profits, which result from the publication fees that they impose on authors.[52] Such services may exploit the fact that they are not liable under Subsection (c)(1) for the materials to which they provide access by *not* taking advantage of their freedom under Subsection (c)(2) to remove materials that others find objectionable.[53]

---

[52] For a discussion of the practices of these journals, *see* Agnes Grudniewicz, et al., *Predatory Journals: No Definition, No Defence,* NATURE (Dec. 12, 2019), https://www.nature.com/articles/d41586-019-03759-y. *See also* Anna Severin & Nicola Low, *Readers Beware! Predatory Journals are Infiltrating Citation Databases*, 64 INT. J. PUB. HEALTH 1123 (2019) ("Publishers of predatory journals are businesses that reap profits by ignoring scientific integrity. They exploit the online open access model of publication, which aims to make research findings freely available to all and to allow authors to retain copyright of their work. Predatory publishers operate large numbers of online 'journals' that offer to publish articles in return for a fee, but do not conduct the kind of peer review, or offer the editorial services, expected from legitimate journal publishers. Indeed, many of their practices are fraudulent.") (citations omitted). *See also* Fed. Trade Comm'n v. OMICS Group, 374 F.Supp.3d 994 (D. Nev. 2019), *affirmed* No. 19-15738 (9th Cir. Sept. 11, 2020) (unpublished opinion) (finding that defendants engaged in unfair and deceptive practices with respect to the publication of online academic journals and organization of scientific conferences). The SAFE TECH Act, *infra* note 109, would eliminate the immunity for content in which the platform has an economic interest.

[53] Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1016 (2008) (noting that "the same economic incentives . . . identified for mass media like newspapers and television stations push ISPs towards promoting advertiser-friendly content. [This makes them] willing to sacrifice individual users for a better image for advertisers and investors, and this pattern is likely to continue as aggregators attempt to monetize popular spaces such as Facebook and YouTube.").

Another source of potentially harmful information are so-called content farms, which are described as "sites that deliberately cater their content to what is trending on search engines at any given time. The credibility of the information generated by them is dubious at best."[54] Similarly, Gupta notes that "content farm sites, which may not be sharing the correct information . . . rank very highly on Google and have the potential to lead [sic] casual readers with the wrong information."[55]

Predatory journals and content farms are not the only examples of platforms whose business models are based on the dissemination of harmful information. For example, Johnson and Castro claim that "[t]here are untold numbers of online services whose users post child sexual abuse material, nonconsensual pornography, defamatory 'gossip,' terrorist communication, and more."[56] Similarly, Citron and Wittes have noted that platforms have "republished content knowing it might violate the law, encouraged users to post illegal content, changed their design and policies for the purpose of enabling illegal activity, or sold dangerous products."[57] Still other examples are websites that post slanderous materials and then attempt to charge the victims to remove the posts.[58] Google recently began adopting algorithmic changes that are intended to make it more difficult for such content to be reached through its platform.[59] Finally, the Department of Justice refers to

---

[54] Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1, 5, n. 17 (2011).

[55] Siddharth Gupta, *Holding Media Channels, Private Corporations and Data-Collecting Entities Accountable for Their Lack of Content Moderation*, RSCH. GATE (May 2020), https://www.researchgate.net/publication/342491765_Holding_Media_Channels_Private_Corporations_and_Data-Collecting_Entities_Accountable_for_their_Lack_of_Content_Moderation.

[56] Ashley Johnson & Daniel Castro, *Proposals to Reform Section 230*, 4 INFO. TECH. & INNOVATION FOUND. (Feb. 22, 2021), https://itif.org/publications/2021/02/22/proposals-reform-section-230.

[57] Citron & Wittes, *supra* note 44, at 408 (citations omitted).

[58] Aaron Krolik & Kashmir Hill, *The Slander Industry*, N.Y. TIMES (Apr. 24, 2021), https://www.nytimes.com/interactive/2021/04/24/technology/online-slander-websites.html.

[59] Pandu Nayak, *Improving Search to Better Protect People from Harassment*, GOOGLE BLOG (June 10, 2021), https://blog.google/products/search/improving-search-better-protect-people-harassment/ ("[W]e're implementing an

platforms that "purposely solicit and facilitate harmful criminal activity . . . ."[60]

Section 230: (i) reduces or eliminates liability that a service may incur in providing access to information for which others are the sources and to that extent reduces its incentives to limit the quantity of "objectionable" material that it disseminates; (ii) has no material incentive effect on the amount of objectionable content offered by a service whose business model is already based on eliminating objectionable content; and (iii) has no suppressing effect on the amount of objectionable material to which a service provides access where offering such material is the source of its profits.[61] By virtue of Section 230, the amount of objectionable material that is offered depends not on the legal liability of the interactive computer services but instead on the legal liability *as a practical matter* of the information content providers to whose materials the service provides access. Content originators stand before the law as they always have, albeit in a technological milieu that the internet has made very different over the last three decades.

In the preponderance of litigated cases, interactive computer service defendants have been found *not* to be liable for the adverse effects of the content that appeared on their services, even where those effects were transparent.[62] For example, in *Force v. Facebook,*

---

improvement to our approach to further protect known victims. Now, once someone has requested a removal from one site with predatory practices, we will automatically apply ranking protections to help prevent content from other similar low-quality sites appearing in search results for people's names . . . . This change was inspired by a similar approach we've taken with victims of non-consensual explicit content, commonly known as revenge porn."). *See also* Kashmir Hill & Daisuke Wakabayashi, *Google Takes Steps to Break the Cycle of Online Slander*, N.Y. TIMES (June 10, 2021), https://www.nytimes.com/2021/06/10/technology/google-algorithm-known-victims.html.

[60] U.S. DEP'T OF JUST., THE JUSTICE DEPARTMENT UNVEILS PROPOSED SECTION 230 LEGISLATION (Sept. 23, 2020), https://www.justice.gov/opa/pr/justice-department-unveils-proposed-section-230-legislation.

[61] 47 U.S.C. § 230.

[62] A partial list of cases, in addition to those discussed here, in which entities were found *not* to be liable for the dissemination of harmful content on the grounds that they were internet service providers includes: Ben Ezra, Weinstein and Co. v. Am. Online, 206 F.3d 980 (10th Cir. 2000); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006); Chicago

Inc., the plaintiffs, who included "U.S. citizen victims, and relatives and representatives of the estates of those victims, of certain terrorist attacks committed by Hamas in Israel," sued Facebook alleging that it had provided Hamas "with a communications platform that enabled those attacks." The Court of Appeals for the Second Circuit upheld a district court's dismissal court of the complaint based on Section 230 immunity.[63]

In *Doe v. Backpage.com, LLC*, each of the three plaintiffs alleged that she was the victim of sex trafficking at age 15 and each alleged that she was subject to rape—"over 1000 times," "over 900 times," and "on numerous occasions," respectively.[64] Although the First Circuit panel, including retired Supreme Court Justice Souter, concluded that the plaintiffs had made a persuasive case "that Backpage has tailored its website to make sex trafficking easier," Section 230 "requires that we . . . deny relief to plaintiffs whose circumstances evoke outrage."[65]

In *Barnes v. Yahoo!*, Section 230 was found to preclude recovery on a state law negligence claim notwithstanding "a dangerous, cruel, and highly indecent use of the internet for the apparent purpose of revenge."[66] In that case, the court found that "Barnes did not authorize her now former boyfriend to post the profiles, which is hardly surprising considering their content."[67] "The profiles contained nude photographs of Barnes and her boyfriend, taken without her knowledge, and some kind of open solicitation, whether express or implied is unclear, to engage in sexual intercourse."[68] "The ex-boyfriend then conducted discussions in Yahoo's online 'chat rooms,' posing as Barnes and directing male correspondents to the fraudulent profiles he had created."[69] "The profiles also included the addresses, real and electronic, and telephone number at

---

Laws.' Comm. For Civ. Rts. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); and Carafano v. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003).

