U.S. DEPARTMENT OF JUSTICE

Section 230 — Nurturing Innovation or Fostering Unaccountability?

WORKSHOP PARTICIPANT WRITTEN SUBMISSIONS

February 2020

Submission by Stewart Baker can be found here:

https://reason.com/wp-admin/post.php?post=8047354&action=edit

February 27, 2020

U.S. Attorney General William P. Barr
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Barr:

Internet Association (IA) welcomes the opportunity to engage with the Department of Justice (DOJ) on the importance of the Communications Decency Act, Section 230. IA was pleased to participate in the Department's workshop titled *"Section 230 - Nurturing Innovation or Fostering Unaccountability?"* on February 19, 2020. The event put a spotlight on specific issues that have become part of the Section 230 discussion, and demonstrated an urgent need for reliable and comprehensive data regarding how Section 230 functions. IA believes that it would be premature for DOJ to reach any conclusions on whether Section 230 should be amended, or how, in the absence of such data. IA has significant concerns that proposals to amend Section 230 will have the unintended result of hindering content moderation activities that IA member companies currently perform. In light of our strong shared interest in promoting safety, we believe that avoiding such a result should be a central consideration.

Background

IA represents over 40 of the world's leading internet companies. IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. IA believes the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure policymakers, and other stakeholders understand these benefits.

IA member companies respect criminal laws and work diligently to promote the safety of those who use their services. All IA member companies prohibit the use of their services for illegal purposes in a Terms of Service or other rules. In fact, IA members often moderate or remove objectionable content well beyond what the law requires. All of this activity is made possible through Section 230.

Alongside governments, civil society and other stakeholders, IA member companies continually work to stop bad actors online. Many companies proactively detect and then report instances of Child Sexual Abuse Material (CSAM) to the National Center for Missing and Exploited Children (NCMEC). IA supported the CyberTipline Modernization Act of 2018 to support coordination between NCMEC, the public, law enforcement, and the internet sector to

eradicate child exploitation online and offline. IA members created technology to identify over 6,000 victims and 2,000 sex traffickers in a single year, which reduced law enforcment's investigation time by 60 percent. Member companies work with the Drug Enforcement Administration, and promote the DEA National Prescription Drug Take Back Day. Member companies also partner with the Global Internet Forum to Counter Terrorism (GIFCT) to organize collaborations between companies to share information, content identifiers, and best practices for the removal of terrorist content. These are just a fraction of the steps that IA companies take to make the online and offline world a safer place.

Benefits of Section 230

Passed as part of the Communications Decency Act in 1996, Section 230 created two key legal principles. First, online platforms are not the speaker of user-generated content posted via their services whether it consists of blogs, social media posts, photos, professional or dating profiles, product and travel reviews, job openings, or apartments for rent. And second, that online services – whether they're newspapers with comment sections, employers, universities, neighbors who run list-serves in our communities, volunteers who run soccer leagues, bloggers, churches, labor unions, or anyone else that may offer a space for online communications – can moderate and delete harmful or illegal content posted on their platform. Most online platforms – and all of IA's members – have robust codes of conduct, and Section 230 allows the platforms to enforce them.

Returning to the world before Section 230 would mean courts would, in many cases, apply publisher and distributor liability regimes to online services. It was the application of these regimes that led to the results in *Cubby v. Compuserve* and *Stratton Oakmont v. Prodigy* that spurred Congress to pass Section 230. Based on case law, absent Section 230, platforms that do not make any attempt to moderate content would escape liability, while those that engage in good-faith moderation would have the same liability as if they wrote the illegal content. This could create a stark choice. On the one hand, online services could decline to moderate because of the strong *disincentives* associated with increased risk of liability. And on the other hand, online services could opt to reduce legal risk associated with moderation by highly curating content with the result of significantly limiting the number and diversity of voices represented. The flourishing middle ground we enjoy today would cease to exist.

This flourishing middle ground is what many would call the best of the internet. Section 230 enables internet users to post their own content and engage with the content of others, whether that's friends, family, co-workers, teachers or mentors, neighbors, government officials, potential employers or landlords, fellow gamers, or complete strangers from the other side of the globe with a shared experience or interest.

Misconceptions regarding Section 230

As noted at the outset, the DOJ event put a spotlight on specific criticisms of Section 230. Going forward, further assessment of the status quo and any future policy options would benefit from a careful study and analysis of the legislative text, cases, and other aspects and outcomes of Section 230.

Participants presented conflicting views of the plain language and operation of the law. The cases cited as emblematic of Section 230's flaws warrant further examination to understand why courts reached specific outcomes, for example whether they were due to Section 230 or unrelated defects in the claims presented. In terms of outcomes, it would be constructive and important to include additional information and context regarding provider efforts to moderate content before advancing to options to "incentivize" additional moderation (or to limit moderation in the case of conservative bias). IA believes that further data is needed to allow an informed evaluation of potential problems and solutions related to Section 230, including on the following critical points:

- **Liability in the absence of Section 230.** There is an urgent need to reach a better informed foundation for discussion on:
    - **The extent to which Section 230 is the sole basis on which courts have dismissed claims against Interactive Computer Services (ICSs).** For example, terrorism cases were pointed to as one example of where Section 230 frustrates recovery for victims,[1] but the Ninth Circuit opinion in *Fields v. Twitter* declined to address Section 230 and instead found that plaintiffs failed to state a claim under the Anti-Terrorism Act because of a lack of causation.[2] Similar terrorism cases have also been dismissed because of the failure to state a claim rather than, or in addition to, Section 230.[3] Despite efforts to connect conservative bias to Section 230, cases brought by plaintiffs' claiming they were improperly censored by an ICS are frequently dismissed based on First Amendment jurisprudence which would control in Section 230 absence.[4] Defamation cases

[1] *Attorney General William P. Barr Delivers Opening Remarks at the DOJ Workshop on Section 230: Nurturing Innovation or Fostering Unaccountability?*, available at: https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-opening-remarks-doj-workshop-section-230 (last accessed February 26, 2020)("For example, the Anti-Terrorism Act provides civil redress for victims of terrorist attacks on top of the criminal terrorism laws, yet judicial construction of Section 230 has severely diminished the reach of this civil tool.").
[2] *Fields v. Twitter*, 2018 WL 626800 (9th Cir. Jan. 31, 2018).
[3] *See, e.g., Crosby v. Twitter*, 2019 WL 1615291 (6th Cir. April 16, 2019); *Clayborn v. Twitter*, 2018 WL 6839754 (N.D. Cal. Dec. 31, 2018); *Cain v. Twitter*, 2018 WL 4657275 (N.D. Cal. Sept. 24, 2018).
[4] *See, e.g., Prager University v. Google LLC*, Case No. 18-15712 (9th Cir. February 26, 2020)(*see* note 3, p. 10, for citations to additional cases with similar holdings); *affirming* 2018 WL 1471939 (N.D. Cal., Mar. 26, 2018, No. 17-CV-06064-LHK).

against ICSs are also dismissed under state Anti-SLAPP statutes[5] or for simply not qualifying as "defamation."[6]

- **What are the liability regimes that would apply in the absence of Section 230 and to what extent would application of those regimes lead to different results than Section 230?** It appears that a starting point for discussions of Section 230 reform is frequently an assumption that, by repealing or limiting the availability of Section 230, ICSs will become liable under the existing legal regimes that would be applied in 230's absence. For example, the idea that repealing Section 230 will address "conservative bias" fails to recognize the First Amendment protections that apply to publishers and distributors.[7] The discussion of Section 230 would benefit from a better understanding of traditional rules of publisher liability and tort law and how courts would apply them to the online environment.[8]
- **What would the impact of eliminating Section 230 as a method of quickly ending frivolous litigation be on small and medium-sized businesses?** Litigation is expensive, even when it lacks merit.[9] Even when defendants are awarded attorney fees after successfully defending a case, recovering those fees is difficult.[10] IA member companies are concerned about the impact on innovation and new entrants to the market. Also concerning is DOJ's view that, "[n]o longer are tech companies the underdog upstarts; they have become titans of US industry."[11] IA represents more than 40 internet industry companies of which the vast majority of which are not "titans" by any measure. The technology industry still features a vibrant pipeline of startups that fuels continued innovation.

---

[5] *See, e.g., International Padi, Inc. v. Diverlink*, 2005 WL 1635347 (9th Cir. Jul. 13, 2005); *Sikhs for Justice v. Facebook*, 144 F. Supp. 3d 1088 (N.D.Cal. 2015)(*affirmed*); *Eade v. Investorshub.com*, 2:11-cv-01315 (C.D. Cal. July 12, 2011); *Heying v. Anschutz Entm't Group*, Case No. B276375. (CA. St. Ct. App 2017)(unpub).

[6] *See, e.g., Mosha v. Yandex*, 2019 WL 4805922 (S.D.N.Y. Sept. 30, 2019); *Darnaa v. Google*, 2017 WL 679404 (N.D. Cal. Feb. 21, 2017); *Hammer v. Amazon*, 392 F. Supp. 2d 423 (E.D.N.Y 2005).

[7] *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974).

[8] For example, at least one court declined to treat online intermediaries as "publishers" even without Section 230. *See, e.g., Lunney v. Prodigy*, 723 N.E.2d 539 (NY 1999).

[9] Engine Advocacy, *Primer: The Value of Section 230*, January 31, 2019 (available at: https://www.engine.is/news/primer/section230costs)(last accessed February 26, 2020)(noting that filing a single motion to dismiss can cost between $15,000-$80,000 and that the average startup begins with around $80,000 in funds). This estimate does not account for the reality that defendants may have to file multiple motions to dismiss in the same action as a result of plaintiffs amending complaints. *See, e.g., Colon v. Twitter*, Case No. 6:18-cv-00515 (M.D. Fla.)(Defendants' motion to dismiss the *third* amended complaint is pending before the court).

[10] *See, e.g., Eade v. Investorshub.com* (review of the docket shows that after winning a Motion to Strike under an Anti-SLAPP statute and being awarded $49,000 in attorneys fees in 2011, defendant is still trying to recover the fees from plaintiff, an attorney, in 2020).

[11] *Attorney General William P. Barr Delivers Opening Remarks at the DOJ Workshop on Section 230.*

- **Liability under Section 230.** Similarly, event participants expressed conflicting views about how Section 230 has been applied by courts and even what the text of the exceptions means. We recommend a thorough assessment be conducted to examine:
  - **What is the plain meaning of each exception to Section 230 and how do courts apply them?** For example, one participant in the afternoon session seemed to suggest that Section 230's exception for "intellectual property" was limited to "copyright," which neither tracks the plain language of the statute, nor the application of the exception by courts, which have applied it to matters ranging from trademark[12] to the right of publicity.[13] As discussed further below, similar confusion was evident regarding federal criminal law and state enforcement exceptions.
  - **What is the impact on criminal law enforcement?** Several participants suggested that criminal laws on a wide range of topics do not apply currently to the online environment. But Section 230 does not restrict the enforcement of federal criminal law. In fact, DOJ's news releases announce numerous successes against online services for activities such as advertising of CSAM,[14] operating criminal marketplaces,[15] cyberstalking,[16] and illegal selling of drugs.[17]
  - **What is the impact on state criminal law enforcement?** The inability of state Attorneys General to successfully prosecute Backpage has left an impression that Section 230 operates as a complete bar to state criminal law enforcement against an ICS. However, this is not consistent with the plain language of Section 230, which allows state criminal law enforcement where it is consistent with

---

[12] *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001).
[13] *Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009).
[14] https://www.justice.gov/opa/pr/dark-web-child-pornography-facilitator-pleads-guilty-conspiracy-advertise-child-pornography (last accessed February 22, 2020); *see also*, https://www.justice.gov/opa/pr/alleged-dark-web-child-pornography-facilitator-extradited-united-states-face-federal-charges
[15] https://www.justice.gov/opa/pr/russian-national-pleads-guilty-running-online-criminal-marketplace (last accessed February 22, 2020).
[16] https://www.justice.gov/opa/pr/florida-man-sentenced-prison-extensive-cyberstalking-and-threats-campaign (last accessed February 22, 2020); *see also*, https://www.justice.gov/opa/pr/new-york-man-sentenced-more-four-years-prison-engaging-extensive-four-year-cyberstalking; https://www.justice.gov/opa/pr/seattle-man-sentenced-over-two-years-prison-cyberstalking-campaign
[17] https://www.justice.gov/opa/pr/darknet-fentanyl-dealer-indicted-nationwide-undercover-operation-targeting-darknet-vendors (last accessed February 22, 2020). *See also*, https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales; https://www.justice.gov/opa/pr/three-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us

federal law.[18] In at least three of the lawsuits between Backpage and State Attorneys General (Cooper,[19] McKenna,[20] and Hoffman[21]), Backpage challenged state laws which were specifically enacted to target online intermediaries by significantly reducing *mens rea* requirements of existing aiding and abetting statutes. In each of these cases, the courts found the new criminal laws were barred by Section 230 because they assigned criminal liability to ICSs simply for display of third party content. Notably, those courts also held or noted First Amendment, Fourteenth Amendment, and Commerce Clause considerations would also prohibit such state laws. *Bollaert v. Gore* is an example of a state prosecution of an ICS where the defendant was successfully prosecuted.[22]

- **Are ICSs who contribute to the illegality of content protected by Section 230?** Many participants seemed to suggest that courts do not allow discovery into the facts necessary to determine whether ICSs play a role in the development of content at issue and that courts do not hold ICSs accountable when they do play such a role. A review of case law suggests otherwise. There are an ample number of cases where courts have required discovery before ruling on the applicability of Section 230,[23] as well as cases where courts refused to apply Section 230 because of the role of the ICS in content development.[24]
- **What does the "context" of Section 230 as part of the CDA mean for congressional intent and interpretation of the text?** Opening remarks noted that the Supreme Court's ruling finding CDA unconstitutional, "left in place an unbalanced statutory regime that preserves technology providers' liability protections, without guaranteeing corresponding protections for minors from harmful material on the Internet." A participant also advocated for a narrow interpretation of the protection for good faith removal of "otherwise objectionable" content[25] based, at least in part, on the overall intent of the CDA. Limiting application of Section 230(c)(2)(A) to indecency would have a

[18] *See* 47 U.S.C. § 230(e)(3)(stating "nothing in this section shall be construed to prevent any State from enforcing any state law that is consistent with this section.").
[19] *Backpage v. Cooper*, 939 F. Supp. 2d 805 (M.D. Tenn. 2013).
[20] *Backpage v. McKenna*, 2012 WL 3064543 (W.D. Wash. July 27, 2012).
[21] *Backpage v. Hoffman*, 2013 WL 4502097 (D.N.J. Aug. 20, 2013).
[22] *Kevin Bollaert v. Gore, 2018 WL 5785275 (S.D. Cal. Nov. 5, 2018)(denying writ of habeus corpus).*
[23] *See, e.g., Florida Abolitionist v. Backpage.com LLC*, 2018 WL 1587477 (M.D. Fla. March 31, 2018); *Pirozzi v. Apple*, 913 F. Supp. 2d 840 (N.D. Cal. 2012); *Cornelius v. Delca*, 709 F. Supp. 2d 1003 (D. Idaho 2010); *GW Equity, LLC v. Xcentric Ventures*, LLC, 2009 WL 62173 (N.D.Tex. Jan. 9, 2009); *Avery v. Idleaire Tech*, 2007 LEXIS 38924 (D. Tenn, 2007).
[24] *Fed. Trade Comm'n v. Leadclick Media, LLC*, 838 F.3d 158 (2d Cir. 2016); FTC v. Accusearch, 570 F.3d 1187, 1197 (10th Cir. 2009); Enigma Software Groupv. Bleeping Computer, 194 F.Supp.3d 263 (2016); *Alvi Armani Medical, Inc. v. Hennessey*, 629 F. Supp. 2d 1302 (S.D. Fla. 2008).
[25] 47 U.S.C. § 230(c)(2)(A).

significant adverse impact on consumers by disrupting existing case law protecting providers who rely on this provision in litigation by spammers.[26]

- **What constitutional limitations apply to the conduct of government actors (and agents of government actors) when it comes to direct or indirect efforts to influence private actors' decisions on content moderation?**
  - **Conservative Bias.** The limits on the government (either through DOJ or directly by Congress) to regulate which content an ICS can be required to display is better understood by reference to the First Amendment, rather than Section 230. Last session, all nine Justices on the Supreme Court emphasized that private platforms are not "subject to First Amendment constraints."[27]
  - **CSAM.** The Tenth Circuit's holding in *U.S. v. Ackerman*[28] that NCMEC is a government actor for purposes of the Fourth Amendment resulted in a wave of criminal defendants seeking to suppress evidence gathered voluntarily on the basis that ICSs are agents of the government. Courts have generally found that ICSs are not agents of the government when they implement voluntary screening for CSAM because they do so for reasons independent of law enforcement. A change to that incentive structure threatens to exercerbate and increase these claims and directly impact the ability of law enforcement to prosecute sexual predators identified through company voluntary efforts. These voluntary efforts by ICSs contribute overwhelmingly to reports of CSAM received by NCMEC which are in turn referred to law enforcement for prosecution.[29]
  - **Prior attempts to regulate online content**. Attempts to regulate content, even illegal content, have been repeatedly struck down by the Supreme Court and other U.S. courts,[30] unless they are well crafted to meet the requirements of the Constitution. This was the case with the other sections of the Communications Decency Act, except for the surviving Section 230.[31] It was also the case for the Child Online Protection Act,[32] and the Child Pornography Prevention Act of 1996.[33] Additionally, the Supreme Court has struck down laws restricting sex offenders from using social media.[34]

---

[26] *See, e.g., Smith v. Trusted Universal Standards in Electronic Communication*, 2011 U.S. Dist. LEXIS 26757 (D.N.J. March 15, 2011); *Holomaxx v. Yahoo!*, 2011 U.S. Dist. LEXIS 94314, (N.D. Cal. August 22, 2011); *Holomaxx v. Microsoft*, 2011 U.S. Dist. LEXIS 94316 (N.D. Cal. Aug. 23, 2011).
[27] *Manhattan Community Access Corp. v. Halleck*, 139 S. Ct. 1921 (2019).
[28] *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).
[29] Google, NCMEC & Thorn, *Rethinking the Detection of Child Sexual Abuse Imagery on the Internet*, p. 4 (available at: https://web.archive.org/web/20190928174029/https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf)(last accessed February 26, 2020).
[30] *See, e.g., Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004).
[31] *Reno v. ACLU*, 521 U.S. 844 (1997).
[32] *Ashcroft v. ACLU*, 535 U.S. 564 (2002).
[33] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).
[34] *Packingham v. North Carolina*, 137 S.Ct. 1730 (2017).

- **International implications.** Section 230 plays a critical role in protecting the ability online services to operate responsibly on a global basis. Foreign jurisdictions generally lack Good Samaritan protections for online services that moderate content. This creates exposure to liability in foreign courts for content that not only doesn't violate U.S. laws, but that is protected expression under the First Amendment. Section 230 provides important protections when international courts are willing to apply forum selection and choice law clauses from contracts and apply U.S. law. Also, under the SPEECH Act, U.S. courts are barred from enforcing foreign libel judgements when they are inconsistent with Section 230.[35] For this reason, Section 230 is a critical bulwark against foreign efforts to engage in censorship of content on U.S. platforms.

Conclusion

Stopping bad actors online can be accomplished without removing a fundamental pillar on which the modern internet was built. The actions that policy makers want online platforms to take against a wide range of inappropriate content are enabled by Section 230. IA's member companies agree on the importance of voluntarily undertaking content moderation activity to promote online and real world safety and in many instances they do – whether using hash values to identify child sexual abuse imagery, using algorithms to detect ISIS and other terrorist content, providing resources to users threatening suicide, or any of the thousands of other actions that happen daily to address harmful content. Section 230 is the law that allows that to happen.

Changes to Section 230 should be considered only after a thorough understanding of the necessity for and the practical and legal implications of such changes is established. It is critical to avoid any actions that could hinder existing industry efforts to maintain and enforce robust codes of conduct, particularly the existing system for the detection and reporting of CSAM, and to avoid establishing rules that could inadvertently support state agent claims that could shield defendant/abusers.

Thank you again for the opportunity to submit an outline of IA's views on this important topic, and IA looks forward to being a resource to the Department of Justice going forward.

Sincerely,

Elizabeth Banker
Deputy General Counsel

[35] 28 U.S.C. § 4102(c)(1). *See, e.g., Joude v. Wordpress*, 2014 WL 3107441 (N.D. Cal. July 3, 2014)(court declined to enforce a foreign defamation judgment under the SPEECH Act).

Adam Candeub
Michigan State University College of Law

Summary: Section 230 of the Communications Decency Act of 1996 grants legal privileges and immunities that non-internet intermediaries do not enjoy. Congress provided for this special treatment in order to aid the nascent internet industry. But, even though internet platforms have emerged as gatekeepers of the American economy and political discussion, they still enjoy section 230's subsidy intended to encourage a new technology. Indeed, court rulings have expanded section 230 in dramatic and indefensible ways, sometimes giving large internet platforms immunity from all suits related to their "editorial judgment," an unheard-of immunity unparalleled in the common law.

Reasonable reform would return section 230 to its plain meaning and original purpose: (i) common law distributor liability and (ii) immunity for editorial decisions related to obscenity and indecency, as those terms would have been understood in 1996 when Congress passed the CDA. This approach would limit platform liability for third-party content so as to encourage the free flow of ideas and give platforms absolute protection in their efforts to curb obscene, indecent, violent, or harassing material. At the same time, this approach treats internet platforms like any other firm for other legal purposes.

Distributor Liability Before Section 230

Section 230, 47 U.S.C. § 230, deals with a question that the common law has long addressed: the liability of so-called "distributors" or "intermediaries." These firms sell or provide access to—but do not write or create—written, electronic, or other types of media. The question is what legal liability distributors or intermediaries face when they distribute or provide access to libelous, fraudulent, or other unlawful material.

Prior to the internet, courts answered this question for intermediaries such as telephone companies, telegraphs, libraries, bookstores, classified ads, and public access television stations. And the answer was clear: *Distributors or intermediaries were immune from liability only if they lacked knowledge of the unlawful content. They did not enjoy absolute immunity.* The Restatement 2d of Torts states, "one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character."[1] The First Amendment did not give intermediaries and distributors immunity, and they faced liability for all material that they distributed—including materials over which they exercised limited editorial control. For instance, newspapers have liability for libelous or discriminatory classified ads.[2]

[1] Restatement 2d of Torts § 581 (1977); *id.* at cmt.e ("Bookshops and circulating or lending libraries come within the rule stated in this Section. The vendor or lender is not liable, if there are no facts or circumstances known to him which would suggest to him, as a reasonable man, that a particular book contains matter which upon inspection, he would recognize as defamatory. Thus, when the books of a reputable author or the publications of a reputable publishing house are offered for sale, rent or free circulation, he is not required to examine them to discover whether they contain anything of a defamatory character. If, however, a particular author or a particular publisher has frequently published notoriously sensational or scandalous books, a shop or library that offers to the public such literature may take the risk of becoming liable to anyone who may be defamed by them."_ *See also id.* at cmt. d (applying the same principle to newsstands).

[2] Braun v. Soldier of Fortune Magazine, Inc., 968 F. 2d 1110 (11th Cir. 1992)("publishers . . . have a duty to the public when they publish an advertisement if 'the ad in question contain[s] a clearly identifiable unreasonable risk, that the offer in the ad is one to commit a serious violent crime, including murder"); United States v. Hunter, 459 F. 2d 205

Intermediaries sometimes received greater immunity, but these cases were limited to situations where the platform had a common carriage or licensee obligation to carry the challenged content. An important example includes the immunity broadcasters enjoy when transmitting political advertisements or broadcasts that they are required to carry.[3]

Online Distributor Liability Before Section 230

As has been discussed countless times, two cases applied online distributor liability prior to section 230's passage in 1996. Both fairly applied existing distributor liability. In *Cubby, Inc. v. CompuServe Inc.,*[4] plaintiff challenged postings on an online bulletin board over which CompuServe exercised no editorial control. The court analogized a CompuServe chatroom to "an electronic, for profit library" and therefore determined it should have the same liability, i.e., distributor liability[5]. In short, *Cubby* applied traditional online distributor liability for online intermediaries, which was not complete immunity but rather distributor liability which included liability for knowingly carrying unlawful content.

In *Stratton Oakmont, Inc. v. Prodigy Servs. Co*.,[6] the plaintiff also complained about libelous bulletin board postings. However, in this case, Prodigy did *not* hold itself out as a distributor or intermediary. Rather it "held itself out to the public and its members as controlling the content of its computer bulletin boards. . . . [and] implemented this control through its automatic software screening program." The court, therefore, held that Prodigy was not an intermediary or distributor and faced liability for all user-generated posts and content.

The CDA Protects Children, and Section 230 was Designed to Overturn Prodigy so as to Encourage Sites to Become Family-Friendly

The *Prodigy* decision created a choice for online platforms: edit their chatrooms and other interactive fora and face liability for all content users post *or* refrain from editing and enjoy the more forgiving distributor liability. Congress, in passing the CDA had the "goal of protecting children from harmful materials,"[7] which meant primarily pornography. Section 230 was intended to protect internet platforms that created family friendly environments from liability, and thus section 230 had has its admitted goal the repeal of *Stratton-Oakmont*.

> One of the specific purposes of this section is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions that have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of

(4th Cir. 1972)(newspaper violated Fair Housing Act for publishing a "classified advertisement tendering for rent a furnished apartment in what was denominated a 'white home.'").

[3] Farmers Educ. and Co-op. Union of Am., N. Dakota Div. v. WDAY, Inc., 360 U.S. 525, 527 (1959)("Since the power of censorship of political broadcasts is prohibited, it must follow as a corollary that the mandate prohibiting censorship includes the privilege of immunity from liability for defamatory statements made by the speakers.").

[4] 776 F. Supp. 135 (S.D.N.Y.1991).

[5] Id. at 140 (S.D.N.Y).

[6] 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[7] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849, 117 S. Ct. 2329, 2334, 138 L. Ed. 2d 874 (1997)

> empowering parents to determine the content of communications their children receive through interactive computer services."[8]

To that end Section 230(c)(2) grants immunity to any internet platform for **"**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."[9] Most courts follow *ejusdem generis* in interpreting "otherwise objectionable," viewing the phrase in light of the previous list, which mostly derives from the Comstack Act, and the CDA's child-protection pornography goal.[10]

Section 230(c)(1) in turn 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."[11] Its plain meaning provides for standard distributor liability for platforms. In other words, as with *Cubby*, platforms that simply distribute or provide access are not fully liable for the content they make available.

Zeran, Hassell, and Beyond

Section 230, therefore, establishes distributor liability for internet platforms and immunity for platforms that edit or curate their content to further the family-friendly goals set forth in the CDA. This is already a considerable gift or immunity designed to help the nascent industry.[12] Oddly, courts expanded and strengthened this immunity even as internet platforms became economic giants.

In the highly influential *Zeran* case, the U.S. Court of Appeals for the Fourth Circuit interpreted Section 230(c)(1) as an absolute immunity for liability for third party content, interpreting "publisher or speaker" liability as excluding distributor liability. Notice this extreme position. In *Zeran,* the plaintiff allegedly was falsely accused of selling T-shirts mocking the Kansas City bombing on an AOL bulletin board. He contacted AOL begging them to take it down as he was receiving death threats. AOL refused.

Applying traditional common law distributor rules discussed above and consistent with the text, the court *could have* held AOL to distributor liability's knowledge standards, holding it harmless for third party posts unless it received notice of the unlawful or harmful content. The court's policy justification for *not*

---

[8] H. R. Conf. Rep. No. 104–230, 104th Cong., 2d Sess. 208 (1996) at 194, *available at* https://www.congress.gov/104/crpt/srpt230/CRPT-104srpt230.pdf#page=194

[9] 47 U.S.C.A. § 230(c)(2).

[10] Sherman v. Yahoo! Inc., 997 F.Supp.2d 1129, 1138 (S.D.Cal.2014)("The Court declines to broadly interpret `otherwise objectionable' material to include any or all information or content."); Nat'l Numismatic Certification, LLC v. eBay, Inc., 2008 U.S. Dist. LEXIS 109793 at *82 ("One may find an array of items objectionable; for instance, a sports fan may find the auction of a rival team's jersey objectionable. However, Congress provided guidance on the term "objectionable" by providing a list of seven examples and a statement of the policy behind section 230. Accordingly, the Court concludes content must, at a minimum, involve or be similar to pornography, graphic violence, obscenity, or harassment."); Goddard v. Google, Inc., 2008 U.S. Dist. LEXIS 101890, *23-24, 2008 WL 5245490; Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 883 (2015); Darnaa, LLC v. Google, Inc., No. 15-CV-03221-RMW, 2016 WL 6540452, at *8 (N.D. Cal. Nov. 2, 2016).

[11] 47 U.S.C.A. § 230.

[12] Samuel J. Morley, How Broad Is Web Publisher Immunity Under § 230 of the Communications Decency Act of 1996?, Florida Bar Journal (Feb. 2010) at 8 ("Passed in 1996, §230 was designed to protect Internet providers from liability for defamatory and other unlawful messages on their servers in an effort to nourish formation of the early Internet and open and robust information exchange.").

doing so: firms such as AOL would be crushed with the expense and trouble of monitoring[13] seems obviated and antiquated with the development of sophisticated AI-tracking. The platforms are as effective in tracking "bad speech"[14] as they are at detecting copyright infringement.[15]

The expansion of section 230 immunity particularly in California state courts continues. For instance, in the recently decided *Hassell v. Bird,*[16] the California Supreme Court ruled that under section 230 platforms have no duty to remove content that courts *had already* adjudged defamatory, libelous, and false. Similarly, mostly in the context of pro se suits, trial courts are ruling that section 230 provides complete immunity—under contract, consumer fraud, and even antidiscrimination laws, for any platform decision implicating its "editorial decisions."[17] In other words, the internet platforms are using section 230 to defends against claims predicated on <u>*their own*</u> promises, fraudulent statements, and even discriminatory behavior. Given the market power of these firms, such immunity threatens not only the marketplace, but the marketplace of ideas as well.

<u>Conclusion</u>

Current Section 230 caselaw has gone well beyond the statute's text and purpose. Originally designed to grant traditional distributor liability to platforms, along with a special immunity to edit obscene and indecent speech, the provision has morphed into a get-out-of-jail free card for internet platforms. Firms that already bestride the narrow world like the Colossus now use section 230 to escape contract, consumer fraud, and even antidiscrimination laws claims based on the platform's *own* conduct. This judicial expansion twists section 230(c)(1) protection beyond any recognizable form, converting distributor liability into absolute immunity. The implications for competition and free expression are significant. Other firms, which compete against the internet platforms, such as newspapers, do not enjoy section 230 protection. And, this immunity also allows the internet platforms to act as unchecked censors. A reasonable reform would take section 230 back to its original purpose and common law origins. Section 230(c)(1) should be interpreted consistently with common law distributor liability, focusing on protecting platforms from libel, fraud and other liability stemming from third-party's or user's "publisher" or "speaker" status. Section 230(c)(2) immunity should be read consistently with its text and purpose: protecting families from pornography and other harmful materials.

---

[13] Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) ("If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.").

[14] Stephen Shankland, Facebook: New AI tech spots hate speech faster, *available at* https://www.cnet.com/news/facebook-says-its-new-ai-tech-spots-hate-speech-faster/ (May 1, 2019).

[15] Chris Griffith, YouTube protects copyright with artificial intelligence, The Australian Business Review (Nov. 28, 2016).

[16] Hassell v. Bird, 5 Cal. 5th 522, 553, 420 P.3d 776, 797 (2018).

[17] Cross v. Facebook, Inc., 14 Cal. App. 5th 190, 207; 222 Cal. Rptr. 3d 250, 264 (Ct. App. 2017); Doe II v. MySpace Inc., 175 Cal.App.4th 561, 573, 96 Cal.Rptr.3d 148 (2009).

Submission by David Chavern

The News Media and Section 230

We want to thank the Department of Justice for holding this workshop on Section 230 of the Communications Decency Act. There is often more heat than light around this topic, but we believe that it is deeply important not only for journalism but also for our civic society as a whole

The News Media Alliance represents approximately 2,000 news organizations across the United States and Europe. These publishers are critical to the communities they serve, but many are struggling financially -- in large part because the online marketplace is dominated by a few platforms that control the digital advertising system and determine the reach and audience for news content.