[63] Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019).

[64] Doe v. Backpage.com, 817 F.3d 12, 17, 29 (1st Cir. 2016).

[65] *Id.* at 15, 29.

[66] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).

[67] *Id.*

[68] *Id.*

[69] *Id.*

Barnes' place of employment."[70] Before long, men whom Barnes did not know were peppering her office with emails, phone calls, and personal visits, all in the expectation of sex.[71]

Similarly, in *Herrick v. Grindr LLC*, the plaintiff, who was "the victim of a campaign of harassment by his ex-boyfriend, who created Grindr profiles to impersonate Herrick and communicate with other users in his name, directing the other users to Herrick's home and workplace," brought suit against Grindr, a "hook-up" application, arguing that it was "defectively designed and manufactured because it lacks safety features to prevent impersonating profiles and other dangerous conduct, and that Grindr wrongfully failed to remove the impersonating profiles created by his ex-boyfriend."[72] A district court ruled that Grindr was an interactive computer service, so Herrick's claims were barred by Section 230, among other factors, and the ruling was upheld by the Court of Appeals for the Second Circuit.[73]

Despite these holdings, some courts have concluded that an interactive computer service was insufficiently passive to qualify for the (c)(1) immunity.[74] For example, in *MCW, Inc. v. badbusinessbureau.com*, the court held that the defendant that created such category headings as "Con Artists" and "Corrupt Companies" for consumer complaints was not immune from liability under the terms of Section 230.[75] In that case, the court found that

> the CDA does not distinguish between acts of creating or developing the content of reports, on the one hand, and acts of creating or developing the titles or headings of those reports, in the other. The titles and headings are clearly part of the web page content. Accordingly, the defendants are information content providers with respect to the website postings and

---

[70] *Id.*

[71] *Id.*

[72] Herrick v. Grindr LLC, 765 F. App'x. 586, 588 (2d Cir. Mar. 27, 2019) (unpublished summary order).

[73] *See id.* at 589–91.

[74] *See* MCW, Inc. v. badbusinessbureau.com, LLC., No. Civ.A.3:02–CV–2727–G**,** 2004 WL 833595, at *10 (N.D. Tex. Apr. 19, 2004).

[75] *Id.*

> thus they are not immune from MCW's claim . . . . [T]he defendants are also information content providers because they are "responsible, in whole or in part, for the creating or development" of third-party derogatory messages.[76]

Fair Housing Council of San Fernando Valley v. Roommates.com, LLC involved a website that required disclosure of personal information—gender, family status, and sexual orientation—as a condition of use and employed profiles derived from the information as an integral part of its real estate service.[77] "By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information."[78] Based on this finding, the Ninth Circuit concluded that Roommates could not claim immunity under the terms of Section 230.[79]

Although these cases illustrate that an entity may risk losing the immunity provided under Section 230 if it behaves as more than a mere conduit for information provided by others, the preponderance of cases reinforces a conclusion that an interactive computer service will be able to avoid being classified as an information provider, and thus subject to liability for harm caused by the content that it disseminates, if it is careful *not* to take actions that modify that content. That is, although Section 230 contains a provision that permits an interactive communication service to delete certain types of materials under (c)(2), there is a risk that it will jeopardize the freedom from liability that it would otherwise possess under (c)(1) if it engages in *any* editorial behavior. Concomitantly, a plaintiff's options regarding the party against which to bring suit are severely limited by the provisions of Section 230. As the California Supreme Court has put it: "We acknowledge that recognizing broad immunity for defamatory republications on the Internet has some troubling

---

[76] *Id.* (quoting 47 U.S.C. § 230(f)(3)).

[77] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F. 3d 1157, 1161 (9th Cir. 2008) (en banc).

[78] *Id.* at 1166.

[79] *Id.* at 1170.

consequences. Until Congress chooses to revise the settled law in this area, however, plaintiffs who contend they were defamed in an Internet posting may only seek recovery from the original source of the statement."[80]

Using Coase's insights, we consider the sources of the "troubling consequences" referred to by the Court and how Congress might revise the law to deal with those consequences. We conclude that revisions that facilitate private actions that seek damages from interactive computer service for the dissemination of harmful content over the internet would have a positive effect in reducing negative externalities. However, we also conclude that such revisions are unlikely, by themselves, to address fully the consequences of the dissemination of harmful content and, as a result, Congress might need to consider more significant reforms.

COASE'S APPROACH TO THE PROBLEM OF SOCIAL COST

Economists have long been engaged in the analysis of legal arrangements in which the activities of one party can affect the well-being of another. In these situations, some economists, guided by the work of Coase, have focused on how the assignment of legal (or property) rights affects the efficiency with which resources are allocated and on whether private voluntary transactions are sufficient to achieve an efficient allocation.[81] Moreover, Coase's insights have not been limited to economists. They have been extraordinarily influential among policymakers over the last several decades, specifically in connection with the deregulatory and non-interventionist milieu of the last five decades and with the

---

[80] Barrett v. Rosenthal, 146 P.3d 510, 525 (Cal. 2006). The opinion contains an exhaustive discussion of Section 230's legislative history and holds that "[b]y declaring that no 'user' may be treated as a 'publisher' of third-party content, Congress has comprehensively immunized republication by individual Internet users." *Id.* at 528. In other words, the re-posters of content enjoy the same (c)(1) immunity as service providers. Only originators of actionable content are exposed to liability under Section 230. For an extended discussion of user immunity and its consequences, see Ronen Perry, *supra* note 33.

[81] For an example of this approach taken by one of the authors of this article *see* Stanley M. Besen, et al., *Copyright Liability for Cable Television: Compulsory Licensing and the Coase Theorem*, 21 J. L. & ECON. 67 (1978).

concomitant assignment of rights and obligations in legislation that affects commercial activities.[82] In this Article, we begin with the basic model analyzed by Coase and modify it to reflect the specific characteristics of the situations covered by Section 230.

The simplest of the situations analyzed by Coase has the following conditions: (1) there is a single entity on each side of the interaction, in his case, one farmer and one rancher; (2) both entities are fully integrated, in particular, the cattle that graze on the rancher's land are owned by the rancher; and (3) the harm that may be occasioned as a result of the interaction between the entities is a by-product of an otherwise legitimate activity, i.e., the rancher benefits from having its cattle graze but the harm that may be done to the farmer's crop does not, by itself, provide any benefits to the rancher.[83] Coase shows that, in this situation, irrespective of whether the rancher is liable for any harm caused by the grazing of his cattle to the farmer's crops—that is, regardless of whether property rights are assigned to the farmer or the rancher—an efficient outcome will result *if transactions between the farmer and the rancher are costless to execute*. If the law holds the farmer safe from damage caused by trespass, the rancher will construct a fence to prevent his cattle from entering the farmer's land if the cost of doing so is less than the value of the crops that would otherwise be damaged.[84] If the rancher is *not* liable, and the cost of constructing a fence is less than the damages to the crops, the farmer will pay the rancher to construct a fence.[85] If the rancher *is* liable for damages to the crops and the cost of constructing a fence is greater than the damages, the rancher will compensate the farmer for the damages but will not construct a fence.[86]

Of course, Coase did not stop his analysis in the case in which transactions are costless. In particular, he observes:

> Once the costs of carrying out market transactions are taken into account, it is clear that . . . a

---

[82] *See, e.g.*, BINYAMIN APPELBAUM, THE ECONOMISTS' HOUR (2019); Medema, *supra* note 9.