News publishing is the only business mentioned in the First Amendment, and we have been at the forefront of fighting for freedom of speech since well before that amendment was written. Therefore, we approach this issue with seriousness and caution. Section 230 of the Communications Decency Act is an unusual legal protection. Fundamentally, it is a government subsidy that was originally intended to nurture a small and immature online environment. It has since become a huge market distortion that primarily benefits the most successful companies in our economy, to the detriment of other market actors.

However, rather than simply addressing whether Section 230 should be completely preserved or revoked, we believe that it's more important to think about the whole ecosystem for news content and how we can mitigate the negative incentives created by Section 230 and create new incentives that favor quality journalism.

Background

Content moderation is and has always been a complex and nuanced problem. But Section 230 is a not complex or nuanced solution. It is blunt instrument that provides special legal protections for a wide range of commercial behavior. It serves to *disfavor* responsible, high quality journalism (as opposed to cheap, inflammatory content) – and is sustained by obsolete ideas about how the internet economy functions.

First, we should dispense with the idea that accountability and responsibility are inconsistent with business growth. Broad government exemptions from liability certainly make building a business easier, but our history is replete with great companies that have grown and succeeded while also accepting full responsibility for

their products and commercial decisions. News publishers, by way of example, have been legally responsible for their content since at least the 1730s, when the *Crown v. Zenger* decision grappled with the appropriate standard for acceptable speech in newspapers. Yet the responsibility for published content did not hinder the tremendous growth of the news industry in the 19th and 20th centuries. When we were the so-called "information gatekeepers," we seemed to find a way to both make money and be accountable.

Second, we need to drop the idea that today's digital "intermediaries" are in any way passive or "dumb pipes." The days of individually typing "www" web addresses into a portal or browser are long over. The vast majority of digital audiences get to their news through one of the major online platforms – notably Google and Facebook -- and those platforms exercise extreme control over how and whether news is delivered and monetized.

Not only are they not passive, but Google's and Facebook's businesses are specifically valued for their capacity to make highly refined, individual content and advertising decisions. They affirmatively curate what news people see and how money is made from it. This algorithmic decision-making is amazing – but also self-interested. Each action represents a commercial choice for the company, and there is nothing wrong with asking them to be responsible for those choices.

In the end, Section 230 has created a deeply distorted variable liability marketplace for media, with one of the largest distortions being that publishers are not compensated for the additional liability they carry. One group of market actors gets the responsibility, and another gets the decision-making authority and most of the money. This separation of accountability from financial return is not only bad for news publishing but for the health of our society. We need to find a better balance.

Section 230 Assumptions

Section 230 is premised on two broad assumptions: 1) that the Good Samaritan provisions encourage good behavior by protecting online platforms when they moderate some limited types of offensive and illegal content; and 2) when someone is harmed by the content published on these platforms, the damaged party can seek remedies from the creators of the content.

Both assumptions have been rendered obsolete by the evolution of technology. First, the online platforms now use Section 230's protections not simply to police for harmful content (as determined solely by them) -- but also to protect their ability to exercise extreme editorial control through algorithms and determine whether and how

content is exposed. This editorial control is similar to the control exercised by publishers and editors over content created by journalists. But unlike news publishers, the platform companies are absolved of all responsibility for their decisions, and therefore have insufficient incentive to promote quality over virality.

Second, Section 230 absolves companies of any accountability for their commercial decisions around promotion and reach. One person may slander another from a street corner with little impact. But an online platform can decide, for its own commercial purposes, to amplify and promote that same speech to hundreds of millions of others in order to increase traffic and, ultimately, profits. That decision about reach is separate from the underlying speech and should carry its own accountability and consequences.

Finally, any online platform that allows for anonymous or pseudonymous speech is intentionally preventing the accountability assumed by Section 230. You can't "sue the speaker" when the system is designed to allow the speaker to hide. These companies may feel that there are commercial and other benefits to the anonymity of their users but, again, that is their commercial choice for which they should then hold responsibility.

It is also absurd and reductive to argue that the platforms have the right to make tremendous amounts of money by using algorithms to manage billions of interactions -- but they then can't be expected to have any responsibility for those same interactions because of the scale of the effort. If you build it and sell it then you also have responsibility for the impacts and outcomes from it. It's not up to the rest of us to clean-up the mess.

Absent any accountability by the online platforms, the effect of Section 230 is to create a huge embedded bias favoring false and inflammatory content over quality news and information. We know that made-up garbage will always be cheaper to produce than professional journalism. If the online platforms are free to value each kind of content the same way, then there simply won't be journalism in many communities.

What to do about Section 230

There are some problems in the online ecosystem that revocation of Section 230 would not necessarily solve. First, not all bad information is legally actionable. We have extensive caselaw, going back hundreds of years, on what kinds of speech gives rise to causes of action (defamation, certain threats, etc.). But that doesn't necessarily cover a whole range of speech that we may consider extremely bad (many kinds of

hostile speech, anti-vaccine messages, etc.) Getting rid of Section 230 won't automatically stop the amplification of speech that is deeply dangerous and offensive.

In a related matter, brand and customer expectations have a huge impact on the kind of information that is delivered. For our part, news publishers believe that the value of their brands is centered in *trust* with readers, and that delivering false or dangerous information would damage that trust. Google and Facebook, on the other hand, are the means by which many people receive horrible and dangerous information. Yet these companies obviously don't believe it hurts their brands or there would be more proactive filtering and monitoring. Revocation of Section 230 alone would not necessarily make these companies more sensitive to the well-being of their users or the broader society.

But the safe harbor embedded in Section 230 is clearly part of the problem and we would suggest three approaches as it is revised:

- We shouldn't be afraid to be incremental. The government has allowed one of the largest parts of our economy to be built around a huge subsidy, and it doesn't have to change that all at once.

- As part of that approach, we should start by focusing on just the very largest companies and limit the exemption for those who both derive the most benefits from Section 230 and have the greatest capacities to take legal responsibility for their commercial decisions around content and reach. With great scale comes great responsibility.

- Finally, we don't need to start from scratch when it comes to defining impermissible speech. Let's start with the existing (and long-standing) standards around defamation and other harmful speech. We then need to continue to work on other business incentives for the online platforms to ultimately value quality content.

In order to further rebalance the relationship between the major platforms and news publishers, we also support the *Journalism Competition & Preservation Act*. This bill would allow news publishers to collectively negotiate with the platforms and return value back to professional journalism. If done right, this could also drive business incentives for the platforms to value quality journalism over overtly bad sources of information about our world and our communities.

Statement of Neil Chilson
U.S. Department of Justice Workshop
"Section 230 – Nurturing Innovation or Fostering Unaccountability?"
Wednesday, February 19, 2020[1]

Thank you to Attorney General William Barr and to the Department of Justice for inviting me to participate in this discussion. I am the senior research fellow for technology and innovation at Stand Together, part of a community of social entrepreneurs, academics, think tanks, community organizers, and policy advocates working to break barriers so that every individual can reach their unique potential. Other organizations in this community include Americans For Prosperity, the Charles Koch Institute, and the Charles Koch Foundation.

At Stand Together, we believe that market-tested innovation has been the primary driver of widespread human prosperity. But innovation doesn't just happen. It requires a culture that embraces innovation rather than fearing it and a regulatory environment that enables innovation.

Section 230 of the Communications Decency Act is a crucial part of the U.S.'s regulatory environment. The principles of individual responsibility embodied in Section 230 freed U.S. entrepreneurs to become the world's best at developing innovative user-to-user platforms. Some people, including people in industries disrupted by this innovation, are now calling to change Section 230. But there is little evidence that changing Section 230 would improve competition or innovation to the benefit of consumers. And there are good reasons to believe that increasing liability would hinder future competition and innovation and could ultimately harm consumers on balance. Thus, any proposed changes to Section 230 must be evaluated against seven important principles to ensure that the U.S. maintains a regulatory environment best suited to generate widespread human prosperity.

I. Section 230 Emphasizes Individual Responsibility

Section 230 embodies a clear and conservative principle of individual responsibility. In the simplest terms, it says that individuals are responsible for their actions online, not the tools they use. This is the normal way that we do things in the U.S. We hold newspapers, not newsstands, liable for news articles. Authors, not bookstores, accountable for book contents. So too do we hold social media users, not services, responsible for users' words online.

Section 230's principle of individual responsibility aligns with our general moral intuitions that individuals ought to be responsible for acts they commit and not for those that others commit. Likewise, harmed parties are owed redress from the person that harmed them, not from others. From a law and economics perspective, this approach sets the proper incentives by imposing the legal penalty for a wrongful act on the party that committed the act.

Counter to that intuition, intermediary liability means holding responsible someone other than the bad actor. Intermediary liability in effect deputizes one party to police others' behavior – and holds the deputy responsible for any violations the policed parties commit. Though counter to

[1] This statement has been revised and was resubmitted February 27, 2020 per Department of Justice staff request.

our moral intuitions, this approach may make economic sense in certain circumstances. But it always has side effects, including on markets and competitive dynamics. Below, I discuss these effects in the context of a new kind of intermediary: internet platforms that connect users to other users.

Section 230 is a limited protection from liability: it does not immunize platforms from liability for their own content or from violations of federal criminal law, violations of intellectual property, or crimes involving sexual exploitation of children, among other carve outs.

II. Section 230 Enables a New Kind of Intermediary

There have always been intermediaries that connected people so that they could talk, trade, or otherwise interact, but over the last twenty years the internet has facilitated an entirely new type of intermediary: the user-to-user platform.[2] On these platforms users generate content for other users to read and view. Users share their content with each other through a software-powered, largely automated process. Such platforms provide individuals with technical tools that make it inexpensive and productive to interact directly with thousands or even millions of other people.

User-generated content (UGC) platforms are extremely powerful. They eliminate middlemen, increasing direct user access to information and reducing transaction costs. By doing so, these platforms enable beneficial interactions that otherwise never would have occurred. In fact, the rise of such user-to-user platforms has transformed nearly every area where people interact: commerce, through services such as Etsy, Thumbtack, and third-party selling on Amazon and Walmart.com; housing through Airbnb and HomeAway; transportation through Uber, Lyft, and Turo; communications on Pinterest, Twitter, YouTube, and Facebook; and even philanthropy through GoFundMe, CaringBridge, and Indiegogo. These are just a few of the hundreds of internet platforms where people go to connect with other people and accomplish something together.

Some companies (like Facebook and YouTube) that operate user-to-user platforms are very large and generate significant advertising revenue. But the primary benefit to users even on these platforms is their connections to each other, usually in a non-commercial interaction that, absent these platforms, would not happen at all. It is important to consider these less tangible benefits when considering competitive impacts.

A personal story might serve as a good example. My wife and I have a 7-month-old daughter. While still in utero, she was diagnosed with a club foot, a birth defect that thanks to the miracles of modern science is entirely correctable. But correcting the problems requires a challenging process that spans many months. As new parents we had many questions, concerns, and worries. Our doctors were great but not always available. You know who was always available? The five thousand plus people in the Facebook Clubbed Foot support group. At any time, day or night, we could hear from people we had never met but who understood what we were going through. And

[2] User-to-user platforms are not the only types of intermediaries protected by Section 230 (see Section VI below), but they are the focus of much of the controversy and therefore the focus of my discussion.

now that we're through the hardest part of this process we can help other parents who need support. I cannot put a dollar value on this experience. It is not the kind of thing you could build a business plan around. But it exists because Section 230 means Facebook's lawyers don't have to review and verify every post to that group.

This is one example of the millions of ways user-to-user platforms benefit real people. No surprise, then, that I think the biggest total harm from changing Section 230 will not fall on platform companies or startups. It will fall on users. Platforms deputized to police their users will face little or no penalties for taking down a post or an entire discussion group but could face expensive lawsuits for leaving something up. The obvious incentive will be to over-remove content. People who use platforms in unanticipated, non-commercial, hard to measure, and easy to ignore ways – like the Clubbed Foot support group – will find platforms a little less welcoming to their uses. Given the huge volume of user interactions on these platforms, even tiny increases in costs to interactions would have enormous negative total cost to users.

Of course, this powerful new way of connecting people has disrupted many old ways of connecting. Companies that professionally generate entertainment or news content now compete with millions of amateur videographers, photographers, and essayists for the attention of the public. This has dramatically affected advertising-supported business models, in part because UGC platforms eroded the regional near-monopolies that newspapers had on distribution of certain kinds of information.[3] Today, middlemen and matchmakers of all kinds are competing against massive online marketplaces that bring together orders of magnitudes more sellers and buyers. Old business models face significant challenges in this new environment. No surprise then that some disrupted competitors are interested in modifying a law that has been central to the rise of these new intermediaries.

III. Imposing Intermediary Liability on UGC Platforms Would Harm Competition and Innovation

So how might we expect changes to Section 230 to affect competition and innovation? All proposed changes to Section 230 seek or threaten to increase the number of actions for which an intermediary would be liable. Increasing intermediary liability would affect competition and innovation in the following ways:

Increasing intermediary liability will raise costs. These higher costs would take two forms. First, companies will have to increase their "policing" of users to reduce litigation risk. For example, even under Section 230 today, Facebook pays tens of thousands of content moderators worldwide.[4] Increasing liability would require many other platforms to engage in expensive moderation. Second, imposing liability will necessarily raise companies' legal bills. Without

[3] *See* Marc Andreessen, *The Future of the News Business* (Feb. 25, 2014), https://a16z.com/2014/02/25/future-of-news-business/.

[4] NPR.org, *Propaganda, Hate Speech, Violence: The Working Lives Of Facebook's Content Moderators* (Mar. 2, 2019), https://www.npr.org/2019/03/02/699663284/the-working-lives-of-facebooks-content-moderators.

Section 230, even meritless lawsuits would become much more expensive to defend – potentially tens of thousands of dollars more expensive.[5] Indeed, Section 230 currently protects small intermediaries "from having to defend against excessive, often-meritless suits—what one court called 'death by ten thousand duck-bites.'."[6]

Increased costs will benefit old gatekeepers and suppress new competitors. Increased costs could affect market structure in two ways. First, if UGC platforms compete against other, non-intermediary companies, increased costs will favor those non-intermediaries. For example, consider the market for advertising. Platforms like Instagram attract users by offering them the ability to view content posted by other users, and then sell advertisements that users see while on the platform. Increasing liability would raise the cost to obtain user-generated content and affect the platform's ability to gain and maintain users, weakening UGC platforms' ability to compete for advertising dollars. Thus, lobbying for changes to Section 230 could serve as a way for business-to-user companies to raise their existing rivals' costs.

Second, and related, increased costs raise barriers to entry into the UGC platform marketplace. New UGC platforms would bear litigation risk from the very first piece of shared user content they hosted. The costs of mitigating such risks would be priced into investment decisions and on the margin would discourage entry into the user-to-user space. As a result, even moderate increases in intermediary liability would tend to concentrate the intermediary market. Absent Section 230, we believe "compliance, implementation, and litigation costs could strangle smaller companies even before they emerge."[7] Higher costs would favor established, sophisticated and profitable UGC platforms over small or new UGC platforms. Established firms can afford to mitigate litigation risk through expensive content moderation and takedowns at scale and can bear the cost of litigation that emerges. Thus "[a]ny amendment to Section 230 that is calibrated to what might be possible for the Internet giants will necessarily *mis*-calibrate the law for smaller services."[8] In short, recalibrating liability to what the biggest platforms can manage could eliminate a wide swath of smaller competitors.[9]

Indeed, even with Section 230 currently limiting the litigation risks of content moderation, the costs of effective content moderation are high enough that many companies, including news

---

[5] Engine, *Section 230 Cost Report*, https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c6c5649e2c483b67d518293/1550603849958/Section+230+cost+study.pdf.

[6] Liability for User-Generated Content Online: Principles for Lawmakers at 2 (July 11, 2019), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical (hereafter "Liability Principles").

[7] Liability Principles at 2.

[8] *Id.*

[9] Eric Goldman, *Want to Kill Facebook and Google? Preserving Section 230 is Your Best Hope* (June 19, 2020) ("In a counterfactual world without Section 230's financial subsidy to online republishers and the competition enabled by that subsidy, the Internet giants would have even more secure marketplace dominance, increased leverage to charge supra-competitive rates, and less incentive to keep innovating."), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398631&download=yes.

companies, avoid doing it. For example, NPR, Reuters, and many others reputable news organizations removed their reader comment sections years ago specifically because they cannot find ways to moderate cost-effectively.[10] Many instead now outsource the public discussion of their content to social media platforms and rely on those platforms to moderate public discussions at scale.[11] Imposing intermediary liability would increase any businesses' in-house content moderation costs and could accelerate the rush of companies outsourcing their user-to-user interactions to the biggest social media companies.

Increasing liability would hinder or eliminate user-to-user interactions. As mentioned above, the primary consumer benefit from user-to-user platforms are the interactions between users. Increasing the scope of user behavior for which platforms could be held liable will decrease the quality and quantity of user interactions on platforms. Such changes would re-insert a middleman into the user interactions, increasing transactions costs such as improper takedowns or bans or delayed posting. Given the sheer number of participants on many platforms, even a small per-interaction increase in costs could swamp any proposed benefits of Section 230 reform.

Furthermore, platforms' incentives as a middleman would conflict with its users' desires. Platforms will seek to avoid penalties and will play it safe when it comes to taking down user content. This risk averseness threatens user speech, as I discuss further below.

IV. Imposing Intermediary Liability Would Likely Reduce Investment into New UGC Platforms

All else being equal, one would expect that increased liability for user content would reduce investment into new user-to-user platforms.[12] The Copia Institute and NetChoice offered empirical evidence from international comparisons to support this expectation. Their recent report examines the effect of Section 230 on investment as compared to other liability approaches around the world.[13] The report concludes that "the broad immunity offered by Section 230 … likely resulted in somewhere between two to three times greater total investment in internet platforms in the US as compared to the more limited protections offered in the EU,"

[10] Elisabeth Jensen, *NPR Website To Get Rid Of Comments* (Aug. 17, 2016), https://www.npr.org/sections/publiceditor/2016/08/17/489516952/npr-website-to-get-rid-of-comments; Justin Ellis, *What happened after 7 news sites got rid of reader comments* (Sept. 16, 2015), https://www.niemanlab.org/2015/09/what-happened-after-7-news-sites-got-rid-of-reader-comments/.

[11] Ellis, *supra* n.9 ("We believe that social media is the new arena for commenting, replacing the old onsite approach that dates back many years.") (quoting Kara Swisher and Walter Mossberg on their decision to drop comments from Recode content.).

[12] It is also possible that heightened barriers to entry could increase investment into the largest incumbent UGC platforms in anticipation of a secured market position they could use to raise prices.

[13] Copia Institute, *Don't Shoot the Message Board*, 1,4 (June 2019), http://netchoice.org/wp-content/uploads/Dont-Shoot-the-Message-Board-Clean-Copia.pdf.

and "[e]ven in situations where there are some intermediary liability standards, the stronger those protections are for the intermediaries, the more investment and economic growth we see."[14]

V. Imposing Intermediary Liability Would Limit Free Expression

Deputizing platforms by making them liable for what their users say would incentivize over-enforcement, reducing users' effective speech. Platforms would face little or no penalty for removing content that does not violate any law, and significant penalties for leaving something up that should be removed. In that situation, platforms will have the incentive to "err on the side of caution and take it down, particularly for controversial or unpopular material."[15] Yet that is precisely the kind of speech that benefits from user-to-user platforms: content that isn't broadly appealing enough to convince a newspaper editor or a radio jockey to pass it along. Indeed, liability changes for platforms will harm the voiceless far more than those who already have large voices in the marketplace of ideas. As free speech litigator and journalist David French has argued,

> "Celebrities have their own websites. They're sought after for speeches, interviews, and op-eds. Politicians have campaigns and ad budgets, and they also have abundant opportunities to speak online and in the real world. If they succeeded in making social media companies liable for users' speech, they would pay no meaningful price. You would, however. Your ability to say what you believe, to directly participate in the debates and arguments that matter most to you would change, dramatically."[16]

If we change Section 230, the famous and the powerful will continue to connect with others through traditional means and gatekeepers that have long favored them. The average, niche, unpopular, disadvantaged, and unusual will find it harder to connect with an audience that platforms today make easy to find.

VI. Any Steps Forward Should Follow Seven Principles

If Congress determines that it ought to adjust Section 230, there are seven key principles it should follow. We at Stand Together, along with an ideologically diverse group of fifty-three academics and twenty-seven other civil society organizations, recommend Congress use these principles for evaluating any changes to Section 230:[17]

---

[14] *Id.,* 1, 4.

[15] Daphne Keller, *Toward a Clearer Conversation About Platform Liability* (Apr. 6, 2018) ("Empirical evidence from notice-and-takedown regimes tells us that wrongful legal accusations are common, and that platforms often simply comply with them."), https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability.

[16] David French, *The Growing Threat to Free Speech Online* (Jan. 24, 2020), TIME, https://time.com/5770755/threat-free-speech-online/.

[17] *See* Liability Principles, *supra n.*5.

Principle #1: Content creators bear primary responsibility for their speech and actions.
Principle #2: Any new intermediary liability law must not target constitutionally protected speech.
Principle #3: The law shouldn't discourage Internet services from moderating content.
Principle #4: Section 230 does not, and should not, require "neutrality."
Principle #5: We need a uniform national legal standard.
Principle #6: We must continue to promote innovation on the Internet.
Principle #7: Section 230 should apply equally across a broad spectrum of online services.

Stand Together fully supports all these principles, but I want to quickly highlight one. Principle #7 discusses the wide range of online intermediaries protected by Section 230. In these comments I've focused on user-to-user services like social media platforms. However, many other internet intermediaries – including internet service providers such as AT&T or Comcast, email marketing services such as MailChimp or Constant Contact, customer relationship management databases such as Salesforce, any of the tens of thousands of webhosts, or domain name registrars such as GoDaddy – do not directly interact with end users. They have only blunt instruments – such as site-wide takedowns – to deal with content problems. Imposing liability on such parties would "risk[] significant collateral damage to inoffensive or harmless content." Thus, Principle #7 recommends that Section 230 protections remain broad enough to protect the actions of companies that do not have direct user interactions.

VII. Conclusion

Thank you again for the opportunity to comment on these important topics. Section 230's principle of individual responsibility has enabled everyday individuals to build powerful and meaningful connections. Section 230 is a vital part of American technology policy and we believe it remains essential to the continued dynamic development of user-to-user internet platforms and the many benefits they bring to Americans. Changing it risks shutting down the voice of the everyday person and solidifying the position of already powerful speakers and gatekeepers.

Statement of Pam Dixon,
Executive Director, World Privacy Forum

U.S. Department of Justice Workshop,
"Section 230 — Nurturing Innovation or Fostering Unaccountability?"

Wednesday February 19, 2020

Thank you for your invitation to speak today about potential solutions to issues relating to Section 230 of the Communications Decency Act. I approach this topic from the perspective of a privacy expert, and as a researcher. In my privacy work at the World Privacy Forum,[1] I focus on systems of data and how those systems affect individuals and groups. My comments on Section 230 are animated by this focus.

I am generally concerned by the lack of systems thinking in the approaches to Section 230 debates, and a surprising lack of comprehensive data patterns to support conclusions. Therefore, my comments today focus on solving the most serious of the fundamental gaps I see in these key areas as a core part of the solution. I recognize that talking about systems thinking and data is not a traditional approach to discussing Section 230. Nevertheless, advancements in these areas are necessary to improve outcomes.

Introduction

Section 230 has been a topic of intense debate since its enactment in 1996.[2] A profound political impasse has developed among competing factions of the debate, each with a different position and approach to the problem. Despite high levels of ongoing public engagement, there has been little progress in resolving the stalemate, which has stalled progress toward resolving the unwieldy tangle of issues relating to Section 230, including issues relating to privacy. The increasing visibility of risks and harms to people within systems of knowledge and data that are regulated by Section 230 has acted, in part, to trigger a new round of discussions regarding how to solve problems.

Despite the intensity and breadth of the current debate, there are key gaps in the discussion.

---

[1] World Privacy Forum, See: https://www.worldprivacyforum.org.

[2] 47 U.S.C. §230.

- First, there has not been a rigorous and comprehensive multi-systems test for privacy that is consistently applied regarding proposed changes to Section 230. This is long overdue and needs to be included in any analysis prior to changes being made.

- Second, observable and verifiable risks and harms in Section 230 environments have not been handled consistently, and in some cases, have not been addressed in a systematic, neutral way. In some cases, risks and harms have not yet been adequately analyzed or addressed. To address this problem it is essential that systems thinking is applied to Section 230 problems. Systems thinking would **recognize interconnections**, **identify and understand feedback**, **understand the system structure**, **differentiate types of data flows and variables, identify non-linear flows, relationships, and components, understand the differing scales of systems, understand dynamic behaviors, and work to reduce complexity**.[3] Systems thinking would allow Section 230 debate participants to appropriately and more precisely define the full scope of Section 230 issues, map the interconnectedness of the problems, and document the dynamic complexities with data that supports the definitions, problems, and solutions.

- Third, statistics and fact patterns around Section 230 are generally lacking; it is an under-researched area. While there is plentiful legal scholarship and discussions, few studies provide national, comprehensive statistics on multiple aspects of the problems, mitigations or actions taken, interconnected data flows, how proposed solutions might impact multiple ecosystems, and so forth. Policies need to be informed by the fact patterns that are documented across the relevant ecosystems. There is a significant gap and opportunity here. It is my experience in privacy that factual documentation of problems in a systems thinking manner is essential to understand the full extent of the problems, define the problem, and to understand how best to mitigate the problems and provide meaningful solutions. If systems thinking is ignored, then the debate becomes about which narrative wins. It is crucial that

---

[3] Barry Richmond coined the term "systems thinking" in 1987. Many iterations of definitions of "systems thinking" have been considered since then. In 2015, Arnold and Wade wrote a synthesis definition based on the literature, and this is the definition referred to in these comments. (Ross D. Arnold, Jon P. Wade, *A definition of systems thinking: A systems approach*. Stevens Institute, 2015. Available online at ScienceDirect.com. The work of Sweeney and Sterman is also important in the Section 230 context. Their work has a focus on the interaction of system agents over time, which may be broadly thought of as dynamic complexity. This is an important component in properly analyzing systems where there Section 230 risks and harms emerging. Without systems thinking, single data point analysis can lead to flawed and inaccurate understanding of the underlying problems that need to be addressed. See: J. Sterman, *Sustaining Sustainability: Creating a Systems Science in a Fragmented Academy and Polarized World.* In M. Weinstein and R.E. Turner (eds), Sustainability Science: The Emerging Paradigm and the Urban Environment. 2012. Springer. 21-58. Available at: https://jsterman.scripts.mit.edu/Online_Publications.html#2011sustaining. See also: L. Booth Sweeney and J. D. Sterman (2000) *Bathtub Dynamics: Initial Results of a Systems, Thinking Inventory*. System Dynamics Review, 16, 249-294. Available at: https://jsterman.scripts.mit.edu/Online_Publications.html#2000Bathtub.

the fact patterns be a requisite part of this conversation. A neutral study commission that would produce a full systems analysis and meaningful, systems-wide statistics and data is essential, as is for a neutral body to factually study the impacts of any proposed solutions within a systems thinking context. This is where a privacy systems analysis needs to be included.

- Fourth, established governance tools exist that could, if used appropriately and with a narrow focus, facilitate voluntary multi-stakeholder problem solving in the context of Section 230, including problems relating to privacy. One particular governance tool, *voluntary consensus standards*,[4] discussed in further detail in these comments, could potentially be effective for solving problems that arise for people and groups of people in some Section 230 ecosystems. These tools will be most effective when used in a systems context, and with procedural and contextual integrity. Voluntary consensus standards already exist and are defined in U.S. law.[5] These types of standards are already in active use, for example, the U.S. Food and Drug Administration has been using voluntary consensus standards that comply with due process requirements as articulated in the U.S. Office of Management and Budget (OMB)[6] Circular A-119 for more than 20 years, which has resulted in more than 1,000 recognized standards applicable to medical devices.[7] The World Trade Organization (WTO), *Agreement on Technical Barriers to Trade*[8] is a core document that outlines how standards may be set by independent parties in a fair and appropriate manner that does not create transactional or other barriers.

---

[4] *Voluntary consensus standards* are a well-defined term of art, and law. A voluntary consensus standard is one that is developed or adopted by Standards Developing Organizations (SDOs), both domestic and international, according to strict consensus principles. Consensus standards contribute to regulatory quality because consensus-based SDOs must demonstrate adherence to the tenets of transparency, openness to participation by interested stakeholders, balance of representation, and due process, among other principles.

[5] OMB Circular A-119, "Federal Participation in the Development and Use of voluntary Consensus Standards and in Conformity Assessment Activities," 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary.

[6] U.S. Office of Management and Budget. See: https://www.whitehouse.gov/omb/.

[7] U.S. Food and Drug Administration Recognized Consensus Standards, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

[8] World Trade Organization, *Agreement on Technical Barriers to Trade*. Available at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm

Section 230 has a lengthy and complex legislative history, which has been skillfully discussed by Kosseff,[9] and also by Citron and Franks.[10] Similar to the contours of legislative debates about privacy, in discussions about Section 230 there appears to be indecision about the best course of action to take to solve problems. Consensus has not yet emerged regarding the best path forward with respect to legislative approaches that would act to curb harms but not hinder innovation.

I propose an alternate approach. If the problem to be solved in the Section 230 debate is also framed as one of *governance*, and not only framed as a problem to be addressed by legislative rules, then a wide range of new strategies and policy instruments become available. Nobel Laureate Elinor Ostrom's design principles for the self-sustaining governance of ecosystems are helpful to understand as a basis for thinking about the potential for additional pathways to solutions.[11]

A. The Work of Elinor Ostrom

Nobel Laureate and economist Elinor Ostrom spent her entire career observing and analyzing governance of complex ecosystems, particularly the commons, or shared resources. Over the span of decades, she observed and distilled the most effective ways of managing complex environmental ecosystems where stakeholders share resources, what Ostrom calls "common pool resources," or CPRs.[12] In digital ecosystems, identity — particularly digital identity or dematerialized identity — is one such common pool resource, as is data, such as transactional data and knowledge generated by the everyday actions of people.[13]

---

[9] Jeff Kosseff, The Twenty Six Words That Created the Internet, Cornell University Press, 2019. See: https://www.jeffkosseff.com.

[10] Danielle Keats Citron and Mary Anne Franks, *The Internet As a Speech Machine and Other Myths Confounding Section 230 Speech Reform.* Boston Univ. School of Law, Public Law Research Paper No. 20-*8,* February 1, 2020. Available at: http://dx.doi.org/10.2139/ssrn.3532691.

[11]Nives Dolšak, Elinor Ostrom & Bonnie J. Mccay, The Commons in the New Millenium (2003) Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

[12] Ostrom defined the term common pool resources as integral parts of a resource system. "The term 'common pool resource' refers to a natural or man made resource system that is sufficiently large as to make it costly (but not impossible) to exclude potential beneficiaries from obtaining benefits from its use. To understand the process of organizing and governing CPRs, it is essential to distinguish between the *resource system* and the flow of *resource units* produced by the system, while still recognizing the dependence of the one on the other." Elinor Ostrom, Governing the Commons (1990, 2015) "The CPR Situation."

[13] *Transactive cognition* occurs wherever knowledge is created, organized, and used across two or more domains simultaneously. See transactive memory in Daniel Wegner et al, Cognitive interdependence in close relationships, in Compatible and incompatible relationships, Springer-Verlag (1985) at 253-276.

Ostrom rigorously eschewed fixed models of resource management that were based on centralization or property rights. However, her work documented that mutually agreed upon governance of resources that are shared can work, and have been proven to work. If we think of data and knowledge as a shared common pool resource, one in which multiple stakeholders have involvement with and an interest in, then we have a pathway to govern those systems as shared resource systems. It is in this context that Elinor Ostrom's work is of central importance in the privacy and in the Section 230 context.