[83] Coase, *supra* note 1.

[84] *Id.*

[85] *Id.*

[86] *Id.*

> rearrangement of rights will only be undertaken when the increase in the value of production consequent upon the rearrangement is greater than the costs which would be involved in bringing it about . . . . In these conditions, the initial delimitation of legal rights does have an effect on the efficiency with which the economic system operates.[87]

In fact, Coase modified his initial example to take account of the costs of "rearranging" rights.[88] With respect to the number of market participants that would have to reach agreement through private voluntary transactions, Coase noted:

> there is no reason why, on occasion . . . government administrative regulation should not lead to an improvement in economic efficiencies. This would seem to be particularly likely *when a large number of people are involved* and in which therefore the costs of handling the problem through the market or the firm might be high.[89]

In this regard, it is interesting to note that among the proposals to modify Section 230 put forward by the Trump Administration's Department of Justice there is one that would enable the federal government to bring *civil claims* against platforms where subject matter is carved out from liability immunity, rather than rely solely on victims to bring civil actions for harms that they experienced from such dissemination.[90] In this kind of legal regime, of course, victims could still choose to bring actions to seek recompense for the injuries that they experience.

Consider a case in which, contrary to Coase's hypothetical, there are many farmers and only one rancher. In that case, the farmers may be unable to unite either to sue to force the rancher to build a fence or to pay him to erect a fence. Moreover, the likelihood that an efficient allocation of resources will be achieved through private

---

[87] *Id.* at 15–16.

[88] *Id.* at 18.

[89] *Id.* at 18 (emphasis added).

[90] *See* THE JUSTICE DEPARTMENT UNVEILS PROPOSED SECTION 230 LEGISLATION, *supra* note 60.

transactions or by legal actions may be affected if, to enlarge the hypothetical, there are many owners of land on which cattle graze and which may harm farmers if they enter their land. In other words, if there are many prospective plaintiffs or defendants, free rider, coordination, or assignment of causality problems could, all else equal, inhibit private efficiency-increasing transactions. For example, even after crops have been damaged, if there are many adjacent ranches, the farmer may be unable to identify the specific owner or owners of the cattle that have caused the damage. In such cases, the efficient alternative may be to *require* all ranchers to build fences. As Coase noted, "there is no reason why, on occasion . . . governmental administrative regulation should not lead to an improvement in economic efficiency. This would seem particularly likely when . . . a large number of people are involved and in which therefore the costs of handling the problem through the market or the firm may be high."[91]

Coase also considered the question of whether the initial assignment of legal rights can affect whether an efficient allocation of resources can be achieved through private voluntary transactions. He noted:

> One arrangement of rights may bring about a greater value of production than any other. But unless this is the arrangement of rights established by the legal system, the costs of reaching the same result by altering and combining results through the market may be so great that this optimal arrangement of rights, and the greater value of production that it would bring, may never be achieved.[92]

Following this approach, we address the question of whether "greater value" can be achieved by the "*re*arrangement of rights" provided by Section 230.[93] In other words, whether "altering and combining these rights through the market"[94] can be achieved, and whether the government should undertake additional actions to limit the dissemination of harmful information through the internet.

---

[91] Coase, *supra* note 1, at 18.

[92] *Id.* at 16.

[93] *Id.* at 15–16.

[94] *Id.*

One factor that we address, not considered in Coase's examples, is that, in analyzing Section 230, we must take account of the fact that interactive computer services and information content providers *both* are able to limit the amount of harm. To modify Coase's example to take this possibility into account, consider A, a farmer, whose land is adjacent to property owned by B, *who allows cattle owned by a large number of different entities to graze on his land*.[95] As in the case described above, it will be efficient to construct a fence between the properties so long as the cost of doing so is less than the value of the crops that would otherwise be destroyed. In that case, a fence *will* be constructed if: (i) B is liable for the damages that are caused by straying cattle and the cost of bringing suit against B is not too large; (ii) the cattle owners are liable for the damages and the cost of bringing suit against them is not too large; or (iii) neither B nor the cattle owners are liable for damages to the crops and A pays B to erect a fence. Note that if the cattle owners, but not B, are liable for damage to A's crops, A will have to identify, and sue, individual owners of straying cattle and no individual cattle owner, even if found liable, may find it profitable to bear the cost of erecting a fence. In that case, the fact that the cattle owners are liable for crop damages would have no effect on their behavior. Of course, A could still pay B to erect a fence.

A second factor that we consider, not considered in Coase's examples, is that the dissemination of harmful information may provide monetary or other benefits to the source of harm. In Coase's examples, the rancher may choose not to erect a fence not because he benefits when his cattle stray and damage the farmer's crops but because he would incur a cost in erecting the fence. However, the rancher could obtain benefits when his cattle stray, say because they are able to graze on the farmer's land or because their condition is improved when they eat the farmer's crops. For similar reasons, an interactive computer service, an information content provider, or both could find it profitable to offer harmful material not only because that reduces the cost of content moderation but because doing so increases the advertising revenues, subscriber fees, or other

---

[95] We have modified Coase's original example to allow for the distinction between the internet services that users access directly and the providers of the information that those services host.

payments that they receive. If that is the case, the service or the provider would take into account not only the harm for which they are liable and the direct costs that they incur in limiting the amount of harmful materials that they generate but also the addition to their profits from the carriage of those materials, which might be thought of as the *opportunity cost* of reducing or eliminating their dissemination of those materials.[96]

That platforms engage in behaviors that are intended to attract users hardly seems controversial, but the proposition becomes contentious in the context of social media's use of algorithms to present and amplify content. For example, a recent press report has observed that "Facebook and other social media platforms use engagement-based ranking to determine which content they believe is most relevant to users' interests. After taking into account a post's likes, shares and comments, as well as a user's past interactions with similar content, the algorithms powering someone's Twitter feed or Facebook's news feed will place posts in front of that person."[97] The report also indicated that, in 2018, Facebook began to employ a new metric, Meaningful Social Interactions, "to give more weight to the posts and engagements of people that Facebook thought were closest to users."[98] Although such activities can be thought of as merely serving the interests of users, some have argued that platforms do not do enough to screen out harmful materials and, indeed, that they lead to the dissemination of such materials if doing so contributes to user engagement.

This consideration—the primacy of user engagement subject to algorithmic magnification—is likely to affect whether private voluntary transactions will be sufficient to limit the amount of harm and whether the initial assignment of legal rights is efficient. It also means that even if the amount of harmful material being disseminated is efficient from an economic point of view in the

---

[96] In a common example in which the operation of a factory contributes to air pollution, the factory owner may prefer to compensate those that are harmed by the pollution rather than remediating it if the resulting cost savings are greater than the liability that it incurs. *See id.* at 41–44.

[97] Ryan Mac, *Engagement Ranking Boost, M.S.I., and More*, N.Y. TIMES (Oct. 5, 2021), https://www.nytimes.com/2021/10/05/technology/engagement-ranking-boost-msi-facebook.html.