B. Ostrom's 8 Principles of Governance

Ostrom set forth 8 principles for governance of complex systems using common pool resources. As mentioned earlier, Ostrom's governance principles were originally derived from observations in complex environmental and other ecosystems. Just as privacy impact assessments (PIAs) originated from environmental impact assessments,[14] the Ostrom principles that have worked to govern complex environmental and other ecosystems sustainably without draining resources can also work to create desired outcomes in complex digital ecosystems.

The Ostrom general principles are as follows:

1. Rules are devised and managed by resource users.
2. Compliance with rules is easy to monitor.
3. Rules are enforceable.
4. Sanctions are graduated.
5. Adjudication is available at low cost.
6. Monitors and other officials are accountable to users.
7. Institutions to regulate a given common-pool resource may need to be devised at multiple levels.
8. Procedures exist for revising rules."[15]

---

[14]Kenneth A. Bamberger and Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in U.S. Government Agencies,* July 22, 2012. D. Wright, P. DeHert (eds.), Privacy Impact Assessment (2012); UC Berkeley Public Law Research Paper No. 2222322. Available at: https://ssrn.com/abstract=2222322 . *See also*: Roger Clarke, *A History of Privacy Impact Assessments*. Available at: http://www.rogerclarke.com/DV/PIAHist.htmlRoger Clarke. *See also*: Roger Clarke, *Privacy Impact Assessment: Its origins and development,* Computer Law & Security Review, Vol. 25, Issue 2, 2009. Available at: https://doi.org/10.1016/j.clsr.2009.02.002.

[15] Nives Dolšak, Elinor Ostrom & Bonnie J. Mccay, The Commons in the New Millenium. (2003). See esp. Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

This governance structure is highly specific, and is what facilitates the creation of practical guidance for implementing data protection and other protective principles which may be broadly worded in statutes or regulations. Governance needs to be particular, iterative, and continually updated. "Living" governance is the key.[16] Governance also facilitates identification and mitigation of digital ecosystem risks, which can then assessed continually in a ongoing benchmarking of established rules against reality. Adjustment of daily practices then are based on actual, provable, repeatable feedback.

However, governance, to be practical and effective for the relevant stakeholders, is best when specific and not overbroad. If governance is created in industry-only standards setting processes, this would omit consumers or other stakeholders. This would not be a good outcome for Section 230 stakeholders. The process needs to be collaborative and not dominated by any one participant in one or more data ecosystems.

In the past, the creation of specific self-governance standards for specific slices of the ecosystem have proven to be an area of considerable difficulty because the standards have been conducted in a "self regulatory" manner.[17] Voluntary consensus standards are not self regulation — they are *due process standards* that adhere to a system of standards creation typified by specific checks and balances contained in, for example, the *ANSI Essential Requirements,*[18] or OMB Circular A-119. In this way, voluntary consensus standards can be an extension, or an implementation, of Ostrom's governance ideas.

C. Voluntary Consensus Standards

In the United States, there are three critical definitional groundings for voluntary consensus standards:

---

[16] NIST's Facial Recognition Vendor Tests are an excellent example of the application of the idea of iterative work. In the past, NIST's tests were periodically conducted. Now, they are ongoing via what NIST calls "living documents." NIST Biometrics Pages, *NIST FRVT 1:N 2018 Evaluation*. Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation.

[17] Robert Gellman and Pam Dixon, *Many Failures: A brief history of privacy self-regulation,* World Privacy Forum, 2011. Available at: https://www.worldprivacyforum.org/2011/10/report-many-failures-introduction-and-summary/.

[18] *ANSI Essential Requirements: Due process requirements for American National Standards,* American National Standards Institute*,* Jan. 2018. Available at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf. The ANSI standards require openness, lack of dominance, balance, coordination and harmonization, notification of standards development, consideration of views and objections, consensus vote, appeals, and written procedures. There are also benchmarking procedures and compliance procedures with the rules.

- The OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,[19] (The National Technology Transfer and Advancement Act (NTTAA) codifies OMB Circular A-119.)

- The ANSI Essential Requirements: Due Process requirements for American National Standards.[20]

- U.S. Congress, Office of Technology Assessment Global Standards: Building Blocks for the Future, TCT - 512, March 1992.[21]

Within the framework of due process guarantees set out in OMB Circular A-119, federal regulators today have the power to recognize compliance with voluntary consensus standards as evidence of compliance with the law for specific, limited regulatory purposes. Federal regulators may only use voluntary consensus standards to create such safe harbors if the standards can be shown to have been developed through processes whose openness, balance, consensus, inclusion, transparency and accountability have been independently verified.

In 1996, the National Technology Transfer and Advancement Act (NTTAA) (Pub. L. No. 104-113), codified OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.[22] The NTTAA and OMB Circular A-119 established that Federal government agencies were to use voluntary consensus standards in lieu of government-unique standards except where voluntary consensus standards are inconsistent with law or otherwise impractical. The ANSI Essential Requirements set forth in detail the definitions and processes that comprise a "due process" standards setting body, and procedures.

The most current definition of a standards body that creates voluntary consensus guidelines is as follows, as found in the 2016 revision of OMB Circular A-119:

---

[19] *OMB Circular A-119, "Federal Participation in the Development and Use of voluntary Consensus Standards and in Conformity Assessment Activitie*s," 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.nist.gov/sites/default/files/revised_circular_a-119_as_of_01-22-2016.pdf.

[20] *ANSI Essential Requirements: Due process requirements for American National Standards*, ANSI. Available at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf.

[21] U.S. Congress, Office of Technology Assessment, *Global Standards: Building Blocks for the Future,* TCT - 512, March 1992. Available at: https://www.princeton.edu/~ota/disk1/1992/9220/9220.PDF

[22] National Technology Transfer and Advancement Act (NTTAA) (Pub. L. No. 104-113).

"Voluntary consensus standards body" is a type of association, organization, or technical society that plans, develops, establishes, or coordinates voluntary consensus standards using a voluntary consensus standards development process that includes the following attributes or elements:

I. **Openness**: The procedures or processes used are open to interested parties. Such parties are provided meaningful opportunities to participate in standards development on a non-discriminatory basis. The procedures or processes for participating in standards development and for developing the standard are transparent.

II. **Balance**: The standards development process should be balanced. Specifically, there should be meaningful involvement from a broad range of parties, with no single interest dominating the decision-making.

III. **Due process**: Due process shall include documented and publicly available policies and procedures, adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views.

IV. **Appeals process**: An appeals process shall be available for the impartial handling of procedural appeals.

V. **Consensus**: Consensus is defined as general agreement, but not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.[23]

The idea of the U.S. Federal Trade Commission (FTC)[24] providing a safe harbor for business in the privacy sphere has continued to arise, particularly in conversations about privacy. But the FTC, and indeed most Federal agencies, must comply with the rules enshrined in the OMB Circular — the FTC cannot simply grant a safe harbor without substantive voluntary consensus standards involvement. Circular A-119 applies to all US Federal "agencies and agency representatives who use standards or conformity assessment and/or participate in the development of standards.

"Agency" means any executive department, independent commission, board, bureau, office, government-owned or controlled corporation, or other establishment of the Federal government.

---

[23] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.nist.gov/sites/default/files/revised_circular_a-119_as_of_01-22-2016.pdf.

[24] U.S. Federal Trade Commission. See: https://www.ftc.gov.

It also includes any regulatory commission or board, except for independent regulatory commissions insofar as they are subject to separate statutory requirements regarding the use of voluntary consensus standards. It does not include the Legislative or Judicial branches of the Federal government."[25]

The OMB Circular states that all Federal agencies[26] must use voluntary consensus standards (in lieu of government-unique standards) in procurement and regulatory activities, except "where inconsistent with law or otherwise impractical." Legislative and judicial branches of the federal government are not subject to OMB Circular A-119. However, the Circular does apply to all federal agencies, including law enforcement, national security, and other regulatory agencies such as the FBI, CIA, and NSA, HHS, the FTC, the FDA, and others.[27]

D. Case Study: FDA Recognition of Voluntary, Consensus Standards

The U.S. Food and Drug Administration (FDA)[28] is one of the agencies that already has a formal system in place to recognize voluntary consensus standards. Specifically, its system for medical device standards has been in place for two decades. The standards development process for medical devices is strictly defined, as articulated in OMB Circular A-119. In 1996, the National Technology Transfer and Advancement Act (NTTAA) (Pub. L. No. 104-113), codified OMB Circular A-119.

The shift to voluntary consensus standards in the 1990s has resulted in the FDA formally recognizing over 1,000 VCS standards, which are housed in a publicly accessible database.[29] Non-recognized standards are also publicly available. The FDA program relies on standards

---

[25] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.nist.gov/sites/default/files/revised_circular_a-119_as_of_01-22-2016.pdf.

[26] ANSI essential requirements can also fully apply to standards governing, for example, the FBI, CIA, and NSA in areas such as the voluntary sharing of information by businesses with law enforcement. The development of due process standards for this category of data flows and activity would be beneficial to all stakeholders, including the public, as these data flows are among the least understood aspects of today's data ecosystems.

[27] WPF has proposed a discussion draft that would allow the FTC to recognize due process VCS. See: Jane K. Winn and Pam Dixon, *Consumer Privacy and Data Security Standards Discussion Draft Bill 2019-2020*, World Privacy Forum. Available at: http://www.worldprivacyforum.org/wp-content/uploads/2019/04/Consumer-Privacy-and-Data-Security-Standards-Act-of-2019-FS.pdf.

[28] U.S. Food and Drug Administration home page. Available at: https://www.fda.gov.

[29] US Food and Drug Administration, Recognized Standards Database, Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

created by "voluntary consensus standards" rules, which have well-established meaning in the US and globally, as discussed.

The FDA's voluntary consensus standards program grew from a long period of reform at the FDA. In 1976, the FDA put an American National Standards Institute (ANSI)[30] standard for medical devices in place. Under the 1976 rules, the production of standards was lagging far behind production of medical devices due to the rigidity of the existing standard development process.[31] To address this lag and other challenges at the FDA, in March 1990, Health and Human Services Secretary Louis Sullivan convened the Edwards Committee, a group of leading FDA experts including Dr. Charles Edwards, the former head of the FDA. The committee was tasked with reviewing the FDA at a high level, and understanding how to improve an agency the committee agreed was at risk.

After a year of deliberation, the Edwards Committee issued a report and recommendations, which included recommendations for regulatory reform. The report noted it was crucial to "recognize that approval of useful and safe new products can be as important to the public health as preventing the marketing of harmful or ineffective products."[32] The report eventually resulted in many changes to the FDA after lengthy deliberations and analysis.

As part of the improvements pursuant to the Reinventing Government program undertaken in 1997,[33] the FDA's voluntary consensus standards program was created to replace the 1976 ANSI standard. The Food and Drug Administration Modernization Act (FDAMA) formally enshrined the voluntary consensus guidelines in the FDA context.[34] The FDA has the authority to recognize voluntary consensus standards, and the FDA may develop its own technical standards if the voluntary consensus standards do not meet FDA's requirements. In recent years, the VCS

---

[30] ANSI is the American National Standards Institute. It is an important standards development organization. See: https://www.ansi.org/.

[31] Department of Health. Education, and Welfare, Food and Drug Administration. Medical Devices, Performance Standards Activities. August 9, 1976. 41 FR 34005 (Aug. 12, 1976.)

[32] Advisory Committee on the FDA, US Department of Health and Human Services, Final Report of the Advisory Committee 14 (1991). *See also*: Dr. Charles Edwards and members of the Edwards Committee regarding its Final Report, Senate Labor Committee, CSPAN, May 15, 1991. Available at: https://www.c-span.org/video/?17990-1/food-drug-administration&start=20.

[33] FDA Backgrounder on FDAMA, Available at: https://www.fda.gov/regulatory-information/food-and-drug-administration-modernization-act-fdama-1997/fda-backgrounder-fdama.

[34] For a regulatory history of the time period between the ANSI standard and the activities surrounding the development of VCS, see Medical Device Reporting Regulation History, FDA, March 27, 2000. Available at: https://wayback.archiveit.org/7993/20170404182017/https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm127985.htm.

have been expanded to encompass an increased range of FDA activities, and the 21st Century Cures Act further elaborated on VCS.[35]

FDA Current Standard Setting and Conformity Assessment Program	
	FDA Appropriate Use of Voluntary Consensus Standards to facilitate premarket review of medical devices
Statutory Authority	1976 Medical Device Amendments to FD&C Act (failed); Food and Drug Administration Modernization Act of 1997 (successful); OMB Circular A-119
Source of standard	Voluntary consensus standards
Definition of voluntary consensus from NTTAA	Consensus (including an attempt to address all comments by interested parties) Openness Balance of interest Due process Appeals process
Access to recognized standards	Internet Database of Recognized and Non-Recognized Standards
Recognition of Standards	Any interested party may request recognition of a standard
Conformity Assessment	Medical device sponsors can use consensus standards to demonstrate certain aspects of safety and effectiveness in a premarket approval application by submitting "Declaration of Conformity" to standard

[35] Food and Drug Administration Modernization Act of 1997 (FDAMA) (Pub. L. No. 105-115). See also: 21st Century Cures Act (Pub. L. 114-255). The FDAMA amends section 514(c) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). Section 514(c) states the FDA "shall, by publication in the Federal Register . . . recognize all or part of an appropriate standard established by a nationally or internationally recognized standard development organization for which a person may submit a declaration of conformity in order to meet a premarket submission requirement or other requirement," 21 U.S.C. 360d(c)(1)(A). (Quoted in part.) *See also*: Guidance Document: CDER's Program for the Recognition of Voluntary Consensus Standards Related to Pharmaceutical Quality, US FDA, Feb. 2019. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cders-program-recognition-voluntary-consensus-standards-related-pharmaceutical-quality.

Legal Result	Reduced compliance burden in Premarket Approval process
Benefit to regulator, regulated entities, public	Voluntary, consensus standards reduce compliance burdens by increasing predictability, streamlining premarket review, providing clearer regulatory expectations, facilitating market entry for safe and effective medical products, and promoting international harmonization.

Figure 1: Overview of the FDA use of voluntary consensus standards

The chart below (*Figure 2*) maps how the FDA Voluntary consensus standards map to potential FTC Voluntary consensus standards.

FDA Current Standard Setting and Conformity Assessment Program compared to FTC Proposed Standard Setting and Conformity Assessment Program		
	FDA Appropriate Use of Voluntary Consensus Standards to facilitate premarket review of medical devices	**FTC Appropriate Use of Voluntary Consensus Standards to encourage conformity with reasonable data administration standards**
Statutory Authority	1976 Medical Device Amendments to FD&C Act (failed); Food and Drug Administration Modernization Act of 1997 (successful); OMB Circular A-119	Prohibition on unfair and deceptive trade practices under FTC Act; OMB Circular A-119
Source of standard	Voluntary consensus standards	Voluntary consensus standards
Definition of voluntary consensus from NTTAA	Consensus (including an attempt to address all comments by interested parties) Openness Balance of interest Due process Appeals process	Consensus (including an attempt to address all comments by interested parties) Openness Balance of interest Due process Appeals process

Access to recognized standards	Internet Database of Recognized and Non-Recognized Standards	Internet Database of Recognized and Non-Recognized Standards
Recognition of Standards	Any interested party may request recognition of a standard.	Any interested party may request recognition of a standard
Conformity Assessment	Medical device sponsors can use consensus standards to demonstrate certain aspects of safety and effectiveness in a premarket approval application by submitting "Declaration of Conformity" to standard	Data administrators can use consensus standards to demonstrate certain aspects of protection for reasonable expectations of privacy; security by submitting "Declaration of Conformity" to standard
Legal Result	Reduced compliance burden in Premarket Approval process	Rebuttable presumption of compliance with FTC act
Benefit to regulator, regulated entities, public	Voluntary, consensus standards reduce compliance burdens by increasing predictability, streamlining premarket review, providing clearer regulatory expectations, facilitating market entry for safe and effective medical products, and promoting international harmonization.	Voluntary, consensus standards reduce compliance burdens by increasing predictability, streamlining enforcement oversight, providing clearer regulatory expectations, facilitating protection of reasonable expectation of privacy; promoting international harmonization.

Figure 2: Comparison of FTC and FDA use of voluntary consensus standards.

E. The Role of Trust in Information Governance

Historically, in the absence of trust, data ecosystems often resort to hierarchical, non-transparent, inflexible, and less than democratic approaches to data use and control. Biometric-based identity installations have been a significant exemplar of how this process has operated when things have gone awry. History has provided numerous examples of large and even national-level identity ecosystems which failed after end-user stakeholders lost trust in those systems and their

controllers.[36] Data and data ecosystems are subject to the same prospects of failure, fragility or robustness that Ostrom observed in her work in environmental systems.

A core element of sustainability in data ecosystems is mutual trust by all participants. Trust issues can arise in "Section 230" ecosystems (and other data ecosystems) regarding sexual harassment, bullying, stalking, and other forms of harassment and harm.[37] Without mitigation such as mutually agreed upon guardrails or standards in data ecosystems, the classic result is the creation of a "social trap," or a situation where there is a significant loss of mutual trust that is deleterious to all parties, as described by Bo Rothstein.[38] In the case of data ecosystems that are large, losses of trust can have profound negative impacts.[39]

Over the long term, people will not tolerate data systems that facilitate harms. We can see some data points regarding general online trust problems emerging already, such as lack of mutual trust

---

[36] The now-disbanded UK National ID Card System is an exemplar of a system that experienced failure at a national level. The system, approximately 8 years in the planning, was launched and partially implemented, but was not trusted due to highly intrusive, non-voluntary measures many of those who were to be subject to the cards objected to. The system was disbanded just after its launch, at significant expense. For background, see: Alan Travis, *ID cards scheme to be scrapped within 100 days,* The Guardian, 27 May, 2010. Available at: https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards . The £ 4.5 billion UK system, which was envisioned to encompass an ID register, biometric passports, and a mandatory ID, was scrapped after 15,000 ID cards were already issued. Legislation was passed abolishing the system in 2010; The Identity Documents Act 2010 repealed the Identity Cards Act 2006. See *Identity Documents Act 2010,* Parliament, UK. Available at: https://services.parliament.uk/bills/2010-11/identitydocuments.html. See also discussions of India's Aadhaar national biometric ID system and its profound failures: Dhananjay Mahapatra, Don't let poor suffer due to lack of infrastructure for authentication of Aadhaar, Times of India, April 24, 2018. https://timesofindia.indiatimes.com/india/dont-let-poor- suffer-due-to-lack-of- aadhaar-tech-sc/articleshow/62842733.cms

[37] Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (And As It Should Be)* Michigan Law Review, Forthcoming. August 9, 2019. Available at SSRN: https://ssrn.com/abstract=3435200 or http://dx.doi.org/10.2139/ssrn.3435200.

[38] Bo Rothstein. Social Traps and the Problem of Trust. Cambridge University Press, (2005). See in particular Chapters 8 and 9.

[39] Large data breaches and unauthorized disclosures are among the types of data problems that have caused loss of trust. For example, the U.S. Office of Personnel Management experienced a data breach affecting 22 million individuals in 2012-2014. See: U.S. OPM, *Cybersecurity Resource Center*. Available at: https://www.opm.gov/cybersecurity/cybersecurity-incidents/. The Equifax data breach of the data of nearly 150 million people caused a generalized loss of trust regarding security practices in segments of the financial sector. See: *Data Protection: Actions taken by Equifax and federal agencies in response to the 2017 breach,* GAO - 18-559. GAO, Sept. 7, 2018. Available at: https://www.gao.gov/products/gao-18-559.

regarding data uses and online activity.[40] Addressing the problems associated with the loss of trust is an important task. Trust, when it has collapsed, is not easy to reestablish — and developing mutual trust must be earned over time.[41] Reestablishing failed trust requires dialogue, cooperation, and other elements that Elinor Ostrom eloquently articulated in her decades of empirical work on governance. In the right context, and with enough definitional focus, voluntary consensus standards processes may assist with rebuilding dialogue and cooperation in a variety of data ecosystems.

F. Conclusion

To allow for forward movement in the Section 230 debate, I have four specific recommendations:

1. The Section 230 debate would benefit from a neutral study commission tasked with undertaking a comprehensive multi-systems analysis of Section 230-related issues. Experts and statisticians who are specifically familiar with researching and documenting dynamic complexity need to be included on the commission. A poor outcome for a study commission would be to have a commission that did not conduct this kind of rigorous comprehensive analysis and documentation work.
2. There has not been adequate attention to a privacy analysis across interrelated systems for proposed changes to Section 230. In our modern privacy context, it is no longer feasible to propose changes to Section 230 without undertaking such an analysis.
3. Voluntary Consensus Standards should only be attempted if a fair, neutral, fact-based approach is used in a well-defined and narrow context. For example, the FDA's use of VCS for medical devices is appropriately narrow; each device gets a standard. The FDA did not

---

[40] The US Census Bureau collected significant national consumer research regarding privacy and trust in July 2015. The results were given to the NTIA and form the basis of an extensive national survey and analyses published in 2016. NTIA, based on the survey results, found that a lack of consumer trust was negatively impacting economic activity. The NTIA noted: "Perhaps the most direct threat to maintaining consumer trust is negative personal experience. Nineteen percent of Internet-using households—representing nearly 19 million households—reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the July 2015 survey." See: NTIA, *Lack of trust in Internet privacy and security may deter economic and other online activities,* May 13, 2016. Available at: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other- online-activities. *See also:* Bo Rothstein. Social Traps and the Problem of Trust. Cambridge University Press, (2005). See in particular Chapters 8 and 9.

[41] Bo Rothstein. Social Traps and the Problem of Trust. Cambridge University Press, (2005). See in particular Chapters 8 and 9. See also generally, the work of Elinor Ostrom, The Commons in the New Millenium: Challenges and adaptation (2003) Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

use VCS to "boil the ocean" and create broad principles, but rather to address specific, well-defined, discrete issues.

4. I encourage the Department to facilitate public comments on the February 19 workshop. Even if a Federal Register Notice is not contemplated for this workshop, an open, transparent process of allowing for comments from the public is appropriate and fair.

Thank you for the opportunity to speak at the workshop, and to submit written comments.

Respectfully submitted,

Pam Dixon

Department of Justice Section 230 Workshop, Feb. 19, 2020 (revised Feb. 27, 2020)

Statement of Dr. Mary Anne Franks,
Professor of Law and Dean's Distinguished Scholar, University of Miami School of Law
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative

Champions of Section 230 claim that the law promotes free speech, stimulates commerce, and allows unprecedented access to information. And they are not wrong. Section 230 has, without a doubt, produced a wealth of expressive, economic, and informational benefits. What is often missing from these exuberant accounts, however, is any acknowledgment of how unequally both the benefits and the harms flowing from the exceptional immunity granted to the tech industry are distributed. For while the ruthlessly anti-regulatory, pro-corporation, techno-utopian system made possible by courts' expansive interpretation of Section 230 immunity certainly does generate enormous capital, both literal and symbolic, the vast majority of that capital stays firmly in the hands of those who have always had more of it than everyone else: the wealthy, the white, the male. While Section 230 does indeed amplify free speech, increase profits, and enable informational dominance for the powerful and the privileged, it also enables the silencing, bankrupting, and subordination of the vulnerable.

We are all living in the world Section 230 built, and it is one riven by inequality: speech inequality, financial inequality, informational inequality. It is a world in which public officials can use a social media platform to threaten foreign powers and their own citizens; where global corporations can extract astronomical profits from exploiting private data, where women can be driven offline by misogynist mobs, where massive disinformation and misinformation campaigns can micro-target populations to create public health crises, incite terrorism, and undermine democracy itself.

The concept of "cyber civil rights" (a phrase coined by Professor Danielle Citron in 2009),[1] highlights how the Internet has rolled back many recent gains in racial and gender equality. The anonymity, amplification, and aggregation possibilities offered by the Internet have allowed private actors to discriminate, harass, and threaten vulnerable groups on a massive scale. Abundant empirical evidence demonstrates that the Internet has been used to further chill the intimate, artistic, and professional expression of individuals whose rights were already under assault offline.[2] Even as the Internet has multiplied the possibilities of expression, it has multiplied the possibilities of repression. The new forms of communication offered by the Internet have been used to unleash a regressive and censorious backlash against women, racial minorities, sexual minorities, and any other groups seeking to assert their rights of expression. The Internet lowers the costs of engaging in abuse by providing abusers with anonymity and social validation, while providing new ways to increase the range and impact of that abuse. The online abuse of women in particular amplifies sexist stereotyping and discrimination, compromising gender equality online and off.[3]

Section 230 contributes to our current dystopian reality by fundamentally undermining the legal principle of collective responsibility, obliterating the distinction between speech and conduct, and

1 Danielle Keats Citron, *Cyber Civil Rights,* 89 B.U. L. REV. 61 (2009);
2 *See* Mary Anne Franks, *The Free Speech Black Hole: Can the Internet Escape the Gravitational Pull of the First Amendment?* Knight First Amendment Institute (August 2019), https://knightcolumbia.org/content/the-free-speech-black-hole-can-the-internet-escape-the-gravitational-pull-of-the-first-amendment
3 Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 Colum. J. Gender & L. 224 (2011).

granting special privileges to online entities unavailable to their offline counterparts.[4] Courts have interpreted Section 230 to protect online classifieds sites from responsibility for advertising sex trafficking,[5] online firearms sellers from responsibility for facilitating unlawful gun sales,[6] and online marketplaces from responsibility for putting defective products into the stream of commerce.[7]

But it does not have to be this way. Careful, modest reform is possible to better align the statute with its original goals, which are evocatively expressed by the title of Section 230's operative clause: "Protection for 'Good Samaritan' blocking and screening of offensive material."[8] This title suggests that Section 230 is meant to provide "Good Samaritan" immunity in much the same sense as "Good Samaritan" laws in physical space. Such laws do not create a duty to aid, but instead provide immunity to people who attempt in good faith and without legal obligation to aid others in distress.[9] While Good Samaritan laws generally do not require people to offer assistance, they encourage people to assist others in need by removing the threat of liability for doing so.

Similarly, one clear purpose of Section 230 was to encourage online intermediaries to render assistance when they have no obligation to do so. Subsection (c)(2) assures providers and users of interactive computer services that they will not be held liable with regard to 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" or "taken to enable or make available to information content providers or others the technical means to restrict access" to such material.[10] Given that it tracks the familiar legal principles of its namesake, subsection (c)(2) is the relatively uncontroversial portion of Section 230.

By contrast, Subsection 230(c)(1), "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,"[11] has been interpreted in ways that are not only at odds with Good Samaritan laws, but with a host of other legal principles and settled law. [12]

To parse this provision, it is useful to recall that while U.S. law does not impose a general duty to aid, it does recognize a limited concept of collective responsibility for harm. In the physical world, third parties can sometimes be held criminally or civilly liable for the actions of other people. Many harmful acts are only possible with the participation of multiple actors with various motivations. The doctrines of aiding and abetting, complicity, and conspiracy all reflect the insight that third parties who assist, encourage, ignore, or contribute to the illegal actions of another person can and should be held responsible for their contributions to the harms that result, particularly if those third parties benefited in some material way from that contribution.

4 *See* Mary Anne Franks, *How the Internet Unmakes the Law,* Ohio State Tech. L. J. (forthcoming 2020).
5 E.g., Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016).
6 E.g., Daniel v. Armslist, LLC, 2019 WI 47, 386 Wis. 2d 449 N.W.2d 710, *cert. denied,* No. 19-153, 2019 WL 6257416 (U.S. Nov. 25, 2019).
7 E.g., Oberdorf v. Amazon.com, Inc., 295 F. Supp. 3d 496 (M.D. Pa. 2017), *aff'd in part*, *vacated in part,* 930 F.3d 136 (3d Cir. 2019), *vacated en banc*, 936 F.3d 182 (3d Cir. 2019).
8 47 U.S.C. § 230 (2018).
9 *See*, *e.g.*, Mueller v. McMillian Warner Ins. Co., 290 Wis. 2d 571, 714 N.W.2d 183 (Wis. 2006).
10 47 U.S.C. § 230(c)(2) (2018).
11 47 U.S.C. § 230(c)(1) (2018).
12 Oberdorf v. Amazon.com Inc., 930 F.3d 136, 151-52 (3d. Cir.), vacated, 936 F.3d 182 (3d. Cir. 2019).

Among the justifications for third-party liability in criminal and civil law is that this liability incentivizes responsible behavior. For example, it is a central tenet of tort law that the possibility of such liability incentivizes individuals and industries to act responsibly and reasonably. Conversely, grants of immunity from such liability risk encouraging negligent and reckless behavior.

Yet courts have interpreted Section 230 (c)(1) to grant online intermediaries near-total immunity even when their products, services, and platforms are used to inflict harm.[13] The provision has been used to provide sweeping immunity to message boards like 8chan (now 8kun), which provide a platform for mass shooters to spread terrorist propaganda, as well as to online firearms marketplaces such as Armslist, which facilitate the illegal sale of weapons to violent domestic abusers. It has even been used by Amazon to attempt to avoid responsibility for facilitating the sale of a defective dog leash that blinded a woman.

These online intermediaries are in no sense "Good Samaritans."[14] They are not individuals who voluntarily intervene to prevent or mitigate harm caused by someone else. They are at best passive bystanders who do nothing to intervene against harm, and at worst, they are accomplices who encourage and profit from harm. If their conduct occurred offline, they could be held legally accountable for their role in causing harm. Why should the fact that it occurs online change this result?

One justification sometimes offered is that the Internet is a medium of speech, and the First Amendment requires regulations of speech to be much less burdensome than regulations of conduct. But even the First Amendment does not protect all speech; Supreme Court free speech cases frequently focus on whether a particular kind of speech is protected, and to what degree, by the First Amendment.[15] Even more fundamentally, the Court is often forced to first determine whether an act is speech *at all* for the purposes of the First Amendment. When presented with the wearing of black armbands, setting flags on fire, making financial contributions to political campaigns, or burning draft cards, the Court has first addressed whether the acts are speech at all before taking up the question of what degree of protection they receive. Because so much online activity involves elements that are not unambiguously speech-related, whether such activities are in fact speech should be a subject of express inquiry.

Conflating Section 230 with the First Amendment short-circuits this inquiry. Intermediaries invoking Section 230 presume, rather than demonstrate, that the acts or omissions at issue are speech, and courts allow them to do so without challenge. In doing so, courts have bestowed on online intermediaries a defense that exceeds even the capacious boundaries of First Amendment doctrine and which is not available to offline intermediaries.

Section 230 could easily be amended to make explicitly clear that the statute's protections only apply to speech by replacing the word "information" in (c)(1) with the word "speech." This revision would put all parties in a Section 230 case on notice that the classification of content as speech is not

[13] *See* Mary Anne Franks, *Our Collective Responsibility for Mass Shootings*, N.Y.TIMES (Oct. 9. 2010), https://www.nytimes.com/2019/10/09/opinion/mass-shooting-responsibility.html [[https://perma.cc/TC43-SD8P]
[14] *See* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 416 (2017).
[15] *See* Danielle Keats Citron and Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Tech Policy Reform,* U. Chi. Legal F. (forthcoming 2020)

a given, but a fact to be demonstrated. If a platform cannot make a showing that the content or information at issue is speech, then it should not be able to take advantage of Section 230 immunity.

Another justification offered for granting immunity to online intermediaries not available to their offline counterparts is scale. Online social media platforms, for example, deal with millions, sometimes billions, of pieces of content on a regular basis; no brick-and-mortar bookstore approaches the number of transactions occurring on Amazon.com every hour. The sheer volume of this content would turn any duty of moderation into a Herculean effort. But it is not obvious why the enormity of scale should translate into less, rather than greater responsibility, for online intermediaries. For one, more activity means more potential for harm, and two, it is precisely the extraordinary scale of Internet activity that helps generate multi-billion-dollar profits–profits that could be put towards ensuring that this activity is reasonably regulated.[16]

Section 230 establishes a dual regime of law, with one rule for offline conduct and another for online conduct. But once Section 230's expansive immunity has been embraced, there is no clear reason to continue to restrict it to online activity. Offline entities can plausibly complain that the differential treatment afforded by broad interpretations of Section 230 violates principles of fairness and equal protection, or to put it more bluntly: if they can do it, why can't we?