[98] *Id.*

sense that victims are fully compensated, that amount may still be substantial.[99]

In fact, some analysts have maintained that platforms may benefit when they provide content that others would regard as harmful. For example, Franks notes:

> [S]ocial media platforms in anti-social disputes often have no incentive to resolve or prevent the conflicts at issue. They may in fact have incentives to ignore or even to aggravate them. This is due in large part to the business model of many social media companies. They do not make money by selling products; they make money by selling ads. Increased engagement with their platforms, whether for pro-social or anti-social purposes, translates into increased profits: "[A]busive posts still bring in considerable ad revenue and the more content that is posted, good or bad, the more ad money goes into their coffers." This can create incentives for platforms to be indifferent to or even encouraging of inequalities of power among users. For some of these platforms, online abuse may be, as the saying goes, "not a bug but a feature."[100]

---

[99] This is in addition to the fact that bringing legal actions against the service or the provider are likely to be highly imperfect means for limiting harm both because there may be a large number of victims each of which experiences only a small amount of harm, which reduces their incentives to bring legal actions, and because of the inevitable shortcomings of the legal system in dealing with harm. One way in which the legal system might compensate for these shortcomings is by awarding successful plaintiffs more than their actual damages. *See, e.g.*, John M. Connor & Robert H. Lande, *The Size of Cartel Overcharges: Implications for U.S. and EU Fining Policies*, 51 ANTITRUST BULL. 983, 984–85 (2006) (noting that "penalties . . . should be equal to the violation's 'net harm to others' divided by the probability of detection and proof of the violation") (citations omitted).

[100] Mary Anne Franks, *Justice Beyond Dispute*, 131 HARV. L. REV. 1374, 1381–82 (2018) (book review) (citations omitted); *see also id.* at 1385–86 ("[Anti-social disputes] are one-sided, antagonistic, and involve dramatic disparities of power as well as unjustifiable allocations of burdens and benefits. They are better characterized as attacks than disputes. The most damaging and widespread social media conflicts, including horrific Facebook Live videos, revenge porn, online harassment campaigns, violent propaganda, conspiracy theories, and 'fake news,' almost always involve involuntary interactions . . . .

Recent congressional testimony by a former Facebook data scientist agreed with that assessment. In her testimony, Frances Haugen told Congress that

> Facebook repeatedly encountered conflicts between its own profits and our safety. *Facebook consistently resolved those conflict in favor of its own profits.* The result has been a system that amplifies division, extremism, and polarization . . . . In some cases, this dangerous online talk has led to actual violence that harms and even kills people.[101]

In effect, Haugen was arguing that, in striking the balance between the costs that it incurs in removing harmful content from its platforms and the additional profits that it obtains when that content attracts additional users, Facebook often strikes the balance in favor of the additional profits.[102] Of course, that balancing is likely be affected, at least in part, by the fact that, under the provisions of Section 230, Facebook incurs no liability for any harm caused by any content that it disseminates.

Other analysts have taken the opposite view. For example, Johnson and Castro have argued that

> companies have powerful economic incentives for keeping harmful or illegal content off their platforms. The first is to protect their brand and reputation, exemplified by the recent "techlash," or backlash

---

The powerful corporations that provide the technology and the platforms for these attacks often have few incentives to stop them, and in some cases are incentivized to ignore or aggravate them.").

[101] Statement of Frances Haugen, United States Senate Committee on Commerce, Science and Transportation, Sub-Committee on Consumer Protection, Product Safety, and Data Security, Oct. 4, 2021, https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49 (emphasis in original). *See also* SHEERA FANKEL & CECILIA KANG, AN UGLY TRUTH: INSIDE FACEBOOK'S BATTLE FOR DOMINATION (2021) (suggesting that Facebook favors growth over safety).

[102] In an October 5, 2021 blog post response to Haugen's testimony, Facebook CEO Mark Zuckerberg wrote that "[t]he argument that we deliberately push content that makes people angry for profit is deeply illogical. We make money from ads, and advertisers consistently tell us they don't want their ads next to harmful or angry content." Mark Zuckerberg, FACEBOOK (Oct. 5, 2021), https://www.facebook.com/zuck/posts/10113961365418581.

> against major tech companies that arose from widespread disinformation on social media surrounding the 2016 U.S. elections. This negative attention chases users away from companies' platforms and motivates lawmakers to consider policies that would be detrimental to companies' business models. The second is advertising revenue. Advertisers do not want their products and services promoted next to harmful or illegal content. If platforms gain a reputation for hosting this content, they risk losing advertiser revenue. A third incentive comes from consumers, most of whom do not want to use online services that are full of harmful or illegal content.[103]

Nonetheless, Johnson and Castro do note that "there are some bad actors that design their platforms to amplify and profit from harmful or illegal content—such as revenge porn websites, websites such as Backpage that protected sex traffickers, or websites such as Dirty World that solicit defamatory statements from commenters—for whom market incentives have little effect."[104] They further explain that "[b]ad actors can and do still end up facing civil and criminal penalties for violating other laws . . . . Law enforcement

---

[103] Ashley Johnson & Daniel Castro, *Fact Checking the Critiques of Section 230: What Are the Real Problems?*, 4 INFO. TECH. & INNOVATION FOUND. (Feb. 2021). *See also* Brent Skorup & Jennifer Huddleston, *The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation*, 72 OKLA. L. REV. 635, 664 (2020) ("Even absent strict regulation, most platforms prefer to exclude obscene and graphic material as a way to grow their user bases and make it easier to cultivate relationships with potential advertisers or other financial supporters.") (citation omitted); *see also* Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet as It Is (and as It Should Be)*, 118 MICH. L. REV. 1073, 1086 (2020) ("To be sure, tech companies do moderate certain content by shadow banning, filtering, or blocking it. They have acceded to pressure from the European Commission to remove hate speech and terrorist activity. They have banned certain forms of online abuse, such as nonconsensual pornography, in response to pressure from users, advocacy groups, and advertisers. When it is bad for business, platforms have expended resources to stem abuse.") (citations omitted).

[104] Johnson & Castro, *supra* note 103, at 4.

can also take action against websites, as Section 230 does not shield online services from federal criminal liability."[105]

APPLYING COASE'S ANALYSIS TO SECTION 230

What if Coase's mode of thinking is applied to Section 230? In this case, the interactive computer service plays the role of the owner of the land on which cattle are permitted to graze, the information content providers play the role of the owners of the grazing cattle, and anyone who might be adversely affected by the materials that are provided through the interactive computer service plays the role of the farmer. As already noted, what is different about this case is that, unlike the Coase example in which there is a single farmer and a single rancher, here there are many "farmers" and many "ranchers" and, moreover, in this case the "land" on which cattle are permitted to graze is owned by someone other than the "owners of the cattle." Moreover, whereas in the Coase example, the land-owning rancher may be liable for the harm done by gazing cattle, Section 230 largely frees the interactive computer service from liability from any harm that is caused by the content that is transmitted over its the facilities, leaving potential liability only for the suppliers of the content itself. Finally, as noted above, the business models of some interactive computer services and information content providers may be based on the dissemination of harmful materials whereas Coase's rancher benefits directly only through his ownership of cattle.

We recognize, of course, that these "economic" considerations were not the primary motivation for the enactment of Section 230, nor do they appear to have played a role in the judicial decisions that have interpreted the Section. For example, as the earliest and most influential construction of Section 230 noted:

> The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive

---

[105] *Id.*

> government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, *with a minimum of government regulation.*" Congress further stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation.*"[106]

In Coase's simplest example, it is at least imaginable that a single farmer could make a payment to a single rancher to avoid the damages that might be caused to the farmer's crops by straying steers, assuming, of course, that the cost of building a fence is smaller than the value of the crops that would otherwise be lost. Presumably the farmer would be aware of the existence of the nearby ranch and could at least estimate the likelihood and

---

[106] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (emphasis added) (internal citations omitted). Notwithstanding the many decisions that follow *Zeran* in declining to weigh the evident negative consequences in finding broad platform immunity, in a filing with the Federal Communications Commission, former Representatives Cox and Wyden, the co-sponsors of Section 230, suggest that some concern about negative externalities was part of their motivation:

> Section 230 was not designed to assist a nascent industry . . . but rather to address a problem already recognizable in 1996 that has only grown in significance since then. A world without Section 230, in which people could be sued for taking down hate speech or misinformation, would be a much more unpleasant place.