In attempting to chart a better course forward, it is useful to consider how Section 230, the law of the Internet, live up to its namesake, the law of the Good Samaritan. The parable of the Good Samaritan, recounted in the book of Luke, is the story of a man set upon by robbers who beat him, steal his possessions, and leave him for dead.[17] A priest comes across the wounded man but does not stop to help; a Levite does the same. But a third man, a Samaritan, stops to help. He tends to the man's injuries, takes him to an inn, and looks after him.

The moral of the parable is generally understood to be that being a "Good Samaritan" means helping another in need even when one is not obligated to do so. While Section 230 (c)(2) hews closely to this idea, Section 230 (c)(1) has been interpreted to ensure that this protection extends not only to bystanders who attempt to help, but also to bystanders who do nothing. Worse yet, it has also been extended to people who are not bystanders at all, but actual participants in harmful conduct. This interpretation of Section 230 treats the priest, the Levite, and *the robbers* the same as the Good Samaritan. In doing so, Section 230(c)(1) not only fails to encourage good behavior, but incentivizes evil behavior.

There is an often-overlooked dimension to the story of the Good Samaritan that even more clearly illuminates the gap between the law of the Internet and the law of the Good Samaritan. The occasion for the parable is an exchange between Jesus and a lawyer who wishes to know what he must do to attain eternal life. Jesus replies, "What is written in the law? How do you read it?" The lawyer answers, "You shall love the Lord your God with all your heart, with all your soul, with all your strength, with all your mind, and your neighbor as yourself." After Jesus verifies that this is the correct answer, the lawyer continues his interrogation by asking "Who is my neighbor?"

It is at that point that Jesus relates the story of the Good Samaritan, which concludes with Jesus asking the lawyer, "Now which of these three do you think seemed to be a neighbor to him who fell

16 *See* Mary Anne Franks, *Moral Hazard on Stilts: 'Zeran's Legacy*, The Recorder, Law.com (Nov. 10, 2017).
17 *Luke* 10:31 (New International Version).

among the robbers?" The lawyer replies, "He who showed mercy on him," and Jesus tells him, "Go and do likewise."[18]

As Jesus leads the lawyer to conclude, the neighbor– the person whom the lawyer is commanded to love as himself–is *the Samaritan*. The significance of this is made apparent by considering the longstanding enmity, recounted in several other New Testament passages, between Jews and Samaritans. By naming a member of a despised group as the neighbor in the parable, Jesus demonstrates the rigor of true compassion: to love one's neighbor means to love the one you have been taught to hate.

Section 230 invokes the vision of the Good Samaritan, but it is used to shield its opposite: the deliberately indifferent, the selfish, and the evil. Reforming the law to truly reward compassion and responsibility is the only way to assure that the Internet's tremendous potential to promote human flourishing is not limited to one's own tribe, but extends to the most vulnerable among us.

[18] *Luke* 10:30–37 (New International Version).

HERRICK V GRINDR: Why Section 230 Must Be Fixed[1]

BY CARRIE GOLDBERG

For two and a half years, I fought in court for the gay dating app Grindr to bear responsibility for the harms my client Matthew Herrick endured because of its defective product. In October, 2019 the Supreme Court denied the petition for a writ of certiorari my co-counsel Tor Ekeland and I filed against Grindr. The district court's decision marked the most extravagant interpretation of Section 230 immunity in the law's now 24 years.

The question was whether the immunity provided to platforms by Section 230 of the Communications Decency Act has any meaningful limits at all. *Herrick v. Grindr* is a civil lawsuit born from the urgent need for immediate help in a life or death situation. While the goal of most Section 230 cases—and litigations in general—is financial compensation for past injuries, Matthew's suffering was ongoing. Matthew's ex-boyfriend, Oscar Juan Carlos Gutierrez, was impersonating him on Grindr and sending men to Matthew's home to have sex with him.

It all started one evening in late October 2016, right before Halloween. Matthew had been sitting on the front stoop of his New York City apartment, smoking a cigarette, when a stranger called to him from the sidewalk and started heading up the steps toward him. The stranger's tone was friendly and familiar. But Matthew had never met this guy before. "I'm sorry," he said. "Do I know you?"

The stranger raised his eyebrows and pulled his phone from his back pocket. "You were just texting to me, dude," he replied, holding out his phone for Matthew to see. On the screen was a profile from the gay dating app Grindr, featuring a shirtless photo of Matthew standing in his kitchen, smiling broadly.

The stranger kept holding up his phone, insisting Matthew had invited him over for sex. But Matthew knew the profile wasn't his. Finally, the stranger became exasperated and left. "Fucking liar!" he shouted in Matthew's direction as he walked away. "You're an asshole!"

Rattled, Matthew went back inside. A few minutes later, he heard his buzzer ring. It was another man insisting that he, too, had made a sex date with Matthew. Two more men showed up that day. And three others came calling the next. "Matt!" they'd holler from the sidewalk, or they'd lean on the buzzer expecting to be let in. At first the strangers only went to his apartment, but by the end of the week a steady stream of men was showing up at the restaurant where Matthew worked as well. Some were in their 20s,

---

[1] Editor's note: This piece is in part a modified excerpt from the author's book, *"Nobody's Victim: Fighting Psychos, Stalkers, Pervs, and Trolls,"* Penguin Random House 2019. A version was published on lawfareblog.com https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed

others much older. A few arrived in business suits, as though on the way to the office. Others were twitchy and sweaty, looking like they'd been up all night getting high. They'd stalk him at work and at home, all hours of the day and night, each one convinced Matthew had invited him over for sex.

He was pretty sure he knew who was behind the attack: Gutierrez, his ex. The pair had met more than a year prior, on Grindr, and dated for 11 months. As time wore on, Gutierrez became increasingly jealous and clingy, accusing Matthew of cheating and doing things like showing up at Matthew's job and refusing to leave. Eventually, Matthew couldn't take it anymore; the pair broke up. The week after he ended his relationship with Gutierrez, strange men began showing up at Matthew's door.

The impersonating profile sent men for fisting, orgies and aggressive sex. In the direct messages, the strangers were told that Matt's resistance was part of the fantasy. It seemed clear to me that Gutierrez was endeavoring to do more than harass and frighten Matthew. He appeared to be trying to recruit unwitting accomplices to perpetrate sexual assaults.

Like many of my clients, before coming to see me Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct. The officers dutifully took down his information but didn't seem to understand the danger he was in.

By the time Matthew came to me for help, the Manhattan district attorney opened an investigation and he'd gotten a family court "stay away" order, but neither was stopping the traffic of strangers coming to his home and work for sex. He also did everything he could to get the imposter profiles taken down. He directly contacted Grindr and its competitor Scruff, which Matthew's ex was also using to impersonate him. In their terms of service, both companies explicitly prohibit the use of their products to impersonate, stalk, harass or threaten. Scruff, the smaller of the two companies, responded to Matthew immediately. It sent him a personal email expressing concern, took down the fake accounts, and blocked Gutierrez's IP address, effectively banning him from the app. When Gutierrez started impersonating Matthew on Jack'd, yet another gay dating app, that company also banned Gutierrez from using its platform to harass Matthew. But Grindr took a different approach: It did absolutely nothing.

In all, about 50 separate complaints were made to the company reporting the fake profiles, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report."

Over the course of ten months more than 1,400 men, as many as 23 in a day, arrived in person at Matthew's home and job.

Grindr is a wildly successful company. In 2018, the dating app reportedly had more than three million users in 234 countries. Like most social media companies, Grindr operates, in large part, as an advertising platform. The free content and services these platforms provide—porn, photo sharing, direct messaging, emailing, shopping, news, -

dating—are really just lures to get people to show up so the companies can collect data about what users buy, who they're friends with and where they're going, and use that information to advertise. Grindr prides itself on its state-of-the-art geolocative feature, which can pinpoint a user's exact location, allowing users to match with others in their vicinity. This is how they rake in advertising revenue—by customizing the ads that users see based on nearby businesses.

Even though Grindr's terms of service state that Grindr can remove any profile and deny anybody the use of their product at the company's discretion, they refused to help. After Matthew's approximately 50 pleas to Grindr for help were ignored, we sued Grindr in New York State Supreme Court, New York County, and obtained immediate injunctive relief requiring that Grindr ban Gutierrez.

It's not clear exactly how Gutierrez was exploiting Grindr to send the strangers to Matthew—it might have been through a spoofing app that worked with Grindr's geolocation software or something more technical. But the strangers who came to Matthew said they were sent through the Grindr app and would show Matthew the fake profiles with his pictures, geolocation maps showing how far away they were from Matthew, and direct messages telling them which buzzer to ring and what kind of sex Matthew was eager to have.

I didn't need to explain on a technical level how Grindr was being used against Matthew at this stage of the litigation; that's what discovery is for. What we knew is that Grindr was in an exclusive role to help stop Matthew's hell, given law enforcement was too slow and Gutierrez had been deterred by neither arrests nor orders of protection.

I knew from the start that Grindr would claim it was immune from liability pursuant to Section 230 of the Communications Decency Act, which states that "[n]o 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."

So I made sure not to sue Grindr for traditional publication torts like defamation. That is, I was not suing them for any words that Gutierrez said on the profiles or communications he'd made on the app. Instead, I tried something new—I sued Grindr using traditional product liability torts. I argued that Grindr is a defectively designed and manufactured product insofar as it was easily exploited—presumably by spoofing apps available from Google and Apple—and didn't have the ability, according to the courtroom admissions of Grindr's own lawyers, to identify and exclude abusive users. For a company that served millions of people globally and used geolocating technology to direct those people into offline encounters, it was an arithmetic certainty that at least some of the time the product would be used by abusers, stalkers, predators and rapists. Failing to manufacture the product with safeguards for those inevitabilities, I argued, was negligent.

On Feb. 8, 2017, Grindr filed a notice of removal from state court to the Southern District of New York. Our temporary restraining order requiring that Grindr ban Gutierrez from its services expired as a matter of law 14 days after the removal—but

when we moved to extend the order, Judge Valerie Caproni denied the extension. Judge Caproni felt our underlying case lacked merit because she suspected Grindr was immune from liability pursuant to the Communications Decency Act, arguing that our claims depended on information provided by another information content provider. If not for Matthew's ex using the app, she reasoned, none of this would have happened to Matthew. She reduced all the harm as flowing from Gutierrez's actions, not Grindr's, and therefore reasoned that the company was immune from liability and had no obligation to Matthew. In April and May of 2017, Grindr and its holding companies filed motions to dismiss our claims. At the time, Matthew's ex was continuing to relentlessly use the app to send strangers to his home and job—a fact the court knew.

We argued in our opposition papers that because we were suing Grindr for its own product defects and operational failures—and not for any content provided by Matthew's ex—Grindr was not eligible to seek safe harbor from Section 230. To rule against Matthew would set a dangerous precedent, establishing that as long as a tech company's product was turned to malicious purposes by a user, no matter how foreseeable the malicious use, that tech company was beyond the reach of the law and tort system.

Nevertheless, on Jan. 25, 2018 Judge Caproni dismissed our complaint entirely. All but a copyright claim was dismissed with prejudice, meaning that even if Matthew learned new information to support his claims, he could not amend his complaint.

Matthew's case was thrown out before we'd even gotten our foot in the door—even though dismissal at the motion to dismiss stage is supposed to be reserved for situations where a complaint is defective on its face, while ours was a detailed, thorough 43 pages and well-pleaded. The judge relied on Grindr's immunity under Section 230.

To our disappointment, on March 27, 2019 the Second Circuit issued a summary order affirming the district court's dismissal of the complaint. On April 11, we filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. On May 9, that too was denied. In October 2019, our writ for certiorari, also was denied. It was the end of the road for *Herrick v Grindr*.

The Supreme Court has never ruled on the proper scope of Section 230. As Matthew's case demonstrates, this is a matter of life or death for victims of stalking and violence caused and exacerbated by computer technologies unimagined when Congress passed the law in 1996. Decades ago, lawmakers had this pie-in-the-sky idea that internet companies would monitor content their users uploaded to protect the rest of us. What's become painfully apparent, and arguably should have been obvious, is that without the threat of legal liability hanging over their heads, companies like Grindr really don't care about who gets hurt.

This debate is muddied by the fact that the federal and state court decisions in this country lack clarity and are often contradictory as to the Communications Decency Act's proper scope, which has led many courts to create an almost absolute immunity for internet companies for their tortious conduct. Courts do this, as the lower courts did in

our case, with overbroad definitions of what constitutes an "interactive computer service" and what constitutes information provided by a different "information content provider." These are, or should be, fact-intensive inquiries, but if cases are dismissed on motions to dismiss for failure to state a claim, as ours was—before discovery and without defendants even needing to plead Section 230 immunity—plaintiffs will never have a chance.

This case is not only about justice for Matthew. We are fighting for future victims' rights to sue any tech company that knowingly, or recklessly, aids their abusers and causes victims harm. What's more, determining the scope of the Communications Decency Act is a crucial component of society's current debate about the responsibility internet companies bear for the harm their technologies arguably propagate. This could be no truer than this moment when mass shooters are radicalizing and posting propaganda on the likes of 8chan, mentally ill people with restraining orders are murdering with weapons purchased from online gun sellers, and individuals with warrants out for their arrests are killing people they match with on dating apps and torturing individuals they meet in the back seats of pooled rideshares.

Most industries would also like to be free from liability for harms their product, services or staff could cause their customers. But the reality is, legal responsibility for one's products and services is the cost of doing business and drives safety innovation.

If our courts won't rein in Section 230, our government must act. We need the following changes made to Section 230:

- Injunctive relief to help in emergency cases like Matthew's where the plaintiff is suffering imminent harm.
- Section 230 immunity must be an affirmative defense that defendants must plead, rather than leave it to judges to play "computer scientist" in 12(b)(6) decisions.
- An ICS can be held responsible for the third-party ICP if the ICS has
    - Breached its own terms of services regarding;
    - Constructive notice of the specific harm and damages; or
    - Receives money from the third-party ICP.
- Define "information content" to include only speech-based content
- Limit immunity to only publication-related torts like obscenity and defamation.

All in all, Section 230 is a government subsidy to the industry least in need and least deserving of it. It's time to fix 230—and if the Supreme Court won't do it, legislators must. And in the meantime, the Department of Justice, should more freely prosecute federal crimes, such as the hosting of child sexual abuse images, against platforms and their executives.

Statement of Prof. Eric Goldman[*]

U.S. Department of Justice Workshop, "Section 230: Nurturing Innovation or Fostering Unaccountability?"

February 13, 2020

Several members of Congress have recently expressed interest in reforming 47 U.S.C. § 230 ("Section 230"), the foundational law that protects Internet services from civil and state criminal liability[1] for user-generated content. Section 230's perceived costs—which are real—are frequently highlighted, but Section 230's benefits often receive less attention. This statement highlights four major benefits that Section 230 produces for the United States and all Internet users.

1. Job Creation: The Internet industry is one of our economy's brightest spots, and Section 230 plays an essential role in powering its economic engine. A 2017 NERA Economic Consulting study indicated that weakening Section 230 and other Internet safe harbors would eliminate over 425,000 jobs and decrease U.S. GDP by $44 billion annually.[2]

2. Promoting Small Businesses: Section 230 deters frivolous and costly lawsuits, and it speeds up resolution when such lawsuits are brought.[3] A 2019 Engine study showed how these procedural advantages can save small businesses tens, or even hundreds of thousands, of dollars of defense costs per bogus lawsuit.[4] These savings reduce the exposure of small online businesses to ruinous litigation and encourage the next generation of start-up businesses aspiring to disrupt the current Internet incumbents.

3. Market Efficiency: Section 230 strengthens markets in at least two ways. First, Section 230 has spurred the creation of new online marketplaces that previously were infeasible due to high transaction costs. Second, Section 230 played an essential role in the emergence of consumer reviews, which in turn improve consumer decision-making[5] and steer consumers towards quality businesses and away from shady ones.

4. Fostering Free Speech for All: Section 230 helps all speakers reach a global audience, including speakers from marginalized communities who historically have been excluded from public discourse. This has led to the proliferation of information supporting communities that previously lacked adequate informational resources. As Elliot Harmon of the Electronic Frontier Foundation wrote, "[Section 230 is] a gift to rural LGBTQ teenagers who depend every day on the safety of their online communities. It's a gift to activists around the world using the internet

---

[*] Professor of Law and Co-Director of the High Tech Law Institute, Santa Clara University School of Law. Website: http://www.ericgoldman.org. Email: egoldman@gmail.com.

[1] Section 230 does not apply to federal criminal prosecutions.

[2] https://cdn1.internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf

[3] https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1074&context=ndlr_online

[4] https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c6c5649e2c483b67d518293/1550603849958/Section+230+cost+study.pdf

[5] For example, 85% of consumers said they would be less likely to buy things online without consumer reviews; and 79% said that good consumer reviews got them to buy a product they were otherwise undecided about. https://internetassociation.org/files/ia_best-of-the-internet-survey_06-26-2019_content-moderation/

to document human rights abuses….Section 230's real beneficiaries are the historically disadvantaged communities that would risk exclusion from online discussions without it."[6]

In sum, despite its costs, Section 230 has an extraordinarily positive impact on our society. Many Americans interact with and benefit from Section 230-facilitated services literally on an hourly or even minute-by-minute basis. As regulators take a closer look at Section 230, I urge them to avoid unanticipated or unwanted consequences that might negate the critical benefits we currently derive from Section 230.

* * *

To supplement my statement, I attach a July 2019 statement of principles, "Liability for User-Generated Content Online," signed by 53 individuals and 28 organizations.

[6] https://thehill.com/opinion/technology/458227-in-debate-over-internet-speech-law-pay-attention-to-whose-voices-are

Liability for User-Generated Content Online:
Principles for Lawmakers
July 11, 2019

Policymakers have expressed concern about both harmful online speech and the content moderation practices of tech companies. Section 230, enacted as part of the bipartisan Communications Decency Act of 1996, says that Internet services, or "intermediaries," are not liable for illegal third-party content except with respect to intellectual property, federal criminal prosecutions, communications privacy (ECPA), and sex trafficking (FOSTA). Of course, Internet services remain responsible for content they themselves create.

As civil society organizations, academics, and other experts who study the regulation of user-generated content, we value the balance between freely exchanging ideas, fostering innovation, and limiting harmful speech. Because this is an exceptionally delicate balance, Section 230 reform poses a substantial risk of failing to address policymakers' concerns and harming the Internet overall. We hope the following principles help any policymakers considering amendments to Section 230.

Principle #1: Content creators bear primary responsibility for their speech and actions.

Content creators—including online services themselves—bear primary responsibility for their own content and actions. Section 230 has never interfered with holding content creators liable. Instead, Section 230 restricts only who can be liable for the harmful content created by others.

Law enforcement online is as important as it is offline. If policymakers believe existing law does not adequately deter bad actors online, they should (i) invest more in the enforcement of existing laws, and (ii) identify and remove obstacles to the enforcement of existing laws. Importantly, while anonymity online can certainly constrain the ability to hold users accountable for their content and actions, courts and litigants have tools to pierce anonymity. And in the rare situation where truly egregious online conduct simply isn't covered by existing criminal law, the law could be expanded. But if policymakers want to avoid chilling American entrepreneurship, it's crucial to avoid imposing criminal liability on online intermediaries or their executives for unlawful user-generated content.

Principle #2: Any new intermediary liability law must not target constitutionally protected speech.

The government shouldn't require—or coerce—intermediaries to remove constitutionally protected speech that the government cannot prohibit directly. Such demands violate the First Amendment. Also, imposing broad liability for user speech incentivizes services to err on the side of taking down speech, resulting in overbroad censorship—or even avoid offering speech forums altogether.

Principle #3: The law shouldn't discourage Internet services from moderating content.

To flourish, the Internet requires that site managers have the ability to remove legal but objectionable content—including content that would be protected under the First Amendment from censorship by the government. If Internet services could not prohibit harassment, pornography, racial slurs, and other lawful but offensive or damaging material, they couldn't facilitate civil discourse. Even when Internet services have the ability to moderate content, their moderation efforts will always be imperfect given the vast scale of even relatively small sites and the speed with which content is posted. Section 230 ensures that Internet services can carry out this socially beneficial but error-prone work without exposing themselves to increased liability; penalizing them for imperfect content moderation or second-guessing their decision-making will only discourage them from trying in the first place. This vital principle should remain intact.

Principle #4: Section 230 does not, and should not, require "neutrality."

Publishing third-party content online never can be "neutral."[1] Indeed, every publication decision will necessarily prioritize some content at the expense of other content. Even an "objective" approach, such as presenting content in reverse chronological order, isn't neutral because it prioritizes recency over other values. By protecting the prioritization, de-prioritization, and removal of content, Section 230 provides Internet services with the legal certainty they need to do the socially beneficial work of minimizing harmful content.

Principle #5: We need a uniform national legal standard.

Most Internet services cannot publish content on a state-by-state basis, so state-by-state variations in liability would force compliance with the most restrictive legal standard. In its current form, Section 230 prevents this dilemma by setting a consistent national standard—which includes potential liability under the uniform body of federal criminal law. Internet services, especially smaller companies and new entrants, would find it difficult, if not impossible, to manage the costs and legal risks of facing potential liability under state civil law, or of bearing the risk of prosecution under state criminal law.

Principle #6: We must continue to promote innovation on the Internet.

Section 230 encourages innovation in Internet services, especially by smaller services and startups who most need protection from potentially crushing liability. The law must continue to protect intermediaries not merely from liability, but from having to defend against excessive, often-meritless suits—what one court called "death by ten thousand duck-bites." Without such protection, compliance, implementation, and litigation costs could strangle smaller companies even before they emerge, while larger, incumbent technology companies would be much better positioned to absorb these costs. Any amendment to Section 230 that is calibrated to what might be possible for the Internet giants will necessarily mis-calibrate the law for smaller services.

[1] We are addressing neutrality only in content publishing. "Net neutrality," or discrimination by Internet access providers, is beyond the scope of these principles.

Principle #7: Section 230 should apply equally across a broad spectrum of online services.

Section 230 applies to services that users never interact with directly. The further removed an Internet service—such as a DDOS protection provider or domain name registrar—is from an offending user's content or actions, the more blunt its tools to combat objectionable content become. Unlike social media companies or other user-facing services, infrastructure providers cannot take measures like removing individual posts or comments. Instead, they can only shutter entire sites or services, thus risking significant collateral damage to inoffensive or harmless content. Requirements drafted with user-facing services in mind will likely not work for these non-user-facing services.

* * *

Individual Signatories
Affiliations are for identification purposes only

1. Prof. Susan Ariel Aaronson, Elliott School of International Affairs, George Washington University
2. Prof. Enrique Armijo, Elon University School of Law
3. Prof. Thomas C. Arthur, Emory University School of Law
4. Farzaneh Badiei, Internet Governance Project, Georgia Institute of Technology (research associate)
5. Prof. Derek Bambauer, University of Arizona James E. Rogers College of Law
6. Prof. Jane Bambauer, University of Arizona James E. Rogers College of Law
7. Prof. Annemarie Bridy, University of Idaho College of Law
8. Prof. Anupam Chander, Georgetown Law
9. Lydia de la Torre, Santa Clara University School of Law (fellow)
10. Prof. Sean Flynn, American University Washington College of Law
11. Prof. Brian L. Frye, University of Kentucky College of Law
12. Prof. Elizabeth Townsend Gard, Tulane Law School
13. Prof. Jim Gibson, University of Richmond, T. C. Williams School of Law
14. Prof. Eric Goldman, Santa Clara University School of Law
15. Prof. Edina Harbinja, Aston University UK
16. Prof. Gus Hurwitz, University of Nebraska College of Law
17. Prof. Michael Jacobs, DePaul University College of Law (emeritus)
18. Daphne Keller, Stanford Center for Internet and Society
19. Christopher Koopman, Center for Growth and Opportunity, Utah State University
20. Brenden Kuerbis, Georgia Institute of Technology, School of Public Policy (researcher)
21. Prof. Thomas Lambert, University of Missouri School of Law
22. Prof. Stacey M. Lantagne, University of Mississippi School of Law
23. Prof. Sarah E. Lageson, Rutgers University-Newark School of Criminal Justice
24. Prof. Jyh-An Lee, The Chinese University of Hong Kong
25. Prof. Mark A. Lemley, Stanford Law School
26. Thomas M. Lenard, Senior Fellow and President Emeritus, Technology Policy Institute
27. Prof. David Levine, Elon University School of Law
28. Prof. Yvette Joy Liebesman, Saint Louis University School of Law

29. Yong Liu, Hebei Academy of Social Sciences (researcher)
30. Prof. Katja Weckstrom Lindroos UEF Law School, University of Eastern Finland
31. Prof. John Lopatka, Penn State Law
32. Prof. Daniel A. Lyons, Boston College Law School
33. Geoffrey A. Manne, President, International Center for Law & Economics; Distinguished Fellow, Northwestern University Center on Law, Business & Government
34. Prof. Stephen McJohn, Suffolk University Law School
35. David Morar, Elliott School of International Affairs, George Washington University (visiting scholar)
36. Prof. Frederick Mostert, The Dickson Poon School of Law, King's College London
37. Prof. Milton Mueller, Internet Governance Project, Georgia Institute of Technology
38. Prof. Ira S. Nathenson, St. Thomas University (Florida) School of Law
39. Prof. Christopher Newman, Antonin Scalia Law School at George Mason University
40. Prof. Fred Kennedy Nkusi, UNILAK
41. David G. Post, Beasley School of Law, Temple University (retired)
42. Prof. Betsy Rosenblatt, UC Davis School of Law (visitor)
43. Prof. John Rothchild, Wayne State University Law School
44. Prof. Christopher L. Sagers, Cleveland-Marshall College of Law
45. David Silverman, Lewis & Clark Law School (adjunct)
46. Prof. Vernon Smith, George L. Argyros School of Business and Economics & Dale E. Fowler School of Law, Chapman University
47. Prof. Nicolas Suzor, QUT Law School
48. Prof. Gavin Sutter, CCLS, School of Law, Queen Mary University of London
49. Berin Szóka, President, TechFreedom
50. Prof. Rebecca Tushnet, Harvard Law School
51. Prof. Habib S. Usman, American University of Nigeria
52. Prof. John Villasenor, Electrical Engineering, Public Policy, and Law at UCLA
53. Prof. Joshua D. Wright, Antonin Scalia Law School at George Mason University

Institutional Signatories

1. ALEC (American Legislative Exchange Council) Action
2. Americans for Prosperity
3. Center for Democracy & Technology
4. Competitive Enterprise Institute
5. Copia Institute
6. Freedom Foundation of Minnesota
7. FreedomWorks
8. Information Technology and Innovation Foundation
9. Innovation Economy Institute
10. Innovation Defense Foundation
11. Institute for Liberty
12. The Institute for Policy Innovation (IPI)
13. International Center for Law & Economics
14. Internet Governance Project
15. James Madison Institute

16. Libertas Institute
17. Lincoln Network
18. Mississippi Center for Public Policy
19. National Taxpayers Union
20. New America's Open Technology Institute
21. Organization for Transformative Works
22. Pelican Institute
23. Rio Grande Foundation
24. R Street Institute
25. Stand Together
26. Taxpayers Protection Alliance
27. TechFreedom
28. Young Voices

CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology respectfully submits these comments to the Department of Justice's Section 230 Workshop Afternoon Roundtable. Since it was founded in 1994, CDT has been advocating for civil liberties and human rights in technology policy in the US and around the world. We have been engaged in the debates around the liability of Internet intermediaries for user-generated content since the very beginning, advocating for the proposal by Representatives Cox and Wyden that became Section 230,[1] and joining the lawsuit that led the Supreme Court in 1997 to strike down the majority of the Communications Decency Act in the case *Reno v. ACLU*.[2] For the past 25 years, CDT has worked to promote law and policy that respects individuals' rights to access information and to speak online.

In these brief comments, we address three topics: the limits the First Amendment places on government officials' ability to regulate content moderation; the risk that changes to the Section 230 framework could hinder online services' ability to effectively tackle abuse of their platforms; and a set of principles that should guide policy discussions about intermediary liability.

The First Amendment limits the government's ability to regulate speech, both directly and via intermediaries.

The First Amendment provides strong protections for individuals' rights to speak, access information, and freely associate online. Government officials are limited in their ability to restrict speech and legislative attempts to regulate online content, both directly and through regulation of intermediaries, have often been unconstitutionally vague, overbroad, or lacked the narrow tailoring required by the First Amendment. In the late 1990s and early 2000s, Congress passed a variety of laws aimed at protecting children online; most of these, including the Communications Decency Act,[3] the Child Pornography Prevention Act,[4] and the Child Online Protection Act,[5] were challenged as violations of the First Amendment and ultimately enjoined by the Supreme Court. One notable exception was the Children's Internet Protection Act (CIPA), which conditioned federal E-Rate funding for schools and libraries on those institutions implementing content filters to limit minors' access to pornography online. This law was also challenged on First Amendment grounds, but was upheld by the Supreme Court on the basis that adults were easily able to ask for the filters to be deactivated.[6]

Courts have also found a variety of efforts to regulate speech via intermediaries to be incompatible with the First Amendment. In *Brown v. Entertainment Merchants Association*, the Supreme Court struck

[1] Center for Democracy & Technology, Policy Post (Aug. 4, 1995), *available at* http://groups.csail.mit.edu/mac/classes/6.805/legislation/cdt-cox-wyden.txt.
[2] Reno v. ACLU, 521 US 844 (1997).
[3] Struck down in Reno v. ACLU, 521 US 844 (1997).
[4] Struck down in Ashcroft v. Free Speech Coalition (2002).
[5] Enjoined in ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008) (cert denied).
[6] United States v. American Library Association, 539 US 194 (2003).

down a law requiring retailers to apply content-rating labels to video games and banning the sale of violent video games to minors.[7] In 2004, the Eastern District of Pennsylvania enjoined a law requiring service providers to block access to websites that appeared on a blacklist developed by the state AG.[8] SESTA-FOSTA, Congress's most recent effort to regulate online content, and first attempt to amend Section 230, is currently facing a First Amendment challenge by organizations and individuals who fear prosecution and face indirect censorship of their lawful speech.[9]

A key dynamic for discussions of intermediary liability for user-generated content is that government officials cannot require or coerce intermediaries into suppressing speech that the government could not regulate directly. Pressure by law enforcement officials, aimed at coercing private actors to take steps that will ultimately censor protected speech, has been found to function as government action that violates the First Amendment.[10] "Incentives" for intermediaries to restrict speech can also be a form of governmental coercion of private actors to censor, especially if providers truly have no choice but to pursue the incentive. Turning the protections of Section 230 into this type of incentive would create this coercive effect. As we described in a recent blog post, "Section 230's liability protections have been essential to the development of the internet as a medium for free expression and access to information. The intermediaries who host, transmit, link to, and otherwise facilitate our speech online simply cannot afford the risk in enabling millions, or even just thousands, of individuals to upload whatever speech they like."[11] Making these key liability protections "incentives" that must be earned would present a false choice to service providers, who would not be able to bear the risk.

Moreover, government involvement in "voluntary" or self-regulatory initiatives may convert these efforts into government action that will face constitutional scrutiny. We have already seen an example of this in the Fourth Amendment context, in *US v Ackerman*.[12] That case concerned the National Center for Missing and Exploited Children, which receives federal funding and which is the recipient of the reports of apparent child sexual abuse material that online service providers are required by law to provide. In the *Ackerman* case, then-Judge Gorsuch wrote that NCMEC was acting as a governmental entity or an agent of the government, and so its searches of an individual's emails and attached files required a warrant. (Indeed, CDT warned about some of the risks of federalizing NCMEC when Congress did so in 2008.)[13] Government efforts to leverage companies' content moderation systems to pursue content regulation would raise similar government-action concerns, particularly if that regulation would go beyond what the government could pursue directly in law.

---

[7] Brown v Entertainment Merchants Association, 564 US 786 (2011).
[8] Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004).
[9] *See* Woodhull Freedom Foundation v. US, No. 18-5298https://www.cadc.uscourts.gov/internet/opinions.nsf/CD2E207B01AAFA4F852584F90053EE7D/$file/18-5298-1825427.pdf.
[10] Backpage.com, LLC v. Dart, 807 F.3d 229 (7th Cir. 2015).
[11] https://cdt.org/insights/privacy-free-expression-and-security-threatened-by-graham-proposal/
[12] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).
[13] https://cdt.org/insights/beyond-the-bailout-congress-passes-a-flurry-of-child-safety-bills/.