Reply Comments of the Co-authors of Section 230 of the Communications Act of 1934, FCC Docket RM-11862 at 8, 9–10 (Sept. 17, 2020).

frequency of crop destruction and the amount of the resulting damages. Indeed, the farmer might even have begun to farm after the rancher had begun operation so might be thought of as "coming to the nuisance."[107]

Of course, Coase recognized that that this outcome may not be achievable through private voluntary transactions so that regulation might be required to achieve an economically efficient outcome.[108] If anything, in the situation that we are examining, the possible harm caused by information that is transmitted over the internet is far worse. Here, economic efficiency may not be achieved through private voluntary transactions irrespective of whether interactive computer services or information providers are liable for damages caused by the dissemination of harmful information. That may be the case for two reasons. First, victims are often likely to find it difficult or impossible to identify the source of the information.[109] As Coase pointed out, an obvious prerequisite, among others, is identifying the counterparty:

> In order to carry out a market transaction it is necessary to discover who it is that one wishes to deal with, to inform people that one wishes to deal and on what terms, to conduct negotiations leading up to a bargain, to draw up the contract, to undertake the inspection needed to make sure that the terms of the contract are being observed, and so on. These operations are often extremely costly, sufficiently costly at any rate to prevent many transactions that would be carried out in a world in which the pricing system worked without cost.[110]

Second, the losses to individual victims may be insufficient to justify their bringing legal actions.[111] Likewise, the cost and

---

[107] *See* Coase, *supra* note 1, at 17.

[108] *Id.*

[109] *See* Johnson & Castro, *supra* note 103, at 5–6.

[110] Coase, *supra* note 1, at 15.

[111] Similarly, where many factories in an area are polluting the environment, someone that is harmed by the pollution is unlikely to be able to identify the specific source or sources and, as a result, direct government regulation may be required to limit the resulting externalities. *Id.* at 16.

inevitable uncertainties surrounding judicial resolution could cause victims to forswear seeking redress.

In Coase's simplest example, the farmer and the rancher are assumed to be able to costlessly negotiate about whether the rancher should erect a fence because both are aware of the possibility that the rancher's cattle will stray and of the amount of damage to the farmer's crops if that occurs.[112] The situation in the case of damage caused by the dissemination of harmful information over the internet is, of course, very different.[113] Even if we ignore the fact that there are many possible victims and many possible sources of harm, no single potential victim is likely to be able to anticipate that it will be harmed, the magnitude of the harm that it will experience if that were to occur, or even to be aware of the potential source or sources of the harmful information. That is, the amount of harm experienced by any *individual* and the identity of the entity that caused the harm can only be determined after it has occurred. In those circumstances, any individual is highly unlikely to be able to pay the source of the harmful information or to engage in legal action to prevent its dissemination.

This problem is compounded, of course, if the same information causes harm to many entities rather to only one, and the problem is likely to persist even if liability for the dissemination of harmful information is expanded from information providers to include interactive computer services, as is the case with respect to the carve outs in Section 230's subsection (e). This makes *ex ante* negotiations or litigation to forestall the harm impossible. Of course, it may be possible, roughly at least, to estimate the amount of harm to all victims *in the aggregate* but that would not facilitate transactions between individual victims and even a single source of potential harm. For that reason, compensation for the damage caused by the dissemination of harmful information can occur only *after* the harm has occurred and even that may not be possible if the harm is

---

[112] *Id.* at 3–8.

[113] The analogy to the construction of a fence by the rancher is, of course, content moderation by an interactive computer service.

sufficiently dispersed that no individual victim finds it feasible to bring legal action against its source.[114]

The incentive and ability of someone who is victimized by the dissemination of harmful information may differ among types of harm. At one extreme, the harm to a single victim of defamatory content may be sufficiently large to warrant bringing legal action against its source. Of course, even in these cases, the incentive of victims to bring suit and their ability to obtain damages will depend, among other things, on whether the source of the content has resources that are sufficient to pay a judgment. As Posner notes, "[m]uch . . . market bypassing cannot be deterred by tort law that is, by privately enforced damage suits. The optimal damages that would be required for deterrence would so frequently exceed the offender's ability to pay that public enforcement and nonmonetary sanctions such as imprisonment are required."[115] This is likely to be the case for many, if not most, information sources.

At the opposite extreme are situations in which there are a very large number of victims but none of which experiences a large amount of harm. In these situations, examples of which might be the dissemination of false information or misleading advertising, no single victim is likely to find it practical to bring suit against a source.[116] Nonetheless, increasing interactive computer services'

---

[114] Of course, individual victims of defamation may, if the damage is large and the source has resources that are sufficient to pay a judgment, bring suit and some have done so. For many other types of harmful content, that alternative is unlikely to be feasible. For instances with numerous victims, class actions brought pursuant to Rule 23 of the Federal Rules of Civil Procedure might afford opportunities for redress and, concomitantly, for deterrence.

[115] Richard A. Posner, *An Economic Theory of Criminal Law*, 85 COLUM. L. REV. 1193, 1195 (1985) (By "market bypassing," Posner means engaging in behaviors that avoid "the system of voluntary, compensated exchange." Note that if an offender's resources are limited, it may not be practical to bring a legal action against him even where the dissemination of a particular piece of information harms only a single individual.).

[116] *See, e.g.*, Carnegie v. Household Int'l, Inc., 376 F.3d 656, 661 (7th Cir. 2004) (Posner, J.) ("[O]nly a lunatic or a fanatic sues for $30."). Of course, if the dissemination of a large amount of harmful content can be anticipated, some form of government intervention may be employed to prevent its dissemination in the future but that is not the same as preventing harm through private negotiations

exposure to liability is likely to reduce, at least somewhat, the amount of harmful information that is disseminated. If, as a general matter, the information providers have only limited assets, it may be more efficient for the services to be made liable instead of the providers, who would be judgment-proof, and thus unconcerned about their liability.[117] To the extent that there are economies of scale in detecting and removing harmful information—perhaps because algorithms can be employed to detect harmful information for which many content providers are the sources or, equally likely, many "users" are republishing content—interactive computer services that provide access to many content providers may be better able than the sources themselves to take actions that prevent the dissemination of harmful information.[118]

Although there may be reasons to make interactive computer services liable for the harmful effects of the dissemination of the content to which the services provide access, it is also possible to imagine situations in which victims could efficiently bring legal actions against content providers. Consider a content provider that offers information that can cause harm, hate speech for example, because the recipients of that information may engage in activities that impose costs on third parties. Assume, moreover, that the content is accessible through more than one interactive computer service, say via Twitter and Parler. Since third-party victims may not know the identity of the computer service through which the recipients of the information obtained access, suing any individual service may not be feasible and it may be impractical to sue all the

---

between potential victims and potential sources of harm. We discuss some possible forms of government action below.

[117] *See* Perry, *supra* note 33, at 764.

[118] *See* CERRE Report, *supra* note 14, at 6 ("[M]any private actors (providers of the material and online platforms) contribute to the problem . . . . [T]he liability regime of online hosting platforms is one part of a broader regulatory framework . . . ."); *id.* at 7 (noting that "when monitoring costs for the platforms are low, they may be best placed to remove illegal material and prevent harm"); *id.* at 47 (further observing that "absent liability of intermediaries, intermediaries may have suboptimal private incentives to prevent harm caused on others, and exert too little effort to detect and prevent it. In this case, imposing liability on the intermediary may induce the intermediary to terminate or mitigate the consequences of the illegal behavior of users.") (citation omitted).

services that provided access to that information.[119] In terms of the Coase example, it is as if a single cattle owner grazed his cattle on land owned by many different land owners. In that case, it could be more efficient to have the cattle owner rather than the numerous land owners be liable for damage caused by straying cattle and, if the cost of fencing is less than the crop damages that would otherwise result, for the cattle owner to pay the land owners to construct fences, or to do so itself. Moreover, knowledge about which information is potentially harmful may be more easily available to specialized information content providers than to general interactive computer services, for example, due to differing levels of cultural awareness, which also argues for the continuing liability exposure of information providers. Nonetheless, for the reasons already discussed, making interactive computer services liable for the dissemination of harmful information is likely to reduce the amount of such information that is distributed over the internet. Furthermore, even if the immunity given to interactive computer services by Section 230 were eliminated, victims could still bring legal actions against information providers if they could be identified.