Prescriptive regulation may hinder service providers' ability to address abusive uses of their services.

Section 230 was originally conceived to avoid the "moderator's dilemma,"[14] in which service providers who took steps to remove abusive posts faced much greater legal risk, under traditional publisher liability, than those who allowed anything and everything to remain online. Section 230 removes this disincentive against moderating content by shielding service providers from liability for their decisions both to remove and to leave up content. This protection has been crucial to the development of content moderation systems across services of all sizes, and is key to enabling many different robust and functional online communities.

As discussed above, government officials are limited in what speech they can regulate. Online service providers have much greater flexibility than the government does in how they moderate user-generated content. Many online service providers, including social media companies, website operators, forum administrators, news sites, and other services that provide a space for users' speech, have content policies that are more restrictive than the First Amendment would allow the law to be. Such policies can, perhaps counterintuitively, be instrumental in ensuring that an online discussion forum remains a constructive and enjoyable opportunity for different individuals to share their opinions and experiences.

Different services rely on different approaches to content moderation in order to best serve their communities and to fight abuse; not every "best practice" will work on every service.
The nature of the primary content on a site (e.g. text, images, videos, live-streaming) will affect the availability and effectiveness of tools that can be used to moderate that content—the ephemeral nature of real-time voice and live video, for example, can make use of tools designed for text-based content moderation difficult if not impossible to use.[15] Certain moderation techniques depend on choices the service has made about site architecture, internal policies, and the empowerment tools made available to users. Sites that incorporate volunteer moderators, such as Reddit, Twitch, and Facebook Groups, have found that their most effective method of discouraging problematic behavior is to "engage personally during incidents to set an example for future interactions," rather than turning to content bans, algorithms, or filters.[16] And techniques that work well at one point in time can become less effective as users find ways to circumvent elements of a moderation system. In some online

[14] Cf. Eric Goldman, Testimony before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology, Hearing on "Latest Developments in Combating Online Sex Trafficking", *available at* https://docs.house.gov/meetings/IF/IF16/20171130/106657/HHRG-115-IF16-Wstate-GoldmanE-20171130-U51.pdf.

[15] Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Article 55. Publication date: November 2019. (pp 4-5)

[16] Seering, J., Wang, T., Yoon, J., & Kaufman, G. (2019). Moderator engagement and community development in the age of algorithms. New Media & Society, 21(7), 1418. https://doi.org/10.1177/1461444818821316.

communities, users have increasingly avoided using hashtags, recognizing that if they avoid labelling their content in a particular way, it can be easier to bypass text-based filtering systems.[17]

In short, there is no one-size-fits-all approach to content moderation. What is effective for one size, type, or user-base of a service may not work well for another, and what is effective will change over time. Regulation that constrains flexibility in content moderation (either by increasing the legal risk of moderation or by mandating content regulation that is contrary to the First Amendment) could take crucial tools for combating abuse off the table.

Principles for Liability for User-Generated Content

In July 2019, CDT joined a group of 27 advocacy organizations and 50 legal scholars in developing a set of principles for policymakers to consider when evaluating liability frameworks for user-generated content.[18] (CDT launched a similar set of principles, aimed at policymakers and the specific legal framework of the European Union.)[19] We include those documents as an appendix, here, and would briefly emphasize a few key points about intermediary liability frameworks in general:

The Internet has enabled user-generated content to be published worldwide at a scale previously unknown in human history. Hosting or otherwise enabling users' speech is unlike any prior form of publishing, and applying traditional publisher liability to online intermediaries creates precisely the wrong incentives to respond to abuse. Any intermediary liability framework needs to grapple first and foremost with the substantially different nature and scale of publishing online speech.

Section 230 provides a very practical, but deeply important, protection for freedom of speech online by enabling service providers to terminate lawsuits over user-generated content early on in the case. Intermediaries have a clear understanding about the (low) legal risk they face in facilitating user-generated content; as we have seen countless times, the moment a user's post becomes the source of potential liability, intermediaries are more likely to remove the content than take on the risk. Any intermediary liability framework needs to account for the threat of high volumes of lawsuits—akin to a heckler's veto—that will render it impossible for many intermediaries to interact with users' speech.

[17] Chancellor S, Pater JA, Clear T, et al. (2016) #thyghgapp: Instagram content moderation and lexical variation in pro-eating disorder communities. In: Proceedings of the 19th ACM conference on computer–supported cooperative work & social computing, CSCW '16. Available at: http://www.munmund.net/pubs/cscw16_thyghgapp.pdf

[18] https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical

[19] https://cdt.org/insights/nine-principles-for-future-eu-policymaking-on-intermediary-liability/

Finally, we would note that CDT has advocated for many years for improvements to online service providers' content moderation systems.[20] We have joined with other free expression advocates to develop the Santa Clara Principles on transparency and accountability in content moderation[21] and have continually emphasized the need for service providers to give their users clear notice about when and how their content is restricted. We know that errors—both false positives and false negatives—are inevitable as providers moderate content at scale, which is why it is so essential for them to provide opportunities to appeal decisions and seek remedies for mistakes. We have cautioned against the proliferation of automated content analysis in moderation systems, as these tools risk perpetuating and amplifying biases and fundamentally changing who has the opportunity to speak online.[22] And we have pushed for greater transparency from these service providers, in their response to government demands for content restriction and user data,[23] in their enforcement of their own Terms of Service,[24] and in providing access to data for researchers to enable independent evaluation of the effects and consequences of their content moderation systems.[25]

We are deeply committed to pursuing a world in which both companies and governments are accountable to the people whose speech and access to information rights they are affecting. But this accountability must work within the constraints of the First Amendment, and with a thorough understanding of the unique dynamics of online speech.

---

[20] Berkman Center and CDT, Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users (2011), https://www.cdt.org/wp-content/uploads/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf.
[21] https://santaclaraprinciples.org/
[22] Natasha Duarte, Emma Llanso, Anna Loup, Mixed Messages: The Limits of Automated Social Media Content Analysis (2017), https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.
[23] Emma Llanso and Susan Morgan, Getting Specific About Transparency, Privacy, and Free Expression Online (2014), https://cdt.org/insights/getting-specific-about-transparency-privacy-and-free-expression-online/; Emma Llanso, Twitter Transparency Report Shines a Light on Variety of Ways Governments Seek to Restrict Speech Online (2017), https://cdt.org/insights/twitter-transparency-report-shines-a-light-on-variety-of-ways-governments-seek-to-restrict-speech-online/.
[24] Liz Woolery, Companies Finally Shine a Light Onto Content Moderation Practices (2018), https://cdt.org/insights/companies-finally-shine-a-light-into-content-moderation-practices/.
[25] Liz Woolery, Three Lessons in Content Moderation from New Zealand and Other High Profile Tragedies (2018), https://cdt.org/insights/three-lessons-in-content-moderation-from-new-zealand-and-other-high-profile-tragedies/.

Liability for User-Generated Content Online
Principles for Lawmakers
July 11, 2019

Policymakers have expressed concern about both harmful online speech and the content moderation practices of tech companies. Section 230, enacted as part of the bipartisan Communications Decency Act of 1996, says that Internet services, or "intermediaries," are not liable for illegal third-party content except with respect to intellectual property, federal criminal prosecutions, communications privacy (ECPA), and sex trafficking (FOSTA). Of course, Internet services remain responsible for content they themselves create.

As civil society organizations, academics, and other experts who study the regulation of user-generated content, we value the balance between freely exchanging ideas, fostering innovation, and limiting harmful speech. Because this is an exceptionally delicate balance, Section 230 reform poses a substantial risk of failing to address policymakers' concerns and harming the Internet overall. We hope the following principles help any policymakers considering amendments to Section 230.

***Principle #1*: Content creators bear primary responsibility for their speech and actions.**

Content creators—including online services themselves—bear primary responsibility for their own content and actions. Section 230 has never interfered with holding content creators liable. Instead, Section 230 restricts only who can be liable for the harmful content created *by others*.

Law enforcement online is as important as it is offline. If policymakers believe existing law does not adequately deter bad actors online, they should (i) invest more in the enforcement of existing laws, and (ii) identify and remove obstacles to the enforcement of existing laws. Importantly, while anonymity online can certainly constrain the ability to hold users accountable for their content and actions, courts and litigants have tools to pierce anonymity. And in the rare situation where truly egregious online conduct simply isn't covered by existing criminal law, the law could be expanded. But if policymakers want to avoid chilling American entrepreneurship, it's crucial to avoid imposing criminal liability on online intermediaries or their executives for unlawful user-generated content.

***Principle #2:* Any new intermediary liability law must not target constitutionally protected speech.**

The government shouldn't require—or coerce—intermediaries to remove constitutionally protected speech that the government cannot prohibit directly. Such demands violate the First Amendment. Also, imposing broad liability for user speech incentivizes services to err on the side of taking down speech, resulting in overbroad censorship—or even avoid offering speech forums altogether.

***Principle #3*: The law shouldn't discourage Internet services from moderating content.**

To flourish, the Internet requires that site managers have the ability to remove legal but objectionable content—including content that would be protected under the First Amendment from censorship by the government. If Internet services could not prohibit harassment, pornography, racial slurs, and other lawful but offensive or damaging material, they couldn't facilitate civil discourse. Even when Internet services have the ability to moderate content, their

moderation efforts will always be imperfect given the vast scale of even relatively small sites and the speed with which content is posted. Section 230 ensures that Internet services can carry out this socially beneficial but error-prone work without exposing themselves to increased liability; penalizing them for imperfect content moderation or second-guessing their decision-making will only discourage them from trying in the first place. This vital principle should remain intact.

***Principle #4*: Section 230 does not, and should not, require "neutrality."**

Publishing third-party content online never can be "neutral."[1] Indeed, every publication decision will necessarily prioritize some content at the expense of other content. Even an "objective" approach, such as presenting content in reverse chronological order, isn't *neutral* because it prioritizes recency over other values. By protecting the prioritization, de-prioritization, and removal of content, Section 230 provides Internet services with the legal certainty they need to do the socially beneficial work of minimizing harmful content.

***Principle #5*: We need a uniform national legal standard.**

Most Internet services cannot publish content on a state-by-state basis, so state-by-state variations in liability would force compliance with the most restrictive legal standard. In its current form, Section 230 prevents this dilemma by setting a consistent national standard—which includes potential liability under the uniform body of federal criminal law. Internet services, especially smaller companies and new entrants, would find it difficult, if not impossible, to manage the costs and legal risks of facing potential liability under state civil law, or of bearing the risk of prosecution under state criminal law.

***Principle #6*: We must continue to promote innovation on the Internet.**

Section 230 encourages innovation in Internet services, especially by smaller services and start-ups who most need protection from potentially crushing liability. The law must continue to protect intermediaries not merely from liability, but from having to defend against excessive, often-meritless suits—what one court called "death by ten thousand duck-bites." Without such protection, compliance, implementation, and litigation costs could strangle smaller companies even before they emerge, while larger, incumbent technology companies would be much better positioned to absorb these costs. Any amendment to Section 230 that is calibrated to what *might* be possible for the Internet giants will necessarily *mis*-calibrate the law for smaller services.

***Principle #7*: Section 230 should apply equally across a broad spectrum of online services.**

Section 230 applies to services that users never interact with directly. The further removed an Internet service—such as a DDOS protection provider or domain name registrar—is from an offending user's content or actions, the more blunt its tools to combat objectionable content become. Unlike social media companies or other user-facing services, infrastructure providers cannot take measures like removing individual posts or comments. Instead, they can only shutter entire sites or services, thus risking significant collateral damage to inoffensive or harmless content. Requirements drafted with user-facing services in mind will likely not work for these non-user-facing services.

---

[1] We are addressing neutrality only in content publishing. "Net neutrality," or discrimination by Internet access providers, is beyond the scope of these principles.

Individual Signatories

Affiliations are for identification purposes only

1. Prof. Susan Ariel Aaronson, Elliott School of International Affairs, George Washington University
2. Prof. Enrique Armijo, Elon University School of Law
3. Prof. Thomas C. Arthur, Emory University School of Law
4. Farzaneh Badiei, Internet Governance Project, Georgia Institute of Technology (research associate)
5. Prof. Derek Bambauer, University of Arizona James E. Rogers College of Law
6. Prof. Jane Bambauer, University of Arizona James E. Rogers College of Law
7. Prof. Annemarie Bridy, University of Idaho College of Law
8. Prof. Anupam Chander, Georgetown Law
9. Lydia de la Torre, Santa Clara University School of Law (fellow)
10. Prof. Sean Flynn, American University Washington College of Law
11. Prof. Brian L. Frye, University of Kentucky College of Law
12. Prof. Elizabeth Townsend Gard, Tulane Law School
13. Prof. Jim Gibson, University of Richmond, T. C. Williams School of Law
14. Prof. Eric Goldman, Santa Clara University School of Law
15. Prof. Edina Harbinja, Aston University UK
16. Prof. Gus Hurwitz, University of Nebraska College of Law
17. Prof. Michael Jacobs, DePaul University College of Law (emeritus)
18. Daphne Keller, Stanford Center for Internet and Society
19. Christopher Koopman, Center for Growth and Opportunity, Utah State University
20. Brenden Kuerbis, Georgia Institute of Technology, School of Public Policy (researcher)
21. Prof. Thomas Lambert, University of Missouri School of Law
22. Prof. Stacey M. Lantagne, University of Mississippi School of Law
23. Prof. Sarah E. Lageson, Rutgers University-Newark School of Criminal Justice
24. Prof. Jyh-An Lee, The Chinese University of Hong Kong
25. Prof. Mark A. Lemley, Stanford Law School
26. Thomas M. Lenard, Senior Fellow and President Emeritus, Technology Policy Institute
27. Prof. David Levine, Elon University School of Law
28. Prof. Yvette Joy Liebesman, Saint Louis University School of Law
29. Yong Liu, Hebei Academy of Social Sciences (researcher)
30. Prof. Katja Weckstrom Lindroos UEF Law School, University of Eastern Finland
31. Prof. John Lopatka, Penn State Law
32. Prof. Daniel A. Lyons, Boston College Law School
33. Geoffrey A. Manne, President, International Center for Law & Economics; Distinguished Fellow, Northwestern University Center on Law, Business & Government
34. Prof. Stephen McJohn, Suffolk University Law School
35. David Morar, Elliott School of International Affairs, George Washington University (visiting scholar)
36. Prof. Frederick Mostert, The Dickson Poon School of Law, King's College London
37. Prof. Milton Mueller, Internet Governance Project, Georgia Institute of Technology
38. Prof. Ira S. Nathenson, St. Thomas University (Florida) School of Law
39. Prof. Christopher Newman, Antonin Scalia Law School at George Mason University
40. Prof. Fred Kennedy Nkusi, UNILAK
41. David G. Post, Beasley School of Law, Temple University (retired)
42. Prof. Betsy Rosenblatt, UC Davis School of Law (visitor)
43. Prof. John Rothchild, Wayne State University Law School

44. Prof. Christopher L. Sagers, Cleveland-Marshall College of Law
45. David Silverman, Lewis & Clark Law School (adjunct)
46. Prof. Vernon Smith, George L. Argyros School of Business and Economics & Dale E. Fowler School of Law, Chapman University
47. Prof. Nicolas Suzor, QUT Law School
48. Prof. Gavin Sutter, CCLS, School of Law, Queen Mary University of London
49. Berin Szóka, President, TechFreedom
50. Prof. Rebecca Tushnet, Harvard Law School
51. Prof. Habib S. Usman, American University of Nigeria
52. Prof. John Villasenor, Electrical Engineering, Public Policy, and Law at UCLA
53. Prof. Joshua D. Wright, Antonin Scalia Law School at George Mason University

Institutional Signatories

1. ALEC (American Legislative Exchange Council) Action
2. Americans for Prosperity
3. Center for Democracy & Technology
4. Competitive Enterprise Institute
5. Copia Institute
6. Freedom Foundation of Minnesota
7. FreedomWorks
8. Information Technology and Innovation Foundation
9. Innovation Economy Institute
10. Innovation Defense Foundation
11. Institute for Liberty
12. The Institute for Policy Innovation (IPI)
13. International Center for Law & Economics
14. Internet Governance Project
15. James Madison Institute
16. Libertas Institute
17. Lincoln Network
18. Mississippi Center for Public Policy
19. National Taxpayers Union
20. New America's Open Technology Institute
21. Organization for Transformative Works
22. Pelican Institute
23. Rio Grande Foundation
24. R Street Institute
25. Stand Together
26. Taxpayers Protection Alliance
27. TechFreedom
28. Young Voices

CENTER FOR DEMOCRACY & TECHNOLOGY

Nine Principles for Future EU Policymaking on Intermediary Liability

Introduction

Many European policymakers and governments have concerns about the impact of several types of online content and user behaviour. These concerns are outlined in the UK Government White Paper on Online Harms. Policymakers worry about content that may be illegal, such as some forms of hate speech, and content that is posted with the intent to incite violence for ideological and/or religious reasons. They are also concerned about content and online behaviours which are not illegal, but which they fear may cause harm to some users. These types of content include promotion of suicide or self-harm, cyberbullying, harassment, and disinformation.

Leading social media and content-sharing platforms have stepped up efforts and dedicated more resources to restricting the availability of both illegal content and legal content that, for reasons such as the aforementioned, is considered undesirable. They have done so in part because of public pressure, and in part to improve the services and user experience they provide.

Policymakers are considering policy and legislation that will 'hold platforms accountable' and make them 'take more responsibility' for the content they host. In European countries, there is a growing sentiment that existing legislation, notably the European E-Commerce Directive (ECD), should be updated. The ECD establishes the principle that content hosts are not liable for user-uploaded content, unless they have been notified of illegality. The Directive's provisions are general, and have been implemented differently in different Member States. The Court of Justice of the European Union (CJEU) has issued a number of rulings that clarify certain questions, but guidance as to the expectations content hosts must meet to maintain safe harbour protection remains vague. The Center for Democracy & Technology (CDT) has argued that the Directive should be supplemented with additional notice-and-action guidelines or legislation, but the Commission decided not to move forward with this type of initiative.

Now, however, the Commission is understood to be preparing policy options for new rules for content hosting; a Digital Services Act. The Act would add to several pieces of EU legislation adopted or proposed in the past few years, and to several Member State legislative initiatives focused on illegal and or harmful content, and overall regulatory supervision of content hosts.

Below, CDT proposes some fundamental principles that should inform future EU policymaking. This input is guided by CDT's mission to protect the fundamental rights of internet users. While the concerns behind several new policy initiatives are legitimate, CDT emphasises that policy initiatives must be very carefully crafted so as not to harm free expression, access to information, and innovation and entrepreneurship on the internet.

Center for Democracy & Technology
Washington, DC | Brussels, Belgium

CENTER FOR DEMOCRACY & TECHNOLOGY

Principles

1. **Policy and legislation must respect human rights principles on freedom of expression.** Legislators are obliged to abide by the principles laid down in human rights instruments, notably Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights. This means that any restriction on free expression must meet the three-part test: it must be provided in law, pursue a legitimate aim, and be necessary and proportionate for achieving that aim. Independent courts must remain the arbiters of what is and is not permissible speech, under clearly articulated laws. Some of the most problematic types of content are proscribed in European law, notably illegal hate speech and terrorist content. However, legal assessment is not straightforward, and even experts and courts differ when evaluating the legality of content. It should not be the case that *de facto* legal standards are set by company reviewers or automated content moderation tools, or delegated to administrative authorities. Moreover, if policymakers consider some types of content unacceptable and harmful, and it is not illegal, it is their job to legislate for it (respecting the human rights and rule-of-law principles referred to above). But it is inconsistent with these principles for governments to leverage private companies to limit speech that authorities cannot not directly restrict.

2. **Policy should be based on the principle that content creators are responsible, under the law, for their online speech and behaviour.** Policy should empower users to post, share, and find content using platforms of their choice. It should also make it possible to hold users accountable for content they post, and how they otherwise behave. It should be clear to individuals that they are ultimately responsible under the law for what they choose to post online. People should be aware that if they post content that constitutes, e.g., illegal hate speech or defamation, they can be prosecuted for it. While online platforms can and should moderate content they host, enforce their terms of service, and restrict illegal content, intermediaries should not be held legally responsible for content authored by third parties.

3. **Policy should be based on solid evidence, and targeted at well-defined and well-substantiated public interest concerns.** Policymakers should recall that several pieces of EU legislation have already been adopted (or are in the process of being adopted) that impose new obligations and responsibilities for platforms. These measures include the DSM Copyright Directive, which obliges a broad range of content hosts to take particular measures, such as filtering, to prevent unlicensed copyrighted content from being uploaded. The Audiovisual Media Services Directive calls for the setting up of codes of conduct in order to ensure that minors are not exposed to types of content that may be considered harmful to them. The current draft Terrorist Content Online Regulation would impose duties of care as well as a requirement on content hosts to suppress content that is deemed illegal under the regulation, within one hour of notification. These pieces of legislation are not yet in force, and their effects are as yet unknown. New measures, such as the possibly forthcoming Digital Services Act,

should be carefully calibrated to focus on clearly defined problems that are not addressed in other legislation.

4. **Policy should ensure clarity about requirements for responding to notifications of illegal speech.** In general, platforms should have adequate and transparent notice-and-action processes that include safeguards and sanctions against wrongful or malicious notification. A content host should not be sanctioned for refusing to remove or downgrade content solely because it has been labeled by a non-judicial actor as illegal. Any new legislation should also be flexible enough to enable platforms to remain passive hosts with regard to some content, and to be active curators and moderators with regard to other content. New legislation will need to grapple with the distinction between active and passive hosting, and determine what level of responsibility companies should take for content it engages with in different ways. It is essential that platforms' efforts to restrict illegal content does not lead to a presumption of knowledge of illegality. Any new legislation should introduce a version of the Good Samaritan principle, in order to ensure that intermediaries are not penalized for good faith measures against illegal content. Sanctions should only be applied in cases of proven systemic failure to respond to valid notifications of illegal content.

5. **Content hosts should not be discouraged from, or limited in their capacity to moderate content.** As a principle, it is both legitimate and desirable that platforms restrict types of lawful content they do not consider, for whatever reason, appropriate for the service they provide. Different platforms serve different communities and purposes, and not all content is suitable for all platforms. It is important to note, however, that the legal status of such content moderation is currently not clear. European courts have in certain cases ruled that a content host may not restrict lawful content, while in other cases ordering hosts to restricting which the host had not considered in violation of either the law or its own terms of service. Any future regulation should be aimed at providing legal certainty to hosts of user-generated content about their ability to moderate their users' lawful speech. Policy should seek to incentivise human rights-respecting content moderation, as recommended by the UN Special Rapporteur on Free Expression.

6. **Use of technological solutions for online content moderation should not be mandated by law.** Content moderation technologies are being used increasingly by a broad range of internet companies. These technologies evolve constantly and will continue to do so, but currently remain quite rudimentary. For example, tools for automating social media content analysis have limited ability to parse the nuanced meaning of human communication, or to detect the intent or motivation of the speaker. They are not able to understand the subtlety of context and meaning, which is necessary to determine whether a statement posted on social media may be considered to violate the law, or terms of service. Policymakers must understand these limitations and should not mandate the use of endorsing or adopting automated content analysis tools or impose time limits on responding to notifications of illegal content, which in

practice will necessitate the use of automated filters to comply with the law. The DSM Copyright Directive has already imposed a *de facto* requirement to use filtering technology. This approach should not be followed in future legislation.

7. **Responsibility for content should not be imposed on other companies than the content host.** Infrastructure service providers, payment providers, advertisers, cybersecurity providers, and others should not be held responsible for content their customers host. These companies lack both the information to effectively make decisions about whether speakers have violated content policies and risk over-censoring in order to avoid liability risks. Only the company with direct relationships with uploaders, and ability to take decisions on discrete pieces of content, should be responsible for it.

8. **Policy should promote, not hinder, innovation and entrepreneurship.** One of the most important and successful features of the limited liability provisions in the ECD is their capacity to encourage innovation and entrepreneurship. Had it not been for these protections, the many thousands of online sites and services that have appeared in Europe and beyond would not have grown and prospered. If new legislation undermines these protections, and introduces new responsibilities and obligations calibrated for global internet companies across the board, it will have a disproportionate negative impact on small companies and start-ups, and could further shrink the diversity of platforms and hosts available to support a broad range of expression online. Compliance, implementation, and litigation costs would disadvantage small companies, while larger, incumbent technology companies would be much better positioned to absorb these costs. It will be essential to ensure that obligations that may be suitable for the largest global networks are not applied to smaller operators.

9. **Content hosts should not be forced to apply one Member State's restrictions on free expression outside that country's territory.** Cross-border enforcement of restrictions would lead to unacceptable infringement of free expression and access to information rights. EU Member State laws vary considerably in how they restrict free expression. For example, some countries criminalise content such as blasphemy, while others have abrogated blasphemy laws; many countries prohibit hate speech but apply those prohibitions differently based on the cultural and historical context of their particular state. If hosts are required to apply one country's speech restrictions broadly, they will inevitably encounter conflicts of law and the space for free expression and public debate would be severely curtailed.

Section 230 Written Submission

The overly expansive judicial interpretation of Section 230, which began almost immediately after its enactment, has provided internet-based companies nearly absolute immunity from tort (and criminal) liability for injuries they inflict upon their users. It is clear from the statute's legislative history that Congress never intended such sweeping protections, but it is equally clear that the inertia of past overbroad judicial decisions will be difficult to overcome without legislative clarification. This submission addresses the narrow issue of changes that are required to sufficiently protect minor victims of sex trafficking.

In 2015, a congressional subcommittee recognized that a nearly 850% increase in child sex trafficking over the prior five years was "directly correlated to the increased use of the Internet to sell children for sex."[1] It also learned that Backpage.com, which was involved in 73% of all child trafficking reports to the National Center for Missing and Exploited Children, was using Section 230 as a shield against civil lawsuits and criminal prosecutions based on its facilitation of sex trafficking.[2] Meanwhile, sex trafficking had been

[1] *Human Trafficking Investigation: Hearing Before the Perm. Subcomm. on Investigations of the S. Comm. On Homeland Security & Governmental Affairs*, 114th Cong. 2 (2015).

[2] *Id.* at 20-21; *Backpage.com's Knowing Facilitation of Online Sex Trafficking: S. Staff Report*, at 6 (Jan. 10, 2017).

criminalized federally and in all 50 states, and statutes providing civil remedies to victims had been passed by Congress, 40 states, and the District of Columbia.[3]

Despite overwhelming evidence that Backpage.com actively facilitated sex trafficking through its website, it was able to use Section 230 to escape liability under both federal and state sex trafficking statutes. In the most notorious case, *Doe v. Backpage.com*, the U.S. Court of Appeals for the First Circuit held that because the victims' causes of action depended in some part upon the content of the traffickers' postings, Section 230 protected Backpage.com from any liability.[4] The court stated that the historic "preference for broad construction" of Section 230 required it to "deny relief to plaintiffs whose circumstances evoke outrage," but it concluded that only Congress could provide a cure:

> If the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation.[5]

---

[3] *See* https://polarisproject.org/wp-content/uploads/2019/09/2015-Civil-Remedy-Issue-Brief.pdf.

[4] *Doe v. Backpage.com, LLC*, 817 F.3d 12 (1st Cir. 2016).

[5] *Id.* at 15, 18-19, 29.

Congress responded the following year by introducing the Fight Online Sex Trafficking Act (FOSTA), which was enacted in 2018.[6] FOSTA's express purpose is "to clarify that section 230 . . . does not prohibit the enforcement against [internet companies] of Federal and State criminal and civil law relating to the sexual exploitation of children or sex trafficking."[7] In an effort to achieve that purpose, FOSTA amended Section 230 by adding a new provision, Subsection (e)(5), entitled "No effect on sex trafficking law." Unfortunately, the structure of the amendment has left room for internet defendants to argue that Section 230 still protects them from sex trafficking laws that provide remedies to victims under state rather than federal law.

The amendment states that nothing in Section 230 "shall be construed to impair or limit" civil actions under a federal sex trafficking statute or state criminal prosecutions for conduct that violates either the federal sex trafficking statute or a new federal statute prohibiting the online facilitation or promotion of prostitution.[8]

---

[6] The report on the Senate bill discussed the First Circuit's opinion in *Doe v. Backpage* and stated that Section 230 "has been held by courts to shield from civil liability and State criminal prosecution nefarious actors, such as the website Backpage.com, that are accused of knowingly facilitating sex trafficking." S. Rep. No. 115-199, at 2 (2018).

[7] FOSTA, Pub. L. No. 115-164, sec. 3, 132 Stat. 1253 (2018).

[8] 47 U.S.C. 230(e)(5).

But civil claims arising under state law—including the common law and myriad of state human trafficking statutes—are not expressly mentioned. At a minimum, such state-law claims should be fully enforceable under the savings clause in Subsection (e)(3) to the extent they are consistent with the relevant federal statutes.[9] Yet, remarkably, internet defendants are now arguing that Congress consciously *chose to protect them from civil claims under state law*, and by extension, to prevent sex trafficking victims from obtaining remedies that the states in which they resided while being victimized have made available. This position is particularly implausible given Congress's awareness of the sex trafficking problem and the proliferation of civil remedies provided by state legislatures.

Though the plaintiff victims should ultimately prevail, further clarification from Congress would avoid costly and time-consuming legal battles over its true intentions in amending Section 230. Additionally, failure to address this problem would implicate serious federalism concerns by effectively preempting state laws in an area of traditional state regulation. The Supreme Court of the United States has recognized that:

[9] The savings clause provides: "Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section." 47 U.S.C. 230(e)(3).

- "[T]he State's interest in fashioning its own rules of tort law is paramount to any discernible federal interest."[10]
- States have a "dominant interest . . . in preventing violence."[11]
- "[W]e can think of no better example of the police power, which the Founders . . . reposed in the States, than the suppression of violent crime and vindication of its victims."[12]
- States have a compelling and "overriding" interest in "safeguarding the physical and psychological well-being of a minor" and "protecting child rape victims."[13]
- The states' interests in preventing "sexual exploitation and abuse of children" and protecting children from "sex offenders plainly applies to internet use."[14]

Section 230 should be further amended to ensure internet companies that facilitate human trafficking are not immunized from legitimate claims by victims under state law and to ensure FOSTA's broad purpose is realized. This may be accomplished by adding an additional carve-out in Subsection (e)(5) for:

---

[10] *Martinez v. State of Cal.*, 444 U.S. 277, 282 (1980).

[11] *McDonald v. City of Chicago, Ill.*, 561 U.S. 742, 901 (2010) (quoting *Automobile Workers v. Wisconsin Employment Relations Bd.*, 351 U.S. 266, 274 (1956)).

[12] *United States v. Morrison,* 529 U.S. 598, 618 (2000).

[13] *Globe Newspaper Co. v. Superior Court for Norfolk County*, 457 U.S. 596, 607 (1982); *id.* at 619-20 (Burger, J., dissenting).

[14] *Packingham v. North Carolina*, 137 S. Ct. 1730, 1739 (2017) (Alito, J., concurring).

> Any claim in a civil action brought under state law that is consistent with section 1591 of Title 18.

This proposed language is narrowly tailored to address the potential loophole for state civil claims, and it mirrors the current carve-out for civil claims under federal law in Subsection (e)(5)(A).

Section 230 Workshop

U.S. Department of Justice

Statement of Corynne McSherry, Ph.D.
Legal Director
Electronic Frontier Foundation

February 19, 2020

(updated February 27, 2020)

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 30,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit Internet users. The majority of EFF's funding comes from ordinary individuals, and over 80% of that funding consists of donations under $10,000. We receive less than five percent of our funding from corporate sponsors.[1]

As a civil liberties organization, EFF's primary reason for defending Section 230 is not just the significant role the law has played in fostering innovation, but the role it plays in empowering Internet *users*. Attempts to change platform behavior by undermining Section 230 will harm the users who rely on those platforms to connect, organize, and learn, particularly the historically marginalized communities that often lack a voice in traditional media. Section 230 enables these voices to get their messages out to the entire world without having to own a distribution platform.