It is also important to recognize that the resources available to detect and remove harmful information likely varies widely among interactive computer services. Whereas services like Facebook and YouTube spend large amounts on moderating content, including employing large numbers of humans in the process, smaller services are unlikely to be able to employ similar amounts of resources.[120]

---

[119] Consider, for example, the difficulty in tracking to its origin the false story leading to the notorious "Pizzagate" incident. *See* Emma Savino, *Fake News: No One Is Liable, and That Is a Problem*, 65 BUFF. L. REV. 1101, 1107–10 (2017). *See also* Marc Fisher et al., *Pizzagate: From Rumor, to Hashtag, to Gunfire in D.C.*, WASH. POST (Dec. 6, 2016), https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtagto-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html (describing an incident in which Edgar Welch entered a pizza restaurant in Washington, D.C. with an assault rifle, fired it into the air, and searched the restaurant because a fake news story reported the pizza place was harboring child sex slaves as part of a child-abuse ring led by Hillary Clinton).

[120] For that reason, Perault, *supra* note 16, at 4, observes that "increasing the costs of platform moderation might reduce the competitiveness of the tech sector . . . . Large platforms like Google, Facebook, and Twitter can afford to hire

Although there are independent entities that smaller services can employ to carry out the content moderation function,[121] to the extent that there are economies of scale in carrying out these activities, smaller interactive computer services are likely to be less effective at identifying and removing harmful materials than their larger rivals.[122]

---

tens of thousands of people to moderate content and to build tools (such as artificial-intelligence classifiers that make content moderation more efficient. Smaller companies often cannot. As a result, expanding liability for platforms will *likely* make the tech sector less competitive overall."

[121] SARAH T. ROBERTS, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOWS OF SOCIAL MEDIA 39–51 (2019). Paul M. Barrett also notes that "major social media companies . . . [outsource] the vast majority of [content moderation] to third-party vendors." Paul M. Barrett, NYU STERN CTR FOR BUS. AND HUM. RTS., *Who Moderates the Social Media Giants: A Call to End Outsourcing*, at 1 (June 5, 2020), https://issuu.com/nyusterncenterforbusinessandhumanri/docs (choose the first listed publication entitled "Who Moderates the Social Media Giants"). He also notes that "[t]oday, 15,000 workers, the overwhelming majority of them employed by third-party vendors, police Facebook's main platform and its Instagram subsidiary." *Id.* at 2. More broadly, a report cited by Cogito Tech estimated that the global content moderation market was more than US $5 billion at the end of 2020 and was expected to reach US $11.8 billion by the end of 2027. Roger Brown, *What are the Content Moderation Industry Trends and Moderation Policy?*, COGITO TECH (Nov. 25, 2020), https://cogitotech.medium.com/what-are-the-content-moderation-industry-trends-and-moderation-policy-691fe2b09e78. *See also* Tarleton Gillespie, *supra* note 19, at 198 ("Content moderation is such a complex and laborious undertaking, it is amazing that it works at all and as well as it does. Moderation is hard. This should be obvious, but it is easily forgotten. Policing a major platform turns out to be a resource intensive and relentless undertaking; it requires making difficult and often untenable distinctions between the acceptable and the unacceptable; it is wholly unclear what the standards for moderation should be, especially on a global scale; and one failure can incur enough public outrage to overshadow a million quiet successes.").

[122] Of course, removing content is not the only option that is available to an interactive computer service. Eric Goldman provides a useful taxonomy of the "remedies" that are open to a service together with examples of their use. Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. (forthcoming Feb. 2022). The categories that Goldman identifies, each of which contains a number of sub-categories, are Content Regulation, which includes removing content, Account Regulation, which includes suspending posting rights, Visibility Reductions, which includes downgrading internal search visibility, Monetary, which includes forfeiting account earnings, and Other, which includes educating

Moreover, as we have discussed above, the dissemination of harmful information may, in fact, increase the profits of both source and service providers if the compensable losses to the "victims" of that dissemination are smaller than the additional profits that accrue as a result.[123] That is, interactive computer services may well find it profitable to provide access to information that others would regard as harmful even if they are not legally immune and simply regard occasional liability for the resulting harm as a cost of doing business. Given the benefits that services receive from providing such information and the difficulties that those harmed by the content experience in bringing legal actions against its sources, it is likely that substantial amounts of harmful information will continue to be offered even if their Section 230 immunity were eliminated.[124] Thus, some form of direct regulation of content that is not constitutionally protected but offered by interactive computer services may be required.

---

users and assigning warnings. *Id.* An approach short of the removal involves supplying context to material. *The Economist* notes that "Twitter attached the label 'China state-affiliated media' to accounts run by official mouthpieces including CGTN, a global broadcaster; Xinhua, the main official news agency; and newspapers such as *People's Daily* and *China Daily*," and that "it would stop giving prominence to these accounts by displacing their tweets among 'top' results in searches." *Twitter May Have Reduced the Influence of China's Propaganda*, ECONOMIST (Jan. 21, 2021), https://www.economist.com/china/2021/01/21/twitter-may-have-reduced-the-influence-of-chinas-propaganda. The announcement of the Twitter policy appears as "New labels for government and state-affiliated accounts." Twitter Support (@TwitterSupport), *New Labels for Government and State-Affiliated Media Accounts*, TWITTER (Aug. 6, 2020), https://blog.twitter.com/en_us/topics/product/2020/new-labels-for-government-and-state-affiliated-media-accounts.

[123] In this regard, it is interesting to note that Cohen has argued that "the core platform business model . . . depends on the relative profitability of *im*moderation." Cohen, *supra* note 16, at 660 (emphasis added). The additional profits can take the form of both subscriber and advertiser revenues that result from the dissemination of harmful material that attracts additional users and savings in the form of reduced costs of content moderation.

[124] Note that, in these circumstances, the harm may continue even if victims receive compensation. However, the services presumably will be motivated to prevent or inhibit the dissemination of harmful content where potential liability is significant.

Finally, in adopting policies that are intended to limit the amount of harmful content that is disseminated over the internet, it is important to be mindful of the possibility that the policies will go "too far." As Genevieve Lakier has observed:

> One of the profound changes that the emergence of the platform public sphere has brought about is a significant democratization of the opportunity to engage in public expression. The result is to increase tremendously the range of speakers—and speech acts—that circulate publicly. This . . . energizes and empowers but it also makes possible all kinds of hateful, harassing, and demeaning speech . . . . [This] heightens the possibility—present whenever the government regulates speech—that laws intended to remove violent or harassing or derogatory speech from the internet will in fact be used to punish politically unpopular speakers, rather than the worst kinds of speech.[125]

Even apart from any political bias, in order to avoid potential liability, a risk averse platform operator may choose to remove content that it fears may be found, with some probability, to be harmful by a court of law. Of course, the possibility that making platforms liable may result in the removal of some content that is not actually harmful must be balanced against the likelihood that more harmful content will be disseminated if platforms are not liable.

SOME PROPOSALS FOR SECTION 230 REFORM

In response to the externality problem, there have been a number of proposals in the United States and Europe to increase platform responsibility for the harmful information that they disseminate, including mandating platform internal processes and increasing liability exposure. Although there may be circumstances in which

---

[125] Genevieve Lakier, *The Limits of Antimonopoly Law as a Solution to the Problems of the Platform Public Sphere*, KNIGHT FIRST AMEND. INST. (Mar. 30, 2020), https://knightcolumbia.org/content/the-limits-of-antimonopoly-as-a-solution-to-the-problems-of-the-platform-public-sphere.

that could lead to reductions in the amount of harmful material that is disseminated over the internet, for the reasons already discussed, such an approach is likely to be a highly imperfect solution to the problem.

It is also important to note that, despite deeply held shared values, United States and European jurisprudence diverge with respect to platform immunity issues for reasons that are fundamental—differences in civil and common law, differences in governing philosophies with respect to communal and individual responsibility—and also instantiated in the First Amendment.[126] As we note below, the European approach allows for more state action

---

[126] The Stigler Committee Report, *supra* note 42, at 191, makes a similar point:

> Jurisdictions outside the US have adopted versions of Section 230, but none provides as much protection. In Europe, platforms have borne more liability and responsibility for removing illegal content. Under the European E-Commerce Directive, for example, intermediaries are exempt from liability for content they host so long as they "play a neutral, merely technical and passive role towards the hosted content." Once they become aware that any hosted content is illegal, the intermediaries "need to remove it or disable access to it expeditiously." Germany enacted the NetzDG law in 2018, enabling courts to fine social media companies with more than 2 million euros up to €50 million if they do not delete posts contravening German hate speech law within 24 hours of receiving a complaint or seven days in more ambiguous cases. There are a number of EU and member state proposals to hold platforms responsible not only for illegal content but also for harmful content and to impose a "duty of care" for managing content in the public's interest.

(citations omitted). *See also* CERRE Report, *supra* note 14, at 21–31 (providing a useful summary of actions taken by the EU since the adoption of the e-commerce Directive. These actions include: (i) adopting rules that make it illegal for platforms to disseminate certain types of materials, including those involving child sexual abuse, terrorism, and hate speech and violence; (ii) providing guidance to platforms for the detection, removal, and prevention of illegal content; and (iii) promoting co- and self-regulation for the removal of some illegal material.); Gillespie, *supra* note 19, at 208 ("European legislators have slowly imposed something like a notice-and-takedown approach around hate speech and terrorist propaganda and have gradually decreased the required time within which platforms must respond.").

whereas the United States approach relies more on individual initiative to suppress negative externalities.[127] A manifestation of the differences is the European Digital Services Act proposal of 2020, which while maintaining platform immunity as the general rule would impose a series of process requirements on platforms that could, among other things, enhance understanding of harms and lead to substantive reforms—for example, expanding the categories of communications deemed illegal and thus subject to take down.[128] The proposal does not define illegal content, but rather enables it to arise as experience warrants from the European Union and national laws.[129] By contrast, the United States relies on established, less flexible judicial processes and consequently depends more on a priori congressional specifications of categories not qualifying for immunity.

Against this background, a wide variety of proposals for amending Section 230 have emerged in the United States, including some from members of Congress. Some commentators have proposed that an interactive computer service should be able to avoid liability if it can demonstrate that it has taken certain precautions to avoid the dissemination of harmful content.[130] For example, Citron and Wittes have argued that

> [i]f providers or users engage in good-faith efforts to address or restrict abusive material, they should be immune from liability even if they were negligent or reckless in doing so. By contrast, the immunity should not apply to platforms designed to host

---

[127] Coase, *supra* note 1, at 28–29 (responding to Pigou's approach to dealing with externalities, which was based almost exclusively on government intervention rather than private action; the various efforts by European countries to deal with externalities that arise from the dissemination of harmful information through state action can thus be thought of as arising from the Pigouvian rather than the Coasian tradition).

[128] EUROPEAN COMMISSION, DIGITAL SERVICES ACT EXPLANATORY MEMORANDUM 4 (Dec. 15, 2020), https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf.

[129] *Id.*

[130] *See, e.g.*, Johnson & Castro, *supra* note 56, at 19–20 (discussing "safe harbor" proposals that would limit the liability of interactive computer service acting in "good faith").

> illegality or sites that deliberately choose to host illegal content.[131]

Others propose more forceful approaches. Perault argues, for example, that "legislators should pass new federal criminal laws that prohibit some of the most harmful forms of online speech, such as voter suppression and incitement to riot."[132] Similarly, Johnson and Castro propose that "Congress . . . should expand federal criminal law to address forms of harmful online activity that are illegal at the state level . . . ."[133]

Proposals made by members of Congress to suppress negative externalities tend to follow Coase's prescription of reliance on individual effort to suppress externalities where possible and to accept government intervention only where it is believed individual initiative would be ineffective. The principal proposals fall into three main categories.

First, some proposals would expand the categories carved out from blanket immunity, thereby permitting victims to bring actions against the platforms conveying harmful content. A leading example is the SAFE TECH bill, which carves out additional categories of harmful material from platform immunity, including civil rights, antitrust, cyberstalking, international human rights, and wrongful death.[134] It eliminates platform immunity in connection with material the platform is paid to distribute or in which it otherwise has an economic interest. It also makes it easier for a plaintiff to secure a take down injunction in the case of material likely to create irreparable harm.

Second, some proposals would require increased transparency and commitment to abide by user-friendly procedures in the event of controversy. For example, the proposed PACT Act[135] takes a more Pigouvian approach, emphasizing platforms' transparency in their content moderation practices and requiring take down within four days of material found by a court to be illegal. It also confirms

---

[131] Citron & Wittes, *supra* note 44, at 417 (citation omitted).

[132] Perault, *supra* note 16, at 5.

[133] Johnson & Castro, *supra* note 56, at 2.

[134] SAFE TECH Act, S. 299, 117th Cong. (2021).

[135] Platform Accountability and Consumer Transparency Act, S. 797, 117th Cong. (2021).

the authority of federal agencies such as the Justice Department and FTC and of State Attorneys General to engage in civil enforcement of federal law.

Third, some proposals would condition immunity specifically on algorithmic reforms, focusing specifically on the amplification of material that results from the algorithms used by a digital service. An example is the Protecting Americans from Dangerous Algorithms Act, which would eliminate immunity for civil rights and international terrorism claims if a platform employs algorithms that amplify or recommend content related to the claims.[136]

OTHER APPROACHES TO THE DISSEMINATION OF HARMFUL CONTENT

The Digital Services Act, the European Union's extensive effort to contend with social media-related externalities, is built on several notable antecedents. The European Union's e-Commerce Directive of 2000, which it amends, like Section 230, does not require any content moderation effort by a platform.[137] Indeed, it provides for exemption from liability for the carriage of potentially harmful content so long as the platform is completely passive vis-à-vis third party content.[138]

Unlike U.S. citizens, European citizens who are adversely affected by the dissemination of harmful information do have the opportunity to seek the assistance of government agencies with regulatory power. Unlike many of the congressional proposals to amend Section 230, the European Union's Digital Service Act proposal is process focused.[139] It would increase the opportunities

---

[136] H.R. 2154, 117th Cong. (2021).

[137] 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), 2000 O.J. 178.

[138] *Id.*

[139] *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* (Dec. 15, 2020), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital-services.

for individuals to attempt to persuade the platforms or government agencies to investigate complaints and to impose resolutions.[140] The European Digital Services Act would not curtail platform immunity.[141] Instead, "[b]y setting out clear due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union and improve the protection of their fundamental rights."[142] In other words, it is a complement to existing judicial rights. Importantly, under the proposal:

> [T]he concept of "illegal content" should be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law.[143]

The proposal reflects the European Commission's and individual European nation's superior ability, compared to that of the United States, to declare harmful expression illegal and thus subject to take down as well as to require intermediaries to curtail harmful content without regard to its legality.[144] The Digital Service Act would increase platform obligations and government powers

---

[140] DIGITAL SERVICES ACT EXPLANATORY MEMORANDUM, *supra* note 128, at 53–55.