We are well aware that online speech is not always pretty—sometimes it's extremely ugly and causes real-world harm. And the effects of this kind of speech are often disproportionately felt by communities for whom the Internet has also provided invaluable tools to organize, educate, and connect. Systemic discrimination, for example, does not disappear and can even be amplified online.

But removing speech does not make societal problems go away; in fact, it magnifies them. Censorship, including private censorship, makes it more difficult for victims to speak out, to find each other, and to get help. What's more, the people silenced most frequently are often those who lack political or economic power.

EFF is also concerned that tinkering with Section 230 could undermine competition in the social media space, permanently entrenching the current tech giants as arbiters of online speech. Unfortunately, regulation of much of our online expression, thought, and association has already been ceded to unaccountable executives and enforced by minimally-trained, overworked staff, and hidden algorithms. Nonetheless many, especially in policy circles, continue to push for companies to — magically and at scale — perfectly differentiate between speech that should be protected and speech that should be erased. If our experience has taught us anything, it is that we have no reason to trust the powerful — whether corporations or governments—to draw those lines. At a minimum, we urge the Department of Justice to ensure that its review of Section 230 is informed by, and informs, the work of the Antitrust Division.

---

[1] *2018 Annual Report*, Electronic Frontier Found. https://www.eff.org/files/annual-report/2018/

A. What Section 230 Does and Does Not Do

Section 230 provides Internet intermediaries, both commercial and noncommercial, with broad—but not absolute—immunity from legal liability for user-generated content. As such, it is a cornerstone for free speech and innovation online.

47 U.S.C. § 230(c)(1) states 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." This means Internet intermediaries that host third-party content are protected against a range of laws that might otherwise be used to hold them legally responsible for what their users, not they themselves, say and do.

At the same time, Section 230 also protects companies when they choose to moderate their platforms. Indeed, part of the genesis of the law was a pair of defamation disputes where one company was held liable for content on its service, and the other was not, because the first company chose to moderate generally but failed to catch the defamatory statement.[2] Section 230 remedied that disparity, providing a safe harbor for moderation.

Thus, while Internet platforms—ISPs, web hosting companies, webmail providers, blogging platforms, social media and review sites, online marketplaces, photo and video sharing platforms, and cloud storage providers—have limited liability for the speech on their platforms, they are also free to remove users or speech that have violated their community standards or terms of service.

It's also important to understand what Section 230 does *not* do. Section 230's safe harbor, while substantial, is significantly narrower than is often supposed because it has important exceptions. While Section 230 provides immunity to platforms against liability under state law (whether criminal or civil) and against liability under federal civil law, it does *not* provide immunity against prosecutions under federal criminal law, or liability based on copyright law or certain sex trafficking laws. For example, a federal judge in the infamous Silk Road case correctly ruled that Section 230 did not immunize the operator of a website that hosted other people's ads for illegal drugs from federal prosecution.[3] Nor does Section 230 provide immunity against civil or state

---

[2] *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)

[3] Cyrus Farivar, *Judge denies Silk Road's demands to dismiss criminal prosecution*, Ars Technica (July 9, 2014), https://arstechnica.com/tech-policy/2014/07/judge-denies-silk-roads-demands-to-dismiss-criminal-prosecution/

criminal liability where the company "is responsible, in whole or in part, for the creation or development of information,"[4] and courts have consistently interpreted the law accordingly.[5]

Another common misconception is that Section 230 protects only "tech companies."[6] Not so. For example, Section 230 makes no distinction between news media and social media platforms. When a news entity operates online, it gets the exact same Section 230 immunity from liability based on someone else's content that a social media platform gets. Nor is Section 230's protection limited to commercial businesses. Wikipedia relies on Section 230, too, as do many of other nonprofits, big and small.

Finally, Section 230 provides immunity to any "provider *or user* of an interactive computer service" when that "provider or user" republishes content created by someone or something else. "User," in particular, has been interpreted broadly to apply "simply to anyone using an interactive computer service."[7] If you have ever forwarded an email, whether a news article, a party invitation, or birth announcement, you have done so with the protection of Section 230. If you have ever maintained an online forum for a neighborhood group, you have done so with the protection of Section 230. And so on.

B. Proceed with Caution: The Risks of Undermining Section 230

We all want an Internet where we are free to meet, create, organize, share, associate, debate, and learn. We want to exercise control over our online environments and to feel empowered by the tools we use. We want our elections free from manipulation and for the speech of women and marginalized communities to not be silenced by harassment.

But chipping away at the legal foundations of the Internet is not the way to accomplish these goals.

1. Over-censorship

As a practical reality, it is very difficult for many platforms to accurately remove all unlawful speech while keeping everything else intact. Therefore, undermining Section 230 effectively forces platforms to put their thumbs on the wrong side of the scale—that is, to remove

---

[4] 47 U.S.C. § 230(f)(3).

[5] *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008); *Anthony v. Yahoo! Inc.*, 421 F.Supp.2d 1257 (N.D. Cal. 2006); *Nemet Chevrolet, LTD. v. Consumeraffairs.com, Inc.*, 591 F.3d 250 (4th Cir. 2009); *Barnes v. Yahoo!*, 570 F.3d 1096 (9th Cir. 2009); *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016).

[6] David Greene, *Section 230 Is Not A Special "Tech Company" Immunity*, Electronic Frontier Found. (May 1, 2019), https://www.eff.org/deeplinks/2019/04/section-230-not-special-tech-company-immunity

[7] *Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006)

far more speech than what is actually unlawful, censoring innocent people and often important speech in the process.

The effects of 2018's Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) offer an object lesson. FOSTA amended Section 230 to create new liability for platforms that host content about sex work. It also broadly and ambiguously expanded federal criminal law to target online platforms where users discuss sex work and related topics.

FOSTA's impact on Internet speech was apparent almost immediately after the law passed. Internet companies increased restrictions on speech discussing sex.[8] Organizations providing support to sex workers, including helping them share information about dangerous clients, had to choose between taking on new legal risk or ceasing operations.[9] Many of them chose the latter.

More broadly, platforms presented with new liability risks over-censored. For example, Craigslist completely removed its message boards dedicated to both personal ads and therapeutic services. The company could not individually review every post on those boards—and even if it could, it would not be able to reliably recognize every unlawful post—so it removed the boards altogether, punishing legitimate, lawful businesses in the process.[10] Similarly, Tumblr—a community which many LGBTQ users have said was vital to them as youth[11]—chose to ban all sexual content. Some smaller, niche personals sites either removed certain features or closed entirely.[12] In recent months, several members of Congress have begun to openly acknowledge the harms that FOSTA has brought to sex workers, including those being trafficked.[13]

---

[8] Elliot Harmon, *Facebook's Sexual Solicitation Policy is a Honeypot for Trolls*, Electronic Frontier Found. (Dec. 7, 2018), https://www.eff.org/deeplinks/2018/12/facebooks-sexual-solicitation-policy-honeypot-trolls

[9] Karen Gullo and David Greene, *With FOSTA Already Leading Censorship, Plaintiffs Are Seeking Reinstatement Of Their Lawsuit Challenging the Law's Constitutionality,* Electronic Frontier Found. (March 1, 2019), https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit

[10] Karen Gullo and David Greene, *With FOSTA Already Leading Censorship, Plaintiffs Are Seeking Reinstatement Of Their Lawsuit Challenging the Law's Constitutionality*, Electronic Frontier Found. (March 1, 2019), https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit

[11] Prodita Sabarini, *Why Tumblr's Ban on Adult Content Is Bad for LGBTQ youth*, The Conversation (Dec. 6, 2018), https://theconversation.com/why-tumblrs-ban-on-adult-content-is-bad-for-lgbtq-youth-108215

[12] *Documenting Tech Actions,* Survivors Against Sesta, https://survivorsagainstsesta.org/documentation/

[13] Anna North, *Sex workers Are in Danger. Warren and Sanders Are Backing a Bill that Could Help,* Vox (Dec. 17, 2019), https://www.vox.com/identities/2019/12/17/21024859/sex-work-bernie-sanders-elizabeth-warren-fosta

Our nation's founders knew that it is impossible to craft laws that only target bad actors, which is why the First Amendment protects most speech, even distasteful or "indecent" speech. Private enforcers face the same problem when crafting and enforcing community standards—and it will only worsen if a failure to enforce perfectly could lead to legal liability.

2. Competition

It's understandable that some people who are concerned about the outsized power of the tech giants are drawn toward proposals to modify Section 230. Unfortunately, any such attempt is likely to backfire. If Section 230 does nothing else, it helps pave the way for competition. As Professor Eric Goldman of Santa Clara University School of Law puts it, "Even as Section 230 privileges the Internet giants, it also plants the seeds of their future destruction."[14]

Simply put, by dramatically reducing the legal cost of hosting third-party speech, Section 230 allows Internet platforms both big and small, commercial and nonprofit, to operate at a global scale. These include Wikipedia, the world's largest (and growing) repository of information, staffed by a mere 350 people worldwide, and the Internet Archive, with a staff of 150 and a budget of just $18 million/year. Eviscerating Section 230, or imposing new burdens in exchange for immunity, would make those operations untenable (much less the smaller operations of many startups, websites, and community forums).

The tech giants, by contrast, would have resources to shoulder those burdens. They also have the legal resources to fight off the lawsuits a weakened Section 230 would invite.[15] More generally, changing the formula after the fact only favors established companies that have used the law to establish a foothold while their would-be usurpers are forced to tread less certain legal waters. And if competing products don't exist, users cannot simply switch services as a means to discipline a company's conduct.

Modifications to Section 230 could also push platforms toward more reliance on automated filtering. Even if such filters weren't notoriously inaccurate, the cost of building and using them makes these tools inaccessible for startups. For example, YouTube's Content ID system cost the

---

[14] Eric Goldman, *Want to Kill Facebook and Google? Preserving Section 230 Is Your Best Hope*, Balkinization, New Controversies in Intermediary Liability Law (June 3, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398631

[15] Elliot Harmon, *Google Will Survive SESTA. Your Startup Might Not,* Electronic Frontier Found. (Sept. 22, 2017), https://www.eff.org/deeplinks/2017/09/google-will-survive-sesta-your-startup-might-not

company approximately $100 million.[16] By comparison, the Wikimedia Foundation (the organization that maintains Wikipedia and several other information-sharing tools) has an annual budget of $80 million.[17]

C. Graham-Blumenthal Proposed Draft Legislation Would Give New Power to Future Administrations at the Expense of Innovation, Competition, and Speech

Bloomberg recently published a draft bill by Senators Lindsey Graham (R-SC) and Richard Blumenthal (D-CT). The so-called EARN IT Act would establish a "National Commission on Online Child Exploitation Prevention." The commission would be tasked with recommending "best practices for providers of interactive computer services regarding the prevention of online child exploitation conduct." Platforms that failed to adhere to those practices would be stripped of Section 230 protections if they were accused (either in civil or criminal court) of carrying unlawful material relating to child exploitation. If the Attorney General disagreed with the Commission's recommendations, the Attorney General could veto them.

The EARN IT Act could cause dramatic collateral damage, effectively letting current and future attorneys general, and/or an unelected commission, force technology companies to change their practices to fit a given administration's political agenda. Moreover, with just two people representing "small" (under 10 million users) platforms, and no one with expertise in free speech and civil liberties, the proposed commission is likely to make recommendations that favor large tech companies.

But even if the proposed commission were staffed more evenly, its rules would likely still confound new innovation in the Internet space. Because Section 230 is flexible and simple, it has provided breathing room for experimentation with business models and services that didn't exist when the law passed in 1996. If Congress had laid out a detailed list of requirements back then, open platforms like Wikipedia likely never would have emerged.

The legislation provides for updating best practices, but that offers cold comfort for many entrepreneurs. Without certainty that their business models would pass muster, they will be hard-pressed to get the investment necessary to bring their services to market. Nonprofits on even tighter budgets will be even less likely to shoulder the risk.

---

[16] Paul Sawers, *YouTube: We've invested $100 million in Content ID and paid over $3 billion to rightsholders*, VentureBeat (Nov. 7, 2018), https://venturebeat.com/2018/11/07/youtube-weve-invested-100-million-in-content-id-and-paid-over-3-billion-to-rightsholders/

[17] *Wikimedia Foundation, Inc., Financial Statements June 30, 2018 and 2017 (With Independent Auditors' Report Thereon)*, KPMG, (Sept. 26, 2018), https://upload.wikimedia.org/wikipedia/foundation/6/60/FY17-18_-_Independent_Auditors%27_Report.pdf

The EARN IT Act is also a direct threat to constitutional protections for free speech. To pass constitutional muster, a law that regulates the content of speech must be as narrowly tailored as possible so as not to chill legitimate, lawful speech.[18] The EARN IT Act does the opposite: under the bill, the commission would effectively have the power to change and broaden the rules however it saw fit, as long as it could claim that its recommendations somehow aided in the prevention of child exploitation.

D. Remedies Exist Under Current Law That Do Not Conflict with Section 230

Critics of Section 230 often forget that the law already affords rights and remedies to victims of harmful speech when it causes injury. Speakers who harm others can and do face serious consequences.

In the infamous *Grindr* case, for instance, a man misused a dating application to intensely harass a former boyfriend. The abuser was arrested and charged with stalking, criminal impersonation, making a false police report, and disobeying a court order.[19] The FBI shut down Backpage.com, a website that was frequently cited in debates over FOSTA, in April 2018, without relying on FOSTA.[20]

States have also crafted a range of laws that hold individuals personally responsible for their harmful conduct. There are state criminal penalties for both stalking and harassment, and a panoply of civil and criminal statutes for conduct that causes physical harm to an individual. The courts can draft restraining orders that include serious penalties for violation. Under current law, if an Internet company discovers that people are using its platforms to distribute child sexual abuse material, it must provide that information to the National Center for Missing and Exploited Children and cooperate with law enforcement investigations.

In addition to criminal charges, victims can use defamation, false light, intentional infliction of emotional distress, common law privacy, interference with economic advantage, fraud, anti-discrimination laws, and other civil causes of action to seek redress against the direct perpetrators. They can also sue a platform if the platform owner is itself creating the illegal content.

---

[18] *Reed v. Town of Gilbert*, 135 S.Ct. 2218 (2015), https://supreme.justia.com/cases/federal/us/576/13-502/

[19] Tyler KingKade and Davey Alba, *A Man Sent 1,000 Men Expecting Sex And Drugs To His Ex-Boyfriend Using Grindr, A Lawsuit Says*, BuzzFeed News (Jan. 10, 2019), https://www.buzzfeednews.com/article/tylerkingkade/grindr-herrick-lawsuit-230-online-stalking

[20] Tom Porter and Reuters, *Backpage Website Shut Down, Founder Charged with* 93 *Counts by FBI in Sealed Document*, Newsweek (Apr. 7, 2018) https://www.newsweek.com/sex-ads-website-backpagecom-co-founder-charged-after-fbi-raid-876333

E. Conclusion

The Internet embodies and represents an extraordinary idea: that anyone with a computing device can connect with the world, anonymously or not, to tell their story, organize, educate and learn. Section 230 helps make that idea a reality. And it is still worth protecting.

Section 230 Written Submission Presented by The Alliance to Counter Crime Online

The Alliance to Counter Crime Online (ACCO) is made up of more than 30 academics, security experts, NGOs and citizen investigators who have come together to counter the spread of serious organized crime and terror activity on the Internet.

Call to Action

ACCO seeks reform of Section 230 of the Communications Decency Act (CDA 230) in order to:

1. Revise immunity protections immunities for hosting terror and serious crime content;
2. Regulate that tech firms must report crime and terror activity to law enforcement; AND
3. Appropriate adequate resources to law enforcement to contend with this data.

The Problem

When CDA 230 passed in 1996, most people connected to the World Wide Web using a telephone dial-up. Social media and smart phones had not been invented.

Today, Internet usage dominates our daily lives, and it should come as no surprise that a lot of illicit activity has shifted online, just like commercial commerce and communications.

The scale and range of illicit activity occurring online represents one of the premier security threats of our time, one that we as a nation can and must solve to protect the health and safety of the American people.

Tech industry leaders want us to believe that illicit activity is mainly confined to the dark web. But study after study by ACCO members and others show that surface web platforms are infested with criminality.

Some of the world's most widely used social media platforms, including but not limited to Facebook, Twitter, YouTube, WeChat and Instagram, have become ground zero for serious organized crime syndicates to connect with buyers, market their illegal goods, and move money, using the same ease of connectivity enjoyed by ordinary users.

Terrorist groups have also weaponized social media, using it as a megaphone for propaganda, to recruit new members, and even as a mechanism for fundraising. This illegal activity often occurs out in the open, or in private groups or encrypted messaging services.

This has happened for four reasons:

1. Many surface web platforms today provide much the same anonymity as the dark web alongside payment systems, connectivity features, and a far greater reach of people;
2. Social media algorithms help criminals and terrorists connect to customers and supporters they would never otherwise have found;
3. Outdated legislation, broadly interpreted by the courts, provides immunity to the tech industry even in cases when firms knowingly hosted illicit content; and
4. This immunity meant that for years tech firms had no incentive – legal or otherwise – to police content, turning major platforms into breeding grounds for transnational crime to flourish.

CDA 230 grants expansive safe harbor to any provider of an "interactive computer service" for user-generated content, but the law did not anticipate a world where tech algorithms drive connectivity – whether it's to help friends share memes or so drug cartels can market opioids to folks in recovery.

The authors of CDA 230 say they intended for tech firms to take reasonable steps to moderate their platforms for illicit content. But the law did not define which content was illegal to host, nor mandate any specific response to illicit and toxic content, much of it evidence of crime. As a result of that ambiguity, the majority of tech firms, when they do take action on content, simply delete it. They are literally operating in a world without rules.

Furthermore, by limiting the liability of tech firms to federal criminal law, CDA230 also effectively removed the right of users harmed by illegal activity occurring online from seeking justice from tech firms. What does this look like in action? Here are some examples:

1. The victim of a cyber stalker can't seek restitution from the firm that hosted the content.
2. Relatives of people murdered on camera can't get tech firms to remove the content, nor can people whose images have been used by online scammers.
3. Girls who have been trafficked online can't get restitution from platforms that hosted the content.

> ***The Online Drug Threat****: The United States in the midst of an addiction crisis that is claiming the lives of more than 60-thousand Americans every year. But Facebook, the world's largest social media company, only began tracking drug postings on its platform last year. In the fourth quarter of 2019, the firm admitted to removing 4.4M pieces of content identified as selling drugs. To put that in perspective, that's 400 times more postings than the notorious Dark Website the Silk Road ever carried. Instagram has never released any data on the volume of drug content on its platform; our research indicates it's an even bigger drug marketplace. And Facebook is not alone. Study after study by ACCO members and others have shown widespread use of Google, Twitter, Facebook Reddit, and YouTube to market and sell fentanyl, oxycodone and other highly addictive, often deadly controlled substances to U.S. consumers, in direct violation of federal law. Some 96% of online pharmacies are illegal, selling counterfeit or illegal drugs, peddling prescription medicines, including opioids, without prescriptions, and/or operating with no pharmacy license. Every major internet platform has a drug problem. Why? Because there is no law that holds tech firms responsible, even when a child dies buying drugs on a web platform.*

Try and imagine another industry that has ever enjoyed such an incredible subsidy from Congress: Total immunity no matter what harm their product brings to consumers.

A brick and mortar pharmacy would face serious civil liabilities for selling illegal, unregulated medicines. But Google can host thousands of illegal online pharmacies, facilitating their illicit sales, without such concern. Financial institutions face costly penalties for facilitating terror groups and drug cartels, but the Sinaloa Cartel has more than 80,000 followers on Twitter and, somehow, that's not a crime.

An auction house like Sotheby's could not legally broker sales of stolen art, but Facebook hosts more than 100 groups, with millions of active members, where plundered conflict antiquities are sold to profit criminals and terror groups alike.

The laws on the books today have allowed the most profitable firms on the planet to generate billions of dollars in revenue – for a quarter century – without any accountability to the users harmed by illegal activity the firms host and facilitate on their platforms.

Moreover, this is a problem that's about to get a lot worse. The largest social media firms are moving to increase the number of private groups, to incorporate end-to-end encryption across their messaging apps, and even to launch anonymous payment systems and blockchain technologies. These proposed policy changes appear to be aimed at insulating tech firms from liability, since firms can't possibly police content they can't read.

This "pivot to privacy" should also be perceived as the digital equivalent of sweeping an enormous problem under the rug. Greater encryption will help illicit actors to cover their tracks. It will make it harder for authorities to track wrongdoing online, and it will further deny crime victims a civil path to justice. Most importantly, it could also turn key social media platforms into darknets that will optimize growth opportunities for marketing and selling illegal goods, enabling organized crime groups and terror groups to reach billions of customers with ease.

Time to Reform CDA 230

The tech industry routinely claims that any modifications to CDA 230 represent a threat to freedom of speech. But CDA 230 is a law about liability, not free speech. No one at ACCO is pushing for change to the 1st Amendment.

Under the original intent of CDA 230 there was to be shared responsibility for keeping cyberspace safe between tech platforms, law enforcement, and civil society organizations like ACCO. The tech industry has not only failed to uphold its end of the bargain, its powerful algorithms play an active role facilitating and spreading harm that should negate CDA 230 immunities.

For example, an anonymous whistleblower filed a May 2019 complaint to the Securities and Exchange Commission (SEC) identifying how Facebook's auto-generation feature was actually creating business pages for terrorist groups and white nationalists, helping them to connect supporters. The company took no action on the feature creating business pages for terrorists, and in September 2019, the whistleblower filed an update to their complaint identifying hundreds of auto-generated business pages for ISIS that had been created by Facebook.

Wildlife Crime Online: *ACCO members are tracking groups on Twitter, Instagram, Google and Facebook where endangered species are sold – items ranging from rhino horn and ivory to live reptiles, bugs and primates. In some cases, the size of these markets is literally threatening key species with extinction. One of our members, the Cheetah Conservation Fund has found that 70 percent of the annual illegal cheetah trade takes place on Facebook and Instagram. More than half the trade in ape species takes place on social media, according to Dr Dan Stiles and Dr Susan Cheyne, two ACCO members tracking that trade. CINTOC ran undercover operations that identified multiple Vietnamese Triads moving tons of ivory every month across Facebook. That investigation brought us to the horrifying conclusion that social media is directly contributing to the extinction of the elephant. There's also an abundance of animal torture on some social media platforms. One ACCO member has tracked dozens of secret groups on Facebook which feature brutal dog-fighting videos that one can place bets on. Former Facebook moderators have described the prevalence of secret groups that auction animal torture video – grotesque videos of family pets, such as cats, being decapitated with hatchets, and puppies being clubbed to death.*

Tech firms could have implemented internal controls to prevent this type of activity from occurring but it was cheaper and easier to scale by looking the other way. The industry was given an incredible freedom, and tech titans have no one to blame but themselves for squandering it.

Congress will inevitably debate whether tech firms should fall under a strict liability regime over illicit content – such as what was established by FOSTA-SESTA for human trafficking – or if a "standard of care" definition of liability is sufficient, at least for some illicit activity.

ACCO supports a strict liability regime for all serious crime and terror content. But we acknowledge there are complex cultural, jurisdictional and privacy issues around defining what is illegal on the Internet.

The borderless, multi-lingual nature of the World Wide Web makes it complex for tech firms to stay across issues, in particular since the size of their moderation teams remains so incredibly small, in comparison to the size of the populations they serve. Understand how few people patrol the Internet, consider that the United States and most developed nations deploy a ratio of about 300 police per 100,000 residents. Facebook, in comparison, employs just 15,000 moderators for a population of 2 billion users. That's a ratio of 3 moderators per every 400,000 users. Google, meanwhile, employs about 7,000 moderators for a population of 2.4 billion users, an even smaller ratio.

Police to population ratios may not be a perfect comparison – but it is certainly striking how few people are patrolling some of the biggest platforms in cyberspace. Moreover, most moderators are low-paid contract workers, with scant training or experience in issues as complex as organized crime and terrorism.

How can tech firms be incentivized to reach out to or contract actual experts in online crime, since we are not listened to nor heeded when we bring them information independently?

There are already crawlers that track the Internet for copyright violations and child abuse content, but these are costly to operate, requiring massive processing power and cloud computing capabilities.

At ACCO we believe industry should bear the burden of these costs, although currently they are often born by underfunded NGOs and public-private partnerships like the National Center for Missing & Exploited Children (NCMEC).

Conflict Antiquities Threat: *Facebook's Community Standards do not prohibit the illicit sale of artifacts, even though this is a known source of funding for terrorists and transnational criminal groups alike. The Antiquities Trafficking and Heritage Anthropology Research (ATHAR) Project has identified multiple members of terrorist groups openly selling artifacts on Facebook. In October 2019, the ATHAR Project co-directors spoke to Facebook policy managers about the threats of terrorist finance on the platform and recommended the firm ban the trade in cultural property as it has done with guns and wildlife. The UN Security Council's Analytical Support and Sanctions Monitoring Team in January 2020 identified Facebook as a key facilitator for the trafficking of antiquities to fund terrorist groups, noting, "Member States reported the increasing use of Facebook and other social media platforms for illegal trafficking in cultural property." As of February 13, 2020, no policy changes on cultural property have been made. The threats of the sale of conflict antiquities trafficked on Facebook are not limited to the Middle East. The ATHAR report found that a massive network of traffickers exists with a global reach: some 488 individual admins managing a collective 1,947,195 members across 95 Facebook Groups. The influence of these traffickers extends as far as the United States, where at least one well-known American antiquities dealer is Facebook friends with an admin of multiple Facebook Groups and dozens more traffickers who are members of the groups. These traffickers are not simply finding one another by chance, Facebook's algorithms promote ways for traffickers to connect. Source: ATHAR Project*

Furthermore, when crawlers flag potential illicit content, that content still has to be verified by human analysts. These systems are badly backlogged, leaving analytic teams drowning in toxic content they don't have the bandwidth to wade through. Police units meant to interdict cyber criminals are stretched even further, when they exist at all. In other words, this isn't just a matter of changing the laws, but properly resourcing the units tasked with upholding it.

What Else Can Be Done

Countering the online crime threat will require a multi-pronged response. Tech firm claim to be working on artificial intelligence solutions, but this is never going to be a silver bullet that solves the problem on its own.

First, there must be significantly more resources invested into identifying, developing and implementing technologies that can support law enforcement and the tech industry to monitor online activity in ways that will not violate civil liberties, nor hamper innovation. These technologies haven't developed precisely because industry has no incentive to develop them. That needs to change.

At ACCO, we believe the tech industry must be part of the solution, and we have already begun reaching out to experts and entrepreneurs in cybersecurity to identify technological responses. At the end of the day, this is a systems problem, so what can we do to clean up these systems?

The tech industry, for example, has an existing certification process for trusted vendors and partners, that could be applied to social media users. The levels would depend on a user's data usage and activity. For example, an ordinary social media user who engages only in public posts and uses little data would qualify for a level 1 rating, requiring little scrutiny. A more active data user who, for example, joins a secret group, or makes multiple purchases online, would need to get a higher level of certification. Certification levels would be higher for users running a private or secret group, and these could go higher as the size of the group they ran increased. As a user rose in levels, the user might be asked to pay a fee, and undergo a greater degree of background checking. That way firms could be assured they were not exposed to risk, the way banks do Know Your Customer and Credit Checks.

Finally, and perhaps most importantly, there is a need for tech moderation teams be trained on how to identify and counter organized crime and terror groups that are weaponizing content, and to work collaboratively with law enforcement to interdict these groups in the real world.

The horrifying irony of the online crime and terror threat is that social media firms that aggressively harvest user data are sitting on an incredible trove of evidence about some of the world's most dangerous and prolific criminals, and on the few occasions they do anything about it, it's normally to delete it.

Without changing the laws, there is no indication these firms have any plan to alter their behavior.

Submission by Alan Rozenshtein can be found here:

https://www.lawfareblog.com/congress-not-attorney-general-should-decide-future-encryption

Statement of Julie Samuels
U.S. Department of Justice Workshop, "Section 230: Nurturing Innovation or Fostering Unaccountability?"
February 19, 2020

47 U.S.C. § 230 ("Section 230") is a crucial driver of innovation and free expression, which was one of the stated purposes of the law. Indeed, the most trafficked websites in the world rely on Section 230 for immunity.[1] While now those websites are household names, they would not have gotten off the ground without Section 230's protections.[2] As such, any consideration to amend Section 230 must seriously take into account the costs on a thriving startup ecosystem that promotes healthy competition.

1. **By allowing startups to thrive, Section 230 protects and supports a competitive marketplace.** This was a primary purpose of Section 230 when it was passed. And it has proven prescient: in 1996, there was no Google, Facebook, or Wikipedia. Without Section 230, those websites would not exist. And even more important, without Section 230, those websites' future competitors likewise will not exist. Indeed, "[w]hen Congress passed [Section 230] in 1996, it was largely looking to future businesses and technologies. In today's age of powerful mega-platforms, the concern about competition is perhaps even more justified."[3] Put more clearly, any narrowing of Section 230 at this point will only harm the next generation of internet companies, the very companies our economy and society should work to foster.
2. **Any changes to Section 230 should consider the expense that would be levied primarily on small startups and other new and growing enterprises.** Litigation is incredibly expensive, particularly for a small company. A single lawsuit can easily cost well into the millions of dollars. Section 230, and its caselaw, currently provide clear guidance to internet platforms. Even more, they provide small companies a path to move early in a case, through a motion to dismiss, to protect itself from unwarranted litigation, before the costly discovery phase. Without Section 230 in its current form, startups would be left fighting even meritless cases at great expense. This would inevitably lead to less funding for internet platform companies and less of an appetite to build those types of businesses, further entrenching the already-large players in the space.

[1] Eric Goldman, *The Ten Most Important Section 230 Rulings,* 20 Tul. J. Tech. & Intell. Prop. 1, 2 & n.8 (2017).
[2] *See, e.g., CDA §230 Success Case: Wikipedia*, Electronic Frontier Foundation, (July 26, 2013), available at https://www.eff.org/deeplinks/2013/07/cda-230-success-cases-wikipedia.
[3] Daphne Keller, *Toward a Clearer Conversation About Platform Liability,* Knight First Amendment Institute (May 7, 2018).

3. **Section 230 protects free expression, realizing the promise of the internet and allowing the United States to lead.** Section 230 is crucial to American dominance of the internet economy.[4] And this trend is poised to continue: a recent study found that over the next decade, Section 230 will contribute an additional 4.25 million jobs and $440 billion in growth to the economy.[5] America's long-time and unique commitment to free expression, enshrined in the First Amendment to our Constitution, has provided a framework that lets speech and creativity thrive. This does not come without challenges, particularly in the current moment, where technology advancements are quickly altering the way we communicate and get information. At its core, the internet has always provided the promise of many-to-many communication at scale for the first time in human history. Any efforts to roll back the ability to use this medium to its fullest, to put the so-called "genie back in its bottle," would be a grave mistake that would usher the worst of the speech on the internet underground. The American experiment is a forward-looking one, one that is about embracing change and innovation. We should not shirk from that responsibility now.

[4] Internet Association, *A Look at American Digital Exports,* (January 23, 2019), available at https://internetassociation.org/publications/a-look-at-american-digital-exports/.
[5]NetChoice and Copia Institute, *Don't Shoot the Message Board: How Intermediary Liability Harms Online Investment and Innovation,* (June 25, 2019), available at http://netchoice.org/wp-content/uploads/Dont-Shoot-the-Message-Board-Clean-Copia.pdf

The Value of Standards-Based Approaches to Address Stakeholder Needs

The following provides an overview of the U.S. voluntary standardization system, the role of the American National Standards Institute[1] (ANSI) in this system, and examples of the value of a standards-based approach in supporting flexible solutions to real world problems. It is intended to provide an informal basis for discussions regarding possible standards-based approaches to address information governance and content moderation challenges. Any opinions expressed in this document are those of the author only.

About the U.S. Voluntary Standardization System

Market-driven and private-sector-led, the U.S. standardization system is dynamic and responsive because it thrives on the active participation and engagement of all affected stakeholders – including industry, government, standards developing organizations, academia, consumers, and others.

As one of the biggest users of standards, the U.S. government's active participation in standardization is of great importance. Through public-private partnership, the U.S. is able to respond most effectively to the strategic needs of the nation on both domestic and international fronts.