[141] *Digital Services Act, supra* note 139.

[142] DIGITAL SERVICES ACT EXPLANATORY MEMORANDUM, *supra* note 128, at 2.

[143] *Id.* at 20.

[144] *Digital Services Act, supra* note 139.

and continue the tradition of government intermediation between platform and citizen. The proposal generally conditions immunity on the adoption and adherence to detailed processes, both internal and external to the firm, that increase with the size of the platform.[145]

The Digital Services Act proposes additional requirements applicable to very large online platforms such as Google and Facebook in light of their importance "in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online."[146] According to the Act, the reach of these platforms poses "systemic risks" that could produce "disproportionately negative impact[s] in the Union."[147] For that reason, the Act proposes that "very large online platforms should . . . assess the systemic risks stemming from the functioning and use of their service, as well as by potential misuses by the recipients of the service" and "deploy the necessary means to diligently mitigate the systemic risks identified in the risk assessment."[148] While the "systemic risks" that the largest platforms would be required to mitigate extend to harmful but not illegal activities—for example, "potential misuses by the recipients"—the proposed regulation leaves the extent of harmful activity undefined,[149] something that would be extremely problematic in United States jurisprudence delimited by the First Amendment.

An intermediate approach that relies on transparency and removal of offensive material once it has been identified is contained in the Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act),[150] which was adopted in Germany in 2017. Section 2 of the Act imposes a number of

---

[145] *See id.*

[146] *Id.* at 31.

[147] *Id.*

[148] *Id.* at 31–32.

[149] *Id.*

[150] *See* Netzwerkdurchsetzungsgesetz [NetzDG] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), Oct. 1, 2017, BEARBEITUNGSSTAND [BGBL I] (Ger.), http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.) Many of the Network Enforcement Act's concepts have been adopted by the European Commission's Digital Services Act proposal.

reporting obligations on platforms, which include a "description of the mechanisms for submitting complaints about unlawful content and the criteria applied in deciding whether to delete or block unlawful content[;]" information regarding "organisation, personnel resources, specialist and linguistic expertise in the units responsible for processing complaints, as well as training and support of the persons responsible for processing complaints[;]" and the "number of complaints in the reporting period that resulted in the deletion or blocking of the content at issue."[151] Section 3 of the Act requires that the platform "removes or blocks access to content that is manifestly unlawful within 24 hours of receiving the complaint;" and "immediately notifies the person submitting the complaint and the user about any decision, while also providing them with reasons for its decision."[152] Significantly, the

> Act shall apply to telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public (social networks). Platforms offering journalistic or editorial content, the responsibility for which lies with the service provider itself, shall not constitute social networks within the meaning of this Act.[153]

In early 2021, the European Union adopted a regulation requiring platforms to take down terrorist content within one hour of notification from an appropriate authority of any Member state.[154] The regulation covers

> material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack . . . . [It] also include[s] material that

---

[151] *Id.* article 1 § 2(2).2, § 2(2).4, and § 2(2).7.

[152] *Id*. article 1 § 3(2).2 and § 3(2).5.

[153] *Id.* article 1 § 1(1).

[154] Council Regulation (EU) 2021/784 of 29 April 2021 (addressing the dissemination of terrorist content online).

> provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, as well as chemical, biological, radiological and nuclear (CBRN) substances, or on other specific methods or techniques, including the selection of targets, for the purpose of committing or contributing to the commission of terrorist offences.[155]

The Online Safety Bill[156] is the United Kingdom's effort to deal with the dissemination of harmful content over the internet. Significantly, the Bill does not create new private causes of action, so that, for example, under its terms, an individual cannot sue a provider for the dissemination of libelous or otherwise damaging content.[157] Instead, it establishes a sweeping regulatory program that obligates open mic and search services to identify risks of harm and take steps to mitigate them.[158] The Bill follows the publication of the Online Harms White Paper,[159] which "set out the intention to improve protections for users online through the introduction of a new duty of care on companies and an independent regulator responsible for overseeing this framework."[160] It would establish a new regulatory regime to address illegal *and* harmful—that is, not intrinsically illegal—content online, with the aim of preventing harm to individuals in the United Kingdom.[161] The Bill would impose duties of care in relation to illegal content—explicitly terrorism and child sexual exploitation and sexual abuse.[162] It also

---

[155] *Id.*

[156] Draft Online Safety Bill (May 12, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

[157] *Id.*

[158] Online Safety Bill 2021, c. 405, Explanatory Notes ¶ 4.

[159] Full Government Response to the Consultation 2020, c. 354, Online Harms White Paper 4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf.

[160] Online Safety Bill, *supra* note 158, at ¶ 7.

[161] *Id.*

[162] *See id.* at ¶ 397–496.

would extend duties of care in relationship to content entailing a material risk of significant adverse physical or psychological impact on a child or adult of ordinary sensibilities.[163] Thus, under the terms of the Bill, lawful but potentially harmful "activity can range from online bullying and abuse, to advocacy of self-harm, to spreading disinformation and misinformation. Whilst this behaviour may fall short of amounting to a criminal offence, it can have corrosive and damaging effects, creating toxic online environments and negatively impacting users' ability to express themselves online."[164] The Office of Communications ("OFCOM"), the United Kingdom's communications regulatory authority, is tasked with reducing this very vague standard to practice through the development of codes of practice applicable to user-generated content ("user-to-user services") and to providers of search engines which enable users to search multiple websites and databases ("search services")[165] and given broad authority to police these online services,[166] including the ability to enjoin activities and impose substantial fines.[167]

The draft Bill also includes platforms' duty to "protect[] users' right to freedom of expression within the law,"[168] a clear reflection of a fundamental value shared with the European Union and the United States. However, it and the Digital Services Act also reflect both the different Constitutional arrangements and the quite different Pigouvian and Coasian preferences that influence European and American policy designs that seek similar ends.

CONCLUSION

In a number of cases, plaintiffs have brought suit against entities that courts subsequently found were immune from liability for the dissemination of harmful information because they were interactive computer services under the provisions of Section 230.[169]

---

[163] *Id.*

[164] *Id.* at ¶ 5.

[165] *See id.* at ¶ 1, 26.

[166] Draft Online Safety Bill, *supra* note 156, at Part 4.

[167] *Id.*

[168] *Id.* at Part 2.

[169] *See* sources cited *supra* note 35.

Presumably, plaintiffs would have prevailed in at least some of these cases in the sense that they had suffered harm that, in the absence of immunity, would be actionable. Moreover, it is reasonable to believe that this experience has discouraged others from bringing similar actions. Therefore, it is reasonable to believe that eliminating the liability shield from interactive computer services for additional categories of harm would result in more actions being brought and at least some services adapting their content moderation practices in order to limit or eliminate their carriage of harmful content. However, as our analysis makes clear, such a change should not be regarded as a panacea. Even if interactive computer services are liable, in many instances the number of entities that are adversely affected by the carriage of a specific piece of harmful information is likely to be so large and the harmful effect on each is likely to be so small that no individual victim is likely to have the incentive to bring suit against the service. Finally, to the extent that interactive computer services find it profitable to disseminate information that others would regard as harmful, these services are likely to continue to provide that information even if they are exposed to full liability for the resulting harm to individuals. Together, these provide an impetus for seriously considering government enforcement against the dissemination of certain types of harmful information that are not protected by the First Amendment.