Reliance on private sector leadership, supplemented by Federal government contributions to standardization processes as outlined in OMB Circular A-119, *Federal Participation in the Development and use of Voluntary Consensus Standards and in Conformity Assessment Activities*, remains the primary strategy for government engagement in standards development. The circular has guided Federal agency implementation of the *National Technology Transfer and Advancement Act of 1995* for more than two decades.

About ANSI

ANSI is a federation whose members are government agencies, trade associations, standards developing organizations, professional societies, companies, academic and international bodies, and consumer organizations looking to harness the power of standards to position themselves for long-term success. ANSI represents the interests of more than 270,000 companies and 30 million professionals worldwide. As the voice of the U.S. standards and conformity assessment system, ANSI empowers its members and constituents to strengthen the U.S. marketplace position in the global economy while helping to assure the safety and health of consumers and the protection of the environment.

Voluntary consensus standards for products, processes, and services are at the foundation of the U.S. economy and society. The United States has a proud tradition of developing and using voluntary standards to support the needs of our citizens and the competitiveness of U.S. industry globally.

---

[1] www.ansi.org

In its role, ANSI oversees the creation, promulgation, and use of thousands of norms and guidelines that directly affect businesses in nearly every sector. Through its wholly owned subsidiary, the ANSI National Accreditation Board (ANAB), ANSI is also actively engaged in accreditation of conformity assessment bodies – assessing the competence of organizations determining conformance to standards. Via its affiliate, Workcred, ANSI supports efforts to strengthen workforce quality by improving the credentialing system, ensuring its ongoing relevance, and preparing employers, workers, educators, and governments to use it effectively.

International Standardization

ANSI promotes the use of U.S. standards internationally, advocates U.S. policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where they meet the needs of the user community. The Institute is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations, the International Organization for Standardization (ISO) and, via our U.S. National Committee (USNC), the International Electrotechnical Commission (IEC). As a founding member of ISO, ANSI plays a strong leadership role in its governing bodies while U.S. participation, via the USNC, is equally strong in the IEC.

To formulate and advance consensus U.S. positions with respect to ISO and IEC work, ANSI accredits U.S. Technical Advisory Groups (TAGs) to ISO and approves USNC TAGs to IEC. The primary purpose of these TAGs is to develop and transmit, via ANSI, U.S. positions on activities and ballots of ISO and/or IEC Technical Committees (and, as appropriate, subcommittees and policy committees). ANSI's *International Procedures* provide the due process-based framework within which U.S. TAGs develop and coordinate U.S. positions.

ANSI is a permanent member of both the ISO Council and Technical Management Board. ANSI and its members participate in nearly 80% of ISO Technical Committees (TCs) and Subcommittees (SCs) and administer 14% of TC and SC Secretariats. ANSI's USNC is a permanent member of the IEC Council Board, Standardization Management Board, and Conformity Assessment Board. The USNC participates in over 92% of IEC TCs and SCs, and administers 13% of TC and SC Secretariats.

American National Standards

Domestically, ANSI accredits standards developing organizations (SDOs) and approves standards from these organizations as ANS. To achieve the ANSI-Accredited Standards Developer (ASD) designation – the first step for developing ANS – SDOs must comply with ANSI's *Essential Requirements* and demonstrate commitment to a set of principles that includes openness, balance, due process, and consensus. The principles contained in the *Essential Requirements* are consistent with the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Agreement principles for the development of international standards. Conformance to these principles means that the U.S. can set an example globally for what open and trusted standardization looks like.

ANSI's many checks and balances, including impartial audits, accreditation requirements, and an appeals process, underpin the integrity of the ANS process, regularly assuring adherence to the Institute's procedures and safeguarding the value of the ANS designation. This voluntary consensus standards process is time-tested, and has been relied on by many government agencies to the benefit of the public, government, industry and many other stakeholders. ASDs meet the definition in OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,* of "voluntary consensus body."

ANSI National Accreditation Board (ANAB)

ANSI's work in the conformity assessment arena includes a complete portfolio of third-party accreditation programs under its wholly owned subsidiary, ANAB. These programs are conducted in accordance with widely accepted international standards and include accreditation of product and management system certification bodies, calibration and testing labs and forensic service providers, personnel credentialing organizations, inspection bodies, police crime units, greenhouse gas validation and verification bodies, reference material producers, and proficiency test providers.

ANSI Standards Panels, Collaboratives and Workshops

More than twenty years ago, ANSI launched the standards collaborative model to address the needs of both government and private sector stakeholders for a mechanism to coordinate and accelerate the development of private sector-led standards and conformity assessment programs to address national and global priorities. Via a variety of mechanisms, including panels, workshops and roadmapping exercises, ANSI has convened stakeholders to

- Coordinate the efforts of the private and public sectors
- Identify existing standards, standards in development, and compliance programs
- Define where gaps exist based on stakeholder needs
- Recommend additional work needed, timelines for its completion, and organizations that can perform the work
- Help to inform resource allocation for standards participation, avoid duplication of effort, and drive coordinated standards activity

The ID Theft Prevention and ID Management Standards Panel (IDSP) provides a relevant example. ANSI created the IDSP in 2006 in partnership with the Better Business Bureau. It's objective was to facilitate cross-sectoral efforts related to the timely development, promulgation and use of voluntary consensus standards and guidelines to equip and assist the private sector, government and consumers in minimizing the scope and scale of identity theft and fraud.

The IDSP released several workshop reports: on best practices for measuring identity theft and calling for a national identity verification standard. In addition, the panel produced a comprehensive report for businesses, government agencies, and other organizations in the fight against the theft of personal and financial information.

IDSP workshops typically involved making an inventory of existing standards and industry guidelines in a subject area, identifying gaps where new or updated guidance may be needed, and making recommendations regarding best practices or the desirability and feasibility of undertaking standards development activity. Each workshop culminated in the publication of a report that presented the workshop's consensus-based findings and recommendations, which in turn drove future standards development activity. The IDSP itself did not develop standards.

Efforts to Address Issues of Governance and Organizational Responsibility in Standards

Most standards address performance aspects of products or services, and/or provide technical details relevant to health or safety, etc. There is, however, a small but growing body of standards efforts focused on aspects of organizational behavior, data privacy and big data analytics.

One example is the International Organization for Standardization (ISO) family of management system standards. ISO management system standards (MSS) help organizations improve their performance by specifying repeatable steps that organizations consciously implement to achieve their goals and objectives, and to create an organizational culture that reflexively engages in a continuous cycle of self-evaluation, correction and improvement of operations and processes. Topics range from quality management to information security to anti-bribery. According to ISO, the benefits of an effective management system to an organization include:

- More efficient use of resources and improved financial performance
- Improved risk management and protection of people and the environment
- Increased capability to deliver consistent and improved services and products, thereby increasing value to customers and all other stakeholders

ISO 26000: *Guidance on Social Responsibility* is a second example. ISO 26000 was developed in response to a growing global focus on corporate responsibility. ISO 26000 defines corporate social responsibility (CSR) as the responsibility of an organization for the impacts of its decisions and activities on society and the environment, with a focus on transparent and ethical behavior that:

- Contributes to sustainable development, including the health and welfare of society;
- Takes into consideration the expectations of its stakeholders;
- Complies with applicable law and is consistent with international norms of behavior; and
- Is integrated throughout the organization and is put into practice in their relationships.

ISO 26000 provides guidance rather than requirements, so it cannot be certified to unlike some other well-known ISO standards. Instead, it helps clarify what social responsibility is, helps businesses and organizations translate principles into effective actions and shares best practices relating to social responsibility, globally. It is aimed at all types of organizations regardless of their activity, size or location.

The standard was launched in 2010 following five years of negotiations between many different stakeholders across the world. Representatives from government, NGOs, industry, consumer groups and labor organizations around the world were involved in its development, which means it represents an international consensus.

A third example is drawn from the Artificial Intelligence (AI) space. In late 2017, the U.S. assumed leadership of the newly formed ISO/IEC Joint Technical Committee (JTC) 1, Subcommittee (SC) 42 on *Artificial Intelligence*, with ANSI serving as the Secretariat. JTC 1/SC 42 is the first standardization committee of its kind looking at the full AI IT ecosystem. Artificial Intelligence is not just one technology, but is a variety of software and hardware enabling technologies (machine learning, deep learning, knowledge representation) that can be applied in various ways in a potentially unlimited number of applications. From transportation to healthcare, financial services to retail, robotics, manufacturing, and more, AI will increasingly drive global innovation to new heights. Content moderation activities, at least in part, may leverage AI.

SC42 work areas include addressing bias in AI systems and AI-aided decision-making, risk management, trustworthiness in AI, governance implications of the use of AI by organizations, and a review of ethical and societal concerns related to AI.

The Value of Relying on Standards to Support Public Policy

Reliance on voluntary, consensus standards developed in the private sector can have significant positive effects on goods, services and on quality of life. These effects are evident whether standards are employed by the private sector or by the public sector. In the private sector, they create market incentives for actors to follow accepted practices by applying competitive pressure (while allowing fair competition) and encourage innovation and growth by fostering technological development. In the public sector, they can enable greater transparency and competition in public procurement and provide essential requirements for industry via their referencing into regulations and laws.

In either context, voluntary consensus standards are efficient and cost-effective tools – they can provide detailed safety, process or performance requirements in the policy guidance or legislation without making it unnecessarily long and complicating it with technical information. And finally, there are a number of important parallels between good policy-making practice and good standardization practice, which has led to the use and referencing of voluntary consensus standards becoming widely and increasingly considered as forming part of good regulatory practice and good public governance. For example, common characteristics of good policy-making and good standardization practice include openness, transparency, effectiveness, global relevance, consensus, and input from expert opinion, with a key criterion for both being that the policy/standard responds to a verified need. Ensuring stakeholder buy-in is also an essential part of good policymaking practice.

Successful standards developing organizations emphasize the importance of stakeholder engagement and believe that it is important that stakeholders are able to express their needs in standards development efforts related to public policy.

Mary Saunders, Vice President for Government Relations and Public Policy
American National Standards Institute
1899 L Street, NW
Washington, D.C.
msaunders@ansi.org

February 13, 2020

CCIA Written Submission on Section 230
February 19 Workshop: "Section 230: Nurturing Innovation or Fostering Unaccountability?"

Overview

Section 230 is an incentive for online services, websites, and many other digital intermediaries to maintain healthy and vibrant ecosystems. It is both a shield and a sword, limiting liability pertaining to third-party content or behavior, while also enabling services to strike unlawful or injurious content or behavior by bad actors. By protecting intermediary decisions whether content is removed or not, Section 230 encourages services to fight misconduct and protect users from online harms by removing disincentives to moderate abusive behavior.

Narrowing this protection would have the perverse result of impeding online services' and websites' efforts to police bad actors. Policymakers should want to strengthen the law that empowers Internet services to take down extremist content, rather than weaken it. There is little to gain by making it harder for online services and websites to kick suspected criminals, jihadis, and foreign agents offline.

Common Misunderstandings About U.S. Intermediary Protection

Despite being recognized as one of the most important laws in U.S. technology policy, Section 230 is often misunderstood.

1. *Section 230 pertains to functions, not business models, and it thus protects far more than Internet services*. Section 230 may protect *any* "interactive computer service," *i.e.*, any entity that operates an online space where third parties may post content—including brick-and-mortar businesses. Section 230's text also explicitly protects schools, libraries, and software developers, among others, in 47 U.S.C. § 230(f)(2). Section 230 even protects traditional publishers, such as newspapers, *provided* it is functioning in an interactive computer service role, like offering a comment section on its articles. By the same token, a social media company that publishes its own content is not protected by Section 230. Accordingly, regardless of whether a company is construed as a "social media company" or a "news publisher." An entity receives Section 230 protection when it provides a "platform" for third-party speech, but receives no protection for speech it publishes on its own.

2. *Section 230 limits liability only with respect to third-party content that interactive computer services do not create, solicit or develop*. Section 230's protections are designed to enable website operators to fight misconduct and protect their users from online harms by removing disincentives to moderate abusive behavior. Courts have made clear, however, that intermediaries can forfeit their Section 230 protection in many cases, including soliciting, "developing," or otherwise participating in the authorship of unlawful content, knowingly paying for content obtained through fraudulent or illegal means, or failing to warn users about known risks (*see, e.g.*, *Roommates.com*; *Jones v. Dirty World*; *Accusearch*; *Doe v. Internet Brands*).

3. *Section 230 provides no protection from federal criminal law, and includes other exceptions as well, such as intellectual property*. Of course, Section 230 has no impact on the liability of the user who actually posted the content, who may always be subjected to litigation or prosecution for their actions. Similarly, online services that themselves engage in criminal conduct have always been liable for these actions.

Section 230's Role in Protecting Small Business

One advantage of the Internet is that startups can outsource to "the cloud" numerous resource-intensive functions which previously needed to be handled at great expense in-house. A new restaurant, for example, may rely upon remote storage, hosting and CDN services for its website, free-to-the-user tools for its email and social media marketing to prospective diners, and free office productivity services for its operational needs. Similarly, it benefits from the reviews on sites like Yelp.com, because diners can rely upon the assessments of their peers before the local food critics have deigned to bless the establishment. If Yelp faced the prospect of liability from every small business that was dissatisfied with a consumer review, this asset to consumers would disappear, diners and new businesses would suffer, and incumbents would benefit. In a time when small business formation has slowed, federal policymakers should not raise new hurdles for startups.

Policy Responses to Problematic Online Content Should Focus on Outcomes

Weakening Section 230 protections is likely to produce different responses from different online services. Smaller operators may avoid moderating content at all, since online services have less legal liability if they engage in no monitoring. As demonstrated in the 1995 *Stratton Oakmont* decision that Section 230 overturned, removing 99% of inappropriate content could create the appearance of endorsing the 1% that an online service overlooked.

An additional outcome would be firms exiting the market — or never entering it — which is also bad for competition and free expression by all stakeholders and viewpoints. Another likely outcome would be even more aggressive editorial policies. Cautious sites and services, wary of anything that could lead to risk, may only give a platform to establishment viewpoints. Marginalized communities would suffer the most, but even more conventional viewpoints may be subject to increased scrutiny by litigation-wary lawyers hoping to avoid controversy.

All stakeholders in the Section 230 debate presumably want moderation of unlawful and injurious content, without collateral damage to legitimate commerce and speech interests. At the same time, there is likely to be uniform agreement that law enforcement needs tools and resources to pursue criminal conduct. For this reason, Section 230 protections should remain, to ensure that the vast majority of intermediaries who moderate objectionable content can continue this important role.

It is evident from the pre-SESTA/FOSTA prosecution of Backpage that law enforcement has tools to prosecute bad actors operating online. Properly wielding these tools may require additional resources, and the prioritization of resources to this end would be a more appropriate focus for policy action.

"**Section 230 – Nurturing Innovation or Fostering Unaccountability?**"

Wednesday, Feb. 19, 2020
U.S. Department of Justice
Washington, D.C.

Statement of the National Center for Missing & Exploited Children regarding its views on section 230 of the Communications Decency Act.

Background on the National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children (NCMEC) is a private, non-profit organization created as a grassroots response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh was with his mother at a Florida shopping mall when he vanished without a trace. His devastated parents, John and Revé Walsh, had nowhere to turn for help. The search for Adam revealed many inadequacies that plagued missing child investigations at the time. There was no coordinated response across multiple law enforcement agencies, no AMBER Alert system to quickly deliver critical information to the public, and no place for families to go for guidance or emotional support.

Revé and John endured 10 excruciating days searching for Adam before he was found murdered 100 miles away. The Walshes channeled their grief and came together with other child advocates to create NCMEC in 1984. Over the past 35 years, NCMEC has served as the national resource center and information clearinghouse and grown to become the leading nonprofit organization addressing issues related to missing and exploited children.

NCMEC's Work to Combat Online Child Sexual Exploitation

Since 1998, NCMEC has operated the CyberTipline, the nation's centralized system for members of the public and electronic service providers (ESPs) to report suspected child sexual exploitation. The vast majority of reports to the CyberTipline are submitted by ESPs, which are required to report apparent child sexual abuse material on their platforms when they become aware of it.

Every day NCMEC sees the constant flow of horrific child sexual abuse content flooding into the CyberTipline. Since its inception almost twenty-two years ago, the CyberTipline has received more than 63 million reports; 16.9 million last year alone. The volume of images, videos, and other content related to child sexual abuse contained in CyberTipline reports continues to increase tremendously. In 2019, over 69 million images, videos, and other content relating to suspected child sexual exploitation were included in reports to NCMEC. For the first time last year, videos constituted the majority of content reported to NCMEC. Just five years ago, the number of videos included in reports to NCMEC was under 350,000; last year over 41 million videos of child sexual abuse were reported.

It's important to understand that the images, videos, and other content reported to the CyberTipline are not merely sexually suggestive or older teenagers who "look young." This is content that depicts crime scene activity and active attempts to entice and sexually abuse children. Children – many so young that they are preverbal and cannot call for help – are raped and abused in these images, and the abuse is documented on film and video and distributed repeatedly on hundreds of online platforms, email services, messenger apps, and file-sharing services. Children are revictimized every time one of their sexually abusive images is traded and a new predator finds pleasure in their anguish or uses

the image to entice another child. In NCMEC's experience, any online service that allows members of the public to share content can be misused by offenders to abuse children and perpetrate this abuse by distributing their images online.

The quantity of images and videos reported to NCMEC is unrelenting, and the continual evolution of technology combined with the global growth of the internet makes combatting these heinous crimes even more complex. The only constant is where NCMEC sees children continually victimized – on the internet. The anonymity of the internet, exacerbated on platforms where end-to-end encryption is implemented without adequate child safety measures, creates an ideal environment for predators to exploit children while often eluding detection or identification. And because technology companies have no legal obligation to search for this abuse or screen content on their systems, and no legal repercussions even when they recklessly allow this content to proliferate, children continue to be sexually abused online undetected, unreported, and continually revictimized.

While the internet can facilitate users' criminal activity, NCMEC is fortunate to have strong partnerships with many technology companies that embrace their societal and corporate responsibilities to manage content on their platforms. These valued stakeholders often go above and beyond the requirements of current law and look for innovative methods to address child sexual abuse material and implement sophisticated tools to identify this content online, report it to NCMEC, and get it taken down quickly.

But NCMEC knows that many companies are not proactive in fighting this insidious problem.[1] Some companies do not search or screen for this abusive content; they make it difficult for users to report content; they do not engage in voluntary measures or implement consistent best practices used by others; and they turn a blind eye even when they know their systems are facilitating and being used to proliferate child sexual abuse. These companies are not persuaded to do the right thing for society, and under the law cannot be obligated to do more to protect children, even when their business practices contribute directly to child sexual abuse online.

Online companies have a social responsibility to protect children on their platforms and should have a legal obligation to engage more meaningfully and consistently in these efforts. These companies should be legally liable to child victims when they act recklessly and disregard knowledge that their own conduct harmed children. There must be a consistent effort to ensure that the internet is a safer place and not used to facilitate enticing children or distributing their images of rape and sexual abuse.

NCMEC and Section 230 of the CDA

As noted above, NCMEC is fortunate to work closely with many "good actor" technology companies. But our years of tracking trends relating to online child sexual exploitation make clear that too many websites fail to undertake adequate – or any – efforts to screen for child sexual abuse material. Some technology companies know this content is being distributed on their sites, and choose to do nothing to locate, report, or remove these images. Other companies behave recklessly with regard to the distribution of child sexual abuse material on their systems, and some have actively facilitated the online sale of children for sex.

[1] http://www.missingkids.org/gethelpnow/cybertipline (see "By the Numbers").

The disparate approach of technology companies to content moderation occurs even though all interactive computer service providers are granted immunity from liability when they engage in good faith efforts to restrict content on their platforms for material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. 230(c)(2)(a). Since the enactment of the CDA, this immunity has been described as an incentive for companies to moderate content on their systems. The impact of this immunity has been more aspirational, but it is clear that the law in its current form has left a gap in child protection.

While good actor technology companies can be counted on to engage in robust content moderation efforts to combat child sexual abuse images, the internet has become so vast and global that the efforts of a few good actors are no longer enough to keep children safe online. NCMEC has seen too many disinterested and bad actor companies that disregard their immunity to moderate content and remove child sexual abuse material. These companies cannot be compelled to take action to stop the proliferation of child sexual abuse material, even though Congress has granted them extraordinary immunity to engage in these efforts. It is especially disheartening that under the law these companies cannot be held accountable for their reckless actions by child victims or state attorneys general. Today, the broad immunities of section 230 often means that there are no repercussions for companies that choose to look the other way when egregious child sexual abuse material is circulated on their platforms.

NCMEC believes that companies should share a goal to engage in consistent, industry-appropriate measures to locate, report, and remove child sexual abuse material. This should be a basic cost of doing business online under the protections granted by the CDA. NCMEC also believes that child victims should have a private right of action to hold accountable every person or entity – including interactive computer service providers – that facilitate, contribute to, perpetuate, or act recklessly to cause their abuse. NCMEC believes state attorneys general should have the authority to protect children in their states accordingly.

NCMEC has spoken out before when section 230 impeded child safety by barring victims of child sex trafficking and state attorneys general from seeking justice against Backpage.com. We supported FOSTA-SESTA's refinements to section 230 to ensure that child victims could get the justice they deserved and needed – even when the facilitator of their trafficking was a website.

NCMEC's victim-centered approach supports our mission to seek refinements to laws when child protection is compromised and children who were raped and sexually abused suffer knowing their abusive images and videos circulate online with no end in sight. We believe more must be done to distinguish good actor companies, which use section 230 immunity to aggressively and consistently moderate child sexual abuse material on their platforms, and to incentivize bad actor companies, who turn away from the suffering of children on their website and knowingly or recklessly allow online abuse, to do more.

What Needs to Change to Better Protect Children?

2020 is a much different world than 1996 when Congress enacted the broad immunity provisions within the CDA to support the growth of the internet. Our laws need to keep up with rapidly changing technology, especially when a child's safety is at stake.

NCMEC supports legal refinements that encourage all technology companies to work harder to protect children online and ensure that bad actors cannot take advantage of section 230 in a manner that causes children to be harmed. The broad immunities of the CDA should come in exchange for the same commitments already made by many of NCMEC's strongest online partners – adoption of consistent processes and technologies to detect, report, and remove child sexual abuse material.

Some recent commentary relating to renewed discussions about screening content has asserted that the issue of child sexual abuse material is being co-opted by other interests on section 230, content moderation, and/or end-to-end encryption. We couldn't disagree more. NCMEC has seen child sexual abuse proliferate online at a rate unimaginable twenty years ago. The methods to detect and report this content are simply not keeping pace with technology, not being used consistently by companies, and are currently threatened with disruption by trends around anonymization and end-to-end encryption. A core element of NCMEC's mission is to prevent and disrupt the proliferation of online child sexual abuse. From NCMEC's view, the issue of online child sexual abuse material should be a focal point in this debate. NCMEC will continue to pursue reducing this intolerable form of child victimization, and we welcome others who share our mission to stand along with us.

Under current law, companies can legally choose to avoid awareness of children being abused on their site – or even act recklessly or contribute to the abuse – and still not be liable directly to the child victim. While some companies choose to close the curtains on abuse, other companies tenaciously fight against the influx of abusive content, making determined efforts to quickly remove it and provide law enforcement with the evidence they need to prosecute offenders who harm children. Currently both types of companies enjoy equal protections under the law. NCMEC advocates for good actors to continue their efforts and bad actors to be incentivized to stop reckless inaction that harms children.

The internet was never intended to be a place where children are enticed, raped, and sexually abused. Yet, today child sexual abuse is documented in millions of images and videos and spread across the globe, often because different laws apply when this abuse occurs online. The current legal structure makes it more difficult to combat the sexual abuse of children online than offline. This is a global problem, without a single solution. But we must start addressing this problem with open eyes and a shared societal goal to protect children.

Stanford | Internet Observatory

Comments for the Workshop on CDA Section 230

February 19, 2019
U.S. Department of Justice

Alex Stamos
Director, Stanford Internet Observatory
Visiting Scholar, Hoover Institution

As one of the few workshop attendees without legal training I will spare this distinguished group my attempts at amateur legal analysis. I would, however, like to contribute some relevant observations I have made during my time working on platform safety as CISO of Yahoo and Facebook.

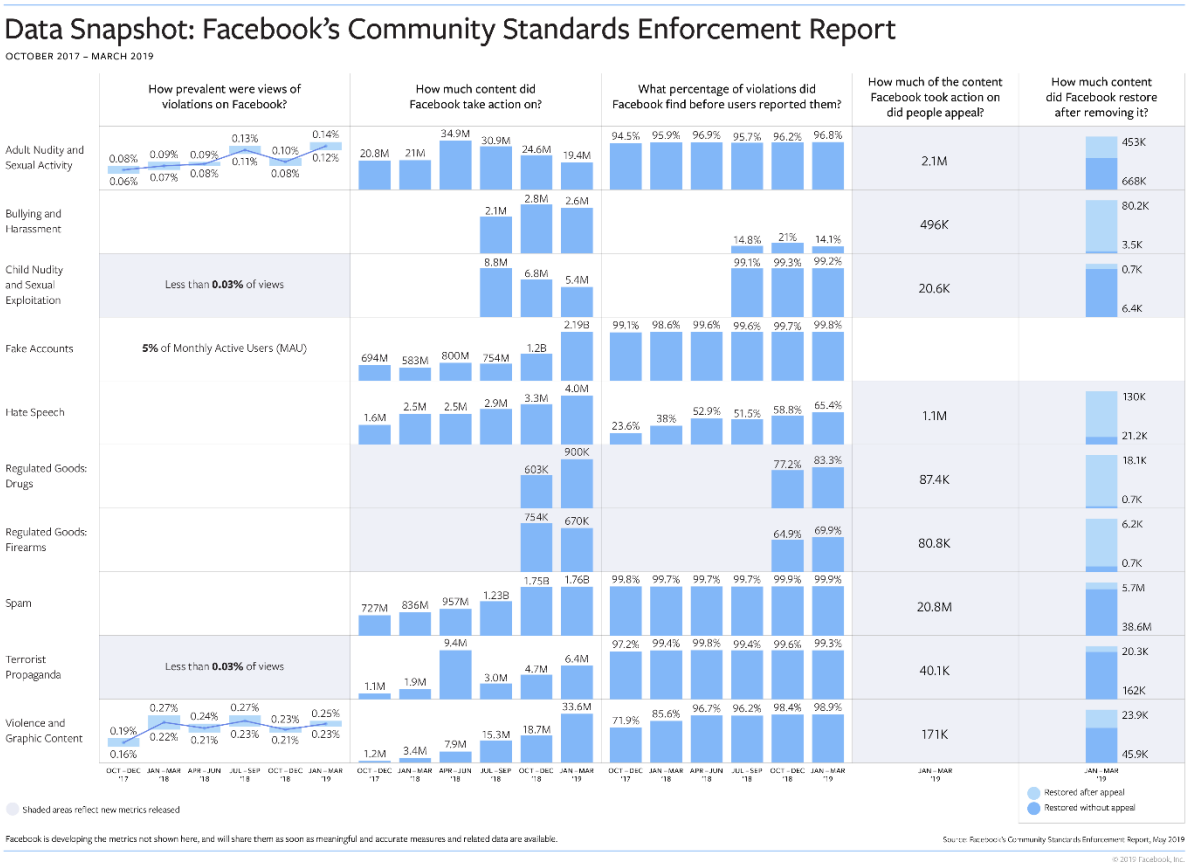
1. **Lawful and unlawful content receive very different treatment by US social media companies.**
    a. Almost all US-based platforms hosting user generated content explicitly disallow any content that is illegal in the United States.
    b. Most US-based platforms maintain their own content policies that go well above and beyond what is required by US law. They do so to make their platforms welcoming and usable to a broad cross-section of users, and to reduce the potential harm to individuals from lawful but odious behavior.
    c. Most moderated content is likely legal in the US. It is unlikely to create any civil liability for the user who created it because it does not rise to the level of violating any law, such as the laws governing harassment, defamation, or invasion of privacy.
    d. Section 230 explicitly allows for intermediate liability for intellectual property violations and unlawful content, so Section 230 is not directly relevant to issues involving IP theft, illegal speech or protected political speech.

2. **For unlawful content, the large platforms have not only made their own standards but have chosen how to balance proactive detection against the privacy rights of their users**
    a. The large platforms have built automatic detection mechanisms for a variety of different types of abuse. The most well known and standardized response has been against the exchange of child sexual abuse material (CSAM).
    b. Hundreds of companies participate in scanning for child sexual abuse material in concert with the National Center for Missing and Exploited Children (NCMEC).
    c. NCMEC's statistics are not generally available, but according to recent articles in the New York Times[1] the distribution of responsibility for NCMEC's 17 million annual reports is highly uneven, with Facebook submitting roughly 90%[2].
    d. The difference in capabilities available to each company is drastic. At Yahoo, one of my priorities was to reconstitute the child safety investigation and threat intelligence team, but resource constraints restricted our ability to grow the team beyond five full-time members.
    e. At Facebook, I supervised dedicated eCrime, child safety, counter terrorism and threat intelligence investigation teams, each with around 10-15 members. There were also dedicated investigation teams for money laundering, advertising fraud and abuse and thousands of community operations staff dedicated to online safety.
    f. These teams would often base their investigations on alerts from automated systems and escalations from the high-volume community operations teams and were responsible for the arrest of hundreds of criminals, child abusers and terrorists.
    g. Several terrorist attacks were prevented by our work during my tenure at Facebook, and our team at Yahoo was responsible for the disruption of a large Manila-based child sex trafficking ring and dozens of arrests worldwide.
    h. Any legislative action should consider the widely differing resources available to different platforms.

3. **Corporate investigation teams are carefully supervised by in-house attorneys to ensure proper adherence to privacy laws and to avoid imperiling potential prosecutions**
    a. Investigators are trained on ECPA/SCA and 4th Amendment considerations to make sure they only share information appropriately with law enforcement and to prevent claims of the companies becoming agents of the state.
    b. Still, some defendants end up claiming that this voluntary work violates their rights or creates liability for service providers[3].
    c. Any legislation that creates new obligations for service providers should be analyzed against the backdrop of current litigation to ensure it does not disrupt the capability of companies to investigate and report major abuses without a search warrant.

[1] https://www.nytimes.com/2020/02/07/us/online-child-sexual-abuse.html
[2] There is some dispute about the numbers contained in the NY Times article, possibly due to double-counting by NCMEC of abusive images and non-abusive images (such as profile images) that have been attached to reports.
[3] See *US vs Rosenow* and *Rosenow vs Facebook*

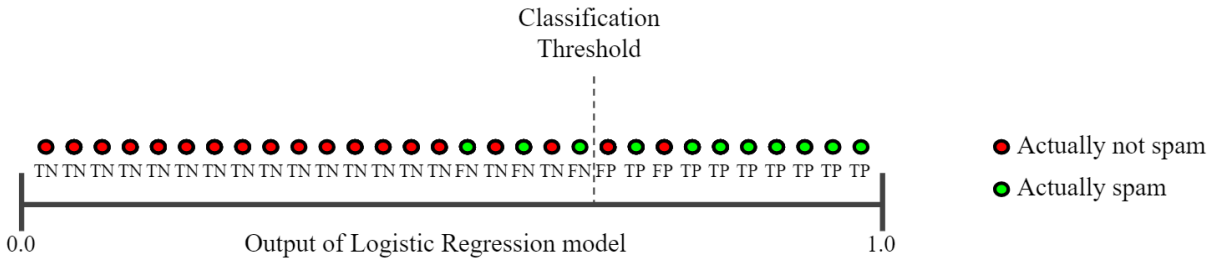
4. **It is difficult to conceptualize the scale of the content moderation challenge or the ratio between the volume of various abuse types**
    a. There is a lot of content created online.
    b. Spam massively outstrips all more serious forms of abuse.
    c. This is a graphic created for Facebook's content moderation report, released in May 2019[4].



    d. The scale of the second column is misleading. Notice that in the first quarter of 2019 (1Q2019), Facebook took down 4 million pieces of hate speech globally. That is roughly one hate speech action taken every two seconds, 24 hours a day. Facebook reported stopping 1.76B pieces of spam that quarter, or roughly 226 actions per second.
    e. Most public discussion of content moderation is driven by anecdote, not hard data. A success rate of finding 99.3% of a certain abuse type, as Facebook reported for terrorist propaganda, still leaves around 44,000 missed items each quarter that an activist or journalist might write up as definitive proof of enforcement failure.
    f. Content moderation transparency is optional. Facebook provides the most comprehensive community standards enforcement report among large providers, but even this level of transparency is not sufficient to properly judge the efficacy of their operations.

[4] https://about.fb.com/news/2019/05/enforcing-our-community-standards-3/

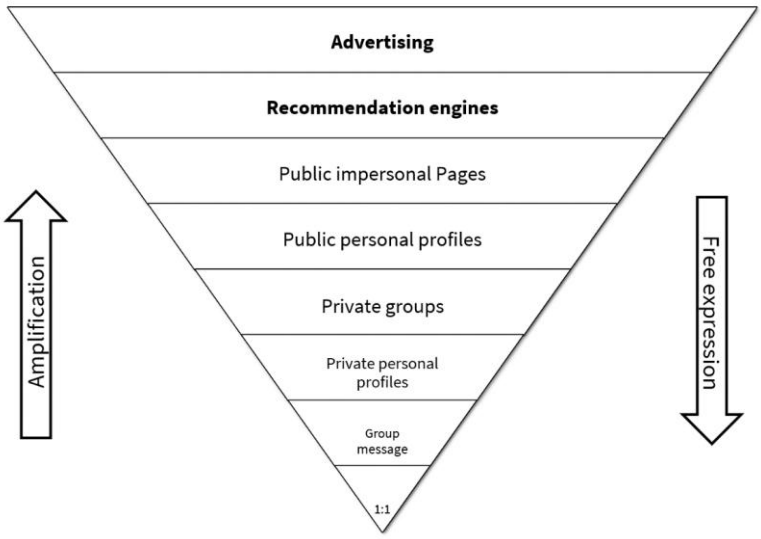
5. **Increasing the number and complexity of content moderation decisions inevitably increases the false positive rate.**
    a. Machine learning is a critical part of being able to do moderation at scale.
    b. Machine learning is not magic, it is effectively a force-multiplication tool that allows individual content reviewers to be more efficient. It cannot replace or replicate human judgment.
    c. The most common category of algorithm used for content moderation is a classifier, which attempts to calculate the likelihood that a piece of content belongs in one of two buckets. For example: is this email "spam" or "not spam"?
    d. The two most important metrics for a machine learning classifier are *precision* and *recall*. Precision measures how many of the pieces of content classified as spam really are spam. Recall, the amount of total spam that was caught.
    e. Precision and recall are always balanced against one another, as the consumer of a classifier's output will always need to draw a line upon which some action is taken. This diagram, taken from a Google course on machine learning[5], shows the tradeoffs inherent in drawing that line. Move the line to the right, and you will accidentally delete more legitimate content, move it to the left and you will miss real abusive material.



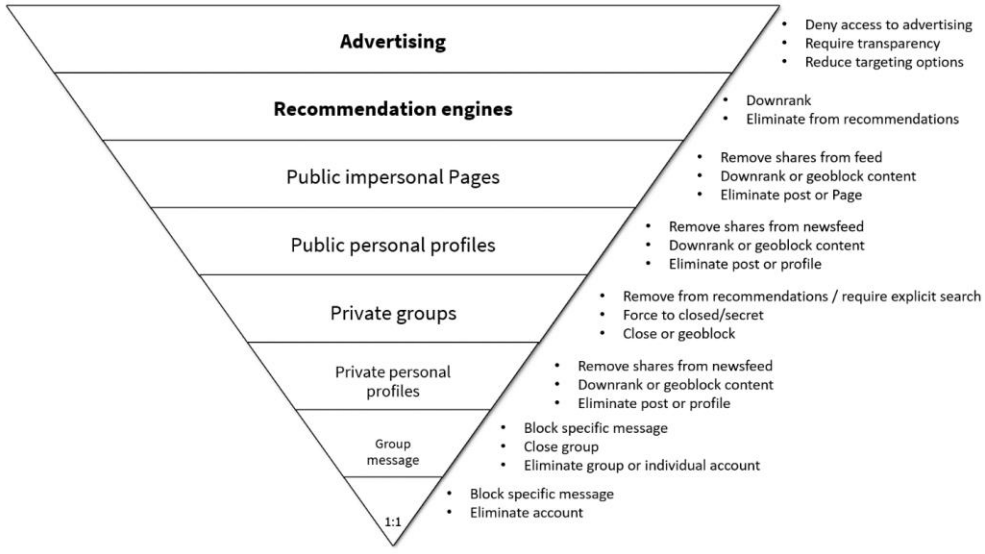
    f. Machine learning systems are trained using thousands or millions of labeled pieces of content, the initial labeling being performed by human reviewers.
    g. When rules are tweaked or changed, then that often leads to the existing machine learning process becoming unusable and needing to be re-trained with new judgments by human reviewers. This can reduce the efficacy of content moderation for a time.
    h. The more complex a decision tree, the less likely it is that either machine and human reviewers will give consistent labels to the same content.
    i. These problems are fundamental and irreducible. You can invest time and money into improving human and machine performance, but there will always be tradeoffs between complexity of rules, comprehensiveness of enforcement and accidental over-enforcement

[5] https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall

6. **Social media platforms look like cohesive experiences to users but are actually multiple products stacked together. Each product provides a different level of potential amplification of speech.**
    a. For lawful speech, I believe the focus of any reforms should be on balancing between the speech rights of the speaker, the rights of people to seek out information/speech they desire (even that speech is distasteful or false) and the privacy rights of users against the amount of amplification provided



    b. If you consider these products as different components with different levels of amplification, a variety of options other than just taking down content present themselves.



    c. Any legislative changes should consider that moderation options exist short of completely removing user generated content

7. **Most of the harm reduction on the Internet does not involve law enforcement**
    a. Each piece of content represented in moderation transparency reports represents an operational action that was taken by a company.
    b. Companies also design their products to reduce the occurrence of certain types of abuse. For example, Instagram is testing mechanisms to warn posters when their messages might be considered harassing before they post.
    c. For the tens of millions of images reported to NCMEC, it is believed that the number of prosecutions might number in the thousands[6].
    d. The prosecution of the worst offenders is important, but the size of those prosecutions is dwarfed by the overall amount of moderation and harm reduction that occurs.

8. **End-to-end encryption is the most powerful mechanism we have to reduce the impact of breaches.**
    a. End-to-end encryption (E2EE) puts data outside of the reach of the provider of a communication service.
    b. This means that a serious breach of a provider's systems might reveal basic subscriber and some message metadata but will not be able to access message content. This is a massive improvement over the status quo, where such breaches (which happen regularly) can lead to real risk for both individuals and the security of the United States.
    c. A tenant of modern security practice is to reduce the risk inherent in one's systems by reducing the amount of data available. End-to-end encryption is the most powerful tool we currently have to reduce risk on communication platforms.
    d. We are only at the beginning of the battle between American and Chinese internet companies to serve the information needs of the world. It is highly unlikely that Chinese companies will ever provide privacy-enhancing features such as end-to-end encryption, and effectively outlawing E2EE weakens up one of the few advantages the US has in this battle.

9. **There are options to reduce the harm of end-to-end encrypted networks without creating backdoors and with controllable privacy impact**
    a. The Stanford Internet Observatory has been running a series of workshops on possible ways to reduce the abuse of end-to-end encrypted messaging products with minimal privacy and security impacts. The first three were held at Stanford, the Real World Crypto conference and the European Parliament and included representatives from child safety groups, privacy NGOs, law enforcement, intelligence agencies, academia and technology companies.

[6] There is no good data available on the outcomes from NCMEC reports and this is a potential area for academic study before any action is taken

b. We believe that addressing abuse on E2E networks requires a more nuanced separation of abuse types and a classification of their fundamental aspects. Here is a draft chart that does so.

Abuse	Prevalence	Impact	Illegal	Victim in convo?	Image based	Amplification -> harm	Metadata useful to LE	ML on content possible
Spam	Very High	Low	No	Yes	Sometimes	Yes	Yes	Yes
Malicious documents/links	High	High	Yes	Yes	Sometimes	Yes	Yes	Yes
Targeted harassment	High	Moderate-High	Rarely	Yes	Sometimes	No	Yes	Yes
CSAM trading	High	High	Yes	No	Yes	No	Yes	Yes
Sextortion/ Grooming	Moderate	High	Yes	Yes	No	No	Yes	Yes
Live abuse	Low	High	Yes	No	Yes	No	Yes	Maybe
Incitement to violence	Low	High	Sometimes	No	Sometimes	Yes	Maybe	Yes
Disinformation	Moderate	Low	No	Yes	Sometimes	Yes	Maybe	Yes
NCII	Moderate	High	Sometimes	Sometimes	Yes	No	Yes	Only with priming from victim
Criminal conspiracy	Low	High	Yes	No	No	No	Yes	No

c. Once you divide the problem by types of abuse, you can consider possible solutions, like below.

Potential Mitigation	Description	Potentially targeted abuses	Impact on liberty/privacy
Limits to group size	Capping group sizes, or reducing certain invite mechanisms (like external URLs) at certain sizes	Disinformation, incitement, spam, malware	**Low**. Would handicap individuals (such as independent journalists) who rely on platforms to reach broad audiences
Limits to forwarding/amplification	Setting limits on the amount of times a user can forward a message or a message can be forwarded	Disinformation, incitement, spam, malware	**Low**. Would impinge on speech whether it abuses ToS or not. Might create traceability.
Client-side image fingerprinting	Push image hashsets to clients to look for banned images	CSAM trading, NCII, disinformation, incitement	**Low-High.** Depends on what actions are automatically taken. Is the image prevented from being sent, user prompted to report or automatically reported?
Client-side ML detection and guided reporting	Use ML on the client (with server-side model training) to detect potential abuse, prompting the user to securely report the conversation/group	Targeted harassment, disinformation, incitement, spam, malware, CSAM trading, NCII, sextortion/grooming	**Moderate**. Has a human user in the loop but could be used by authoritarians to prompt users to report for political content.
Detection and removal of fake accounts with metadata-based ML	Using ML to identify inauthentic behavior patterns and registration data	All	**Low**. Will have irreducible FPs, might require retention of more metadata
Historical metadata available with process	Storing conversational metadata and providing it with lawful process (e.g. who is in which groups, when messages are sent)	CSAM trading, sextortion, criminal conspiracies, incitement,	**High**. Creates potential for law enforcement overreach, corporate surveillance

d. I have seen no legislative proposals that would allow for solutions such as these.

10. **The incumbent tech giants will welcome weakening of Section 230 to create a durable competitive advantage.**
    a. Silicon Valley's most successful companies have traditionally been built on the corpses of the predecessors they disrupted and replaced.
    b. This cycle has been weakened by the capital and data advantages that have been built by the current large incumbents. Multiple competition regulators around the world have noticed these moats and are moving to reduce their effectiveness at warding off new competitors.
    c. Legislation that creates a huge burden for hosting user-generated content is an attractive option to the large incumbents for gaining a government-supported advantage.
    d. I believe that Facebook would welcome a legislative environment where billions of dollars of artificial intelligence and tens of thousands of content moderators are required to host user generated content. This would lock in Facebook's position and greatly increase its negotiating leverage over rapidly growing competitors that cannot keep up with the subsequent growth in legal liability.

11. **In conclusion…**
    a. Any legislative changes should be based upon empirical data, not anecdotes or assumptions.
    b. Policymakers should consider ways to engage with the reality of how content moderation occurs at large platforms, including embedding their staffers with actual content policy, content operations and investigation teams.
    c. Legislators should engage with the reality that the vast majority of online harms is currently prevented by tech platforms, not law enforcement.
    d. The best practices in fighting various forms of abuse are still emerging. There is no one checklist that fits every platform and any such checklist would be extremely difficult for a government body to maintain.
    e. Any changes to Section 230 should be carefully constructed to not disrupt the careful legal balance upon which companies are able to cooperate with each other and law enforcement today.
    f. Changes to Section 230 that restrict the ability of American companies to deploy end-to-end encryption will greatly reduce the security of American citizens and the competitiveness of the US tech industry, especially against consumer technology companies in the People's Republic of China.
    g. Increasing the risk of hosting user generated content will naturally benefit large companies with sophisticated content moderation, large legal teams and the ability to self-insure. This might be a reasonable tradeoff, but nobody should think that eliminating Section 230 will help competition. Such an action would effectively restrict the space of possible UGC hosts to the current giants.

Liability for User-Generated Content Online
Principles for Lawmakers
July 11, 2019

Policymakers have expressed concern about both harmful online speech and the content moderation practices of tech companies. Section 230, enacted as part of the bipartisan Communications Decency Act of 1996, says that Internet services, or "intermediaries," are not liable for illegal third-party content except with respect to intellectual property, federal criminal prosecutions, communications privacy (ECPA), and sex trafficking (FOSTA). Of course, Internet services remain responsible for content they themselves create.

As civil society organizations, academics, and other experts who study the regulation of user-generated content, we value the balance between freely exchanging ideas, fostering innovation, and limiting harmful speech. Because this is an exceptionally delicate balance, Section 230 reform poses a substantial risk of failing to address policymakers' concerns and harming the Internet overall. We hope the following principles help any policymakers considering amendments to Section 230.

***Principle #1*: Content creators bear primary responsibility for their speech and actions.**

Content creators—including online services themselves—bear primary responsibility for their own content and actions. Section 230 has never interfered with holding content creators liable. Instead, Section 230 restricts only who can be liable for the harmful content created *by others*.

Law enforcement online is as important as it is offline. If policymakers believe existing law does not adequately deter bad actors online, they should (i) invest more in the enforcement of existing laws, and (ii) identify and remove obstacles to the enforcement of existing laws. Importantly, while anonymity online can certainly constrain the ability to hold users accountable for their content and actions, courts and litigants have tools to pierce anonymity. And in the rare situation where truly egregious online conduct simply isn't covered by existing criminal law, the law could be expanded. But if policymakers want to avoid chilling American entrepreneurship, it's crucial to avoid imposing criminal liability on online intermediaries or their executives for unlawful user-generated content.

***Principle #2:* Any new intermediary liability law must not target constitutionally protected speech.**

The government shouldn't require—or coerce—intermediaries to remove constitutionally protected speech that the government cannot prohibit directly. Such demands violate the First Amendment. Also, imposing broad liability for user speech incentivizes services to err on the side of taking down speech, resulting in overbroad censorship—or even avoid offering speech forums altogether.

***Principle #3*: The law shouldn't discourage Internet services from moderating content.**

To flourish, the Internet requires that site managers have the ability to remove legal but objectionable content—including content that would be protected under the First Amendment from censorship by the government. If Internet services could not prohibit harassment, pornography, racial slurs, and other lawful but offensive or damaging material, they couldn't facilitate civil discourse. Even when Internet services have the ability to moderate content, their

moderation efforts will always be imperfect given the vast scale of even relatively small sites and the speed with which content is posted. Section 230 ensures that Internet services can carry out this socially beneficial but error-prone work without exposing themselves to increased liability; penalizing them for imperfect content moderation or second-guessing their decision-making will only discourage them from trying in the first place. This vital principle should remain intact.

***Principle #4*: Section 230 does not, and should not, require "neutrality."**

Publishing third-party content online never can be "neutral."[1] Indeed, every publication decision will necessarily prioritize some content at the expense of other content. Even an "objective" approach, such as presenting content in reverse chronological order, isn't *neutral* because it prioritizes recency over other values. By protecting the prioritization, de-prioritization, and removal of content, Section 230 provides Internet services with the legal certainty they need to do the socially beneficial work of minimizing harmful content.

***Principle #5*: We need a uniform national legal standard.**

Most Internet services cannot publish content on a state-by-state basis, so state-by-state variations in liability would force compliance with the most restrictive legal standard. In its current form, Section 230 prevents this dilemma by setting a consistent national standard—which includes potential liability under the uniform body of federal criminal law. Internet services, especially smaller companies and new entrants, would find it difficult, if not impossible, to manage the costs and legal risks of facing potential liability under state civil law, or of bearing the risk of prosecution under state criminal law.

***Principle #6*: We must continue to promote innovation on the Internet.**

Section 230 encourages innovation in Internet services, especially by smaller services and start-ups who most need protection from potentially crushing liability. The law must continue to protect intermediaries not merely from liability, but from having to defend against excessive, often-meritless suits—what one court called "death by ten thousand duck-bites." Without such protection, compliance, implementation, and litigation costs could strangle smaller companies even before they emerge, while larger, incumbent technology companies would be much better positioned to absorb these costs. Any amendment to Section 230 that is calibrated to what *might* be possible for the Internet giants will necessarily *mis*-calibrate the law for smaller services.

***Principle #7*: Section 230 should apply equally across a broad spectrum of online services.**

Section 230 applies to services that users never interact with directly. The further removed an Internet service—such as a DDOS protection provider or domain name registrar—is from an offending user's content or actions, the more blunt its tools to combat objectionable content become. Unlike social media companies or other user-facing services, infrastructure providers cannot take measures like removing individual posts or comments. Instead, they can only shutter entire sites or services, thus risking significant collateral damage to inoffensive or harmless content. Requirements drafted with user-facing services in mind will likely not work for these non-user-facing services.

---

[1] We are addressing neutrality only in content publishing. "Net neutrality," or discrimination by Internet access providers, is beyond the scope of these principles.

Individual Signatories

Affiliations are for identification purposes only

1. Prof. Susan Ariel Aaronson, Elliott School of International Affairs, George Washington University
2. Prof. Enrique Armijo, Elon University School of Law
3. Prof. Thomas C. Arthur, Emory University School of Law
4. Farzaneh Badiei, Internet Governance Project, Georgia Institute of Technology (research associate)
5. Prof. Derek Bambauer, University of Arizona James E. Rogers College of Law
6. Prof. Jane Bambauer, University of Arizona James E. Rogers College of Law
7. Prof. Annemarie Bridy, University of Idaho College of Law
8. Prof. Anupam Chander, Georgetown Law
9. Lydia de la Torre, Santa Clara University School of Law (fellow)
10. Prof. Sean Flynn, American University Washington College of Law
11. Prof. Brian L. Frye, University of Kentucky College of Law
12. Prof. Elizabeth Townsend Gard, Tulane Law School
13. Prof. Jim Gibson, University of Richmond, T. C. Williams School of Law
14. Prof. Eric Goldman, Santa Clara University School of Law
15. Prof. Edina Harbinja, Aston University UK
16. Prof. Gus Hurwitz, University of Nebraska College of Law
17. Prof. Michael Jacobs, DePaul University College of Law (emeritus)
18. Daphne Keller, Stanford Center for Internet and Society
19. Christopher Koopman, Center for Growth and Opportunity, Utah State University
20. Brenden Kuerbis, Georgia Institute of Technology, School of Public Policy (researcher)
21. Prof. Thomas Lambert, University of Missouri School of Law
22. Prof. Stacey M. Lantagne, University of Mississippi School of Law
23. Prof. Sarah E. Lageson, Rutgers University-Newark School of Criminal Justice
24. Prof. Jyh-An Lee, The Chinese University of Hong Kong
25. Prof. Mark A. Lemley, Stanford Law School
26. Thomas M. Lenard, Senior Fellow and President Emeritus, Technology Policy Institute
27. Prof. David Levine, Elon University School of Law
28. Prof. Yvette Joy Liebesman, Saint Louis University School of Law
29. Yong Liu, Hebei Academy of Social Sciences (researcher)
30. Prof. Katja Weckstrom Lindroos UEF Law School, University of Eastern Finland
31. Prof. John Lopatka, Penn State Law
32. Prof. Daniel A. Lyons, Boston College Law School
33. Geoffrey A. Manne, President, International Center for Law & Economics; Distinguished Fellow, Northwestern University Center on Law, Business & Government
34. Prof. Stephen McJohn, Suffolk University Law School
35. David Morar, Elliott School of International Affairs, George Washington University (visiting scholar)
36. Prof. Frederick Mostert, The Dickson Poon School of Law, King's College London
37. Prof. Milton Mueller, Internet Governance Project, Georgia Institute of Technology
38. Prof. Ira S. Nathenson, St. Thomas University (Florida) School of Law
39. Prof. Christopher Newman, Antonin Scalia Law School at George Mason University
40. Prof. Fred Kennedy Nkusi, UNILAK
41. David G. Post, Beasley School of Law, Temple University (retired)
42. Prof. Betsy Rosenblatt, UC Davis School of Law (visitor)
43. Prof. John Rothchild, Wayne State University Law School

44. Prof. Christopher L. Sagers, Cleveland-Marshall College of Law
45. David Silverman, Lewis & Clark Law School (adjunct)
46. Prof. Vernon Smith, George L. Argyros School of Business and Economics & Dale E. Fowler School of Law, Chapman University
47. Prof. Nicolas Suzor, QUT Law School
48. Prof. Gavin Sutter, CCLS, School of Law, Queen Mary University of London
49. Berin Szóka, President, TechFreedom
50. Prof. Rebecca Tushnet, Harvard Law School
51. Prof. Habib S. Usman, American University of Nigeria
52. Prof. John Villasenor, Electrical Engineering, Public Policy, and Law at UCLA
53. Prof. Joshua D. Wright, Antonin Scalia Law School at George Mason University

Institutional Signatories

1. ALEC (American Legislative Exchange Council) Action
2. Americans for Prosperity
3. Center for Democracy & Technology
4. Competitive Enterprise Institute
5. Copia Institute
6. Freedom Foundation of Minnesota
7. FreedomWorks
8. Information Technology and Innovation Foundation
9. Innovation Economy Institute
10. Innovation Defense Foundation
11. Institute for Liberty
12. The Institute for Policy Innovation (IPI)
13. International Center for Law & Economics
14. Internet Governance Project
15. James Madison Institute
16. Libertas Institute
17. Lincoln Network
18. Mississippi Center for Public Policy
19. National Taxpayers Union
20. New America's Open Technology Institute
21. Organization for Transformative Works
22. Pelican Institute
23. Rio Grande Foundation
24. R Street Institute
25. Stand Together
26. Taxpayers Protection Alliance
27. TechFreedom
28. Young Voices

The "S" in "Notice-and-Takedown" Stands for "Security"

Eugene Volokh
UCLA School of Law
volokh@law.ucla.edu

Dear Fellow Workshop Members:

I'm sure that many of you have written in detail about the various advantages and disadvantages of the current § 230 scheme. Instead of repeating that, I wanted to focus on the one area where I've done original research, and which may shed some light on any possible notice-and-takedown alternatives to § 230.

My key point: Any notice-and-takedown scheme is likely to be plagued with massive attempted fraud—if such a scheme is to be implemented, it should be implemented in a way that minimizes this danger.

* * *

In 2016, Google received a copy of a Miami-Dade County default judgment in *MergeworthRX, Inc. v. Ampel*, No. 13-13548 CA. A certain web page, the judgment said, was libelous:

> 2. The reports posted on or about December 30, 2014 by Defendant, CELIA AMPEL on www.bizjournals.com regarding Plaintiffs, MERGEWORTHRX, INC. and STEPHEN CICHY (the "Report"), which is available at http://www.bizjournals.com/southflorida/news/2014/12/30/miami-acquisition-cpmpany-mergeworthrx-to-dissolve.html contains defamatory statements regarding Plaintiffs.

The submitter therefore asked Google to "deindex" that page—remove it from Google's indexes, so that people searching for "mergeworthrx" or "stephen cichy" or "anthony minnuto" (another name mentioned on the page) wouldn't see it.

Google often acts on such requests, as it did on this one, effectively vanishing the material from the Internet. And why not? It's a service to Google's users, who presumably want to see true information, not information that's been found libelous. It's good for the people who were libeled. It can let people at Google feel that they are doing good. And it's respectful of the court judgment, even though it's not strictly required by the judgment. Win-win-win-win.

Except there was no court order. Case No. 13-13548 CA was a completely different case. Celia Ampel, a reporter for the South Florida Daily Business Review, was never sued by MergeworthRX. The file submitted to Google was a forgery.

It was one of more than 85 forgeries that I have found that were submitted to Google (and to a few hosting platforms). Google's well-meaning deindexing policy has prompted a rash of such forgeries, some seemingly home-brewed and some done for money as part of a "reputation management company" business model. Such reputation management, whether fraudulent or otherwise, is big business.

And those 85 items are just the outright forgeries, which are possible for Google to spot. Google seems to check most of the submissions it gets against court records, many of which are available online (as the Miami-Dade County records are). Most such forgeries, I think, are identified as forgeries and thus ignored by Google—though, a few, such as the *MergeworthRX* forgery, do get acted on.

But what if a reputation management company engineers a real lawsuit involving a fake defendant? It sends the court a complaint, purportedly from the plaintiff, and an answer admitting liability and stipulating to a judgment, purportedly from the defendant. The court is generally happy to accept the apparent stipulation, enter the

injunction, and get the case off its docket—having no idea, of course, that the defendant doesn't really exist. I've found about 30 cases that seem to fit this pattern.

Or what if such a company engineers a real libel lawsuit involving a real defendant—but one who has nothing to do with the allegedly libelous post? The company again sends the court a complaint and an answer with a stipulation, and the answer and stipulation are signed by the real defendant; indeed, the defendant's signature is even notarized. It's just that the stipulation that the defendant authored the post and admits that it's false is itself false. But again, the court doesn't know, so it issues the injunction; and Google doesn't know that, either. I've found what appear to be about 30 of those, though here the evidence is less open and shut.

Or what if the plaintiff doesn't try really hard to find the defendant, but instead gets authorization to serve the defendant by publication (which the defendant is nearly certain never to learn about), and then gets a default judgment when the defendant doesn't show up? In normal lawsuits, where the point of the judgment is to get damages or force the defendant to do something, defendants would move to set aside the defaults on the grounds that they hadn't been properly served, and would often win. But the point of these particular lawsuits isn't to get the defendants to do something: It's to persuade Google to do something, and Google has no idea whether the plaintiffs had done a good enough job of finding the defendants. I've found likely around 50 cases like this, though here too the evidence is less clear.

And there's more: Some orders, for instance, were gotten against people who wrote comments attached to mainstream media articles, but were then submitted to Google in an attempt to deindex the whole article, though there is no evidence that the underlying article is libelous. Indeed, it's possible that some of the comments were actually planted by a reputation management company precisely as an excuse to justify the lawsuit.

Some other orders have the URLs of government documents or of newspaper articles buried in a long list of URLs that were supposedly written by the defendant, even though there's no reason to think the defendant posted those documents. Still others use alleged confessions by defendants quoted in newspaper articles as a tool for trying to vanish the article as a whole.

In all, I found about 700 seemingly legitimate U.S. libel case orders submitted to Google for takedown and then forwarded to the Lumen Database from 2012 up to mid-October 2016. I also found, from the same date range,

- over 50 forged orders (my total forgery count includes some post-October 2016 submissions),
- over 30 fake-defendant cases,
- likely over 30 fake-claim-of-authorship cases,
- about 10 cases aimed at deindexing government documents or newspaper articles, which were undoubtedly not written by the defendant, and
- about 60 cases in which there seemed to be no real attempt to track down and serve the defendant.

That's a total of about 180 either obviously forged or fraudulent or at least highly suspicious cases. (I should add that I've tried to report all the clear forgeries and frauds to law enforcement or to court authorities, but this has led, to my knowledge, to only three forgery prosecutions, one bar discipline in a fake-defendant scam, one judicial sanctions order in a fake-defendant scam, and one state attorney general enforcement

action in a fake-claim-of-authorship scam. Perhaps this misbehavior would be less frequent if it were more commonly prosecuted—but many laws, as we know, are too often flouted and too rarely enforced.)

And it's hard to tell how many of the 700 seemingly legitimate orders might also have involved various kinds of frauds that were just too subtle to catch. I'm sure there are many perfectly proper libel judgments that lead to deindexing requests. But many deindexing orders are suspect in various ways. I go through the details of these shenanigans—and others—in a forthcoming Utah Law Review article (see http://www.law.ucla.edu/volokh/shenanigans.pdf).

* * *

All these phenomena have, of course, arisen in an era when 47 U.S.C. § 230 has largely immunized online intermediaries from liability posted by third parties. But say § 230 is replaced, even in part, with a notice-and-takedown regime, under which Google or hosting services or other platforms have to remove material on demand—or risk liability. The incentive to use such frauds would then become even greater, since fraudulent orders, like genuine orders, would be more likely to succeed in getting a platform to remove or deindex material. And the difficulty of identifying these frauds will remain.

Say, for instance, that WordPress gets a notice that some blog post on a blog it hosts allegedly libels Joe Schmoe. How is WordPress to know whether the blog post is indeed libelous?

WordPress would presumably e-mail the blogger to hear his side of the story; but the result is likely to be a "Did Not!"/"Did Too!" dispute that WordPress may find hard to adjudicate—especially given that both the complainant and the blogger might be lying. Even if (as with the copyright notice-and-comment regime) the parties are required to file statements under penalty of perjury, we know this is going to be of little use.

People whose reputations are on the line, and companies hired by those people, are often willing to forge court orders, file fraudulent court documents, and perjure themselves in court filings. It follows that plenty of people will lie when it comes to mere takedown demands and libel lawsuit threats. And hard as it is to get prosecutors to prosecute for outright forgery of judges' signatures, it would likely be harder still to get them to prosecute over perjury in documents that never made their way to court.

This problem is likely to be more severe than with copyright law, because a typical libel dispute tends to be harder to resolve than a typical copyright dispute. If someone posts an unauthorized literal copy of *Game of Thrones* on his site, it will usually be clear that it's a copy, and it will often be clear that it's not licensed by HBO and not a fair use (especially if it's a literal copy posted with no commentary, parody, or other justification). But in libel cases, if someone posts an allegation that some lawyer, doctor, or plumber has served him badly, it will often not be at all clear whether that allegation is correct.

And even copyright takedown notices often prove to be unfounded; indeed, some such notices appear to be part of organized fraudulent schemes. Here's one, for instance, sent to Google in the name of Fox18 News Network LLC, asking that Google deindex a *New York Daily News* article:

> Copyright claim #1 ...
>
> DESCRIPTION the source of my article is being used here . Everything is copied and even the image . Please look into this matter .

> ORIGINAL URLS: http://fox18news.com/2014/11/25/teen-missing-from-north-carolina-wilderness-therapy-camp-found-dead-after-breaking-hip-in-stream-autopsy/
>
> ALLEGEDLY INFRINGING URLS: http://www.nydailynews.com/news/national/teen-missing-n-therapy-camp-found-dead-article-1.2025238 [1]

The *Daily News* article did indeed have the same text as Fox 18 News, and the Fox 18 article was dated Apr. 25, 2014, one day before the *Daily News* article. Things thus looked clear: The *Daily News* article infringed the Fox 18 article. And indeed, Google apparently deindexed the *Daily News* article.

But how do we know when the Fox 18 article was actually posted? We could have looked at the date stamp on the article, but that's on Fox 18's site, and under its control. We might be able to see the creation date of Fox 18's web page, but that too was under its control; computer owners can change the creation dates of files on their own computers.

In fact, tracking down when the Fox18News.com site was registered suggests that the site wasn't even set up until 2016, over a year after the Daily News article was posted. It is the Fox 18 version that's the copy of the Daily News original—a copy backdated to pretend to be the original. And this is just one of many examples of this DMCA backdating scam; and there are other kinds of fraudulent DMCA takedown attempts as well.

Any notice-and-takedown libel regime would thus set a challenging task for Google, WordPress, and every site, large or small, that allows user comments. Such platforms would have to evaluate claims about which allegations are true and false—what courts are generally supposed to do, however imperfectly—but without the tools that courts have: no cross-examination, no subpoena authority, no realistic risk of punishment for false statements within the takedown process.

Moreover, the virtue of notice-and-takedown compared to the current regime—that it would be vastly cheaper and quicker for complainants to use, compared to the costs and delays of litigation—would likely become a vice. Imagine that everyone can indeed easily and cheaply demand that (say) Google deindex material that allegedly libels them, and (unlike now) their demands have real teeth, in the form of the threat that Google would lose its immunity if it rejects the demands. Everyone would then indeed make such demands. And many of the demands won't just be about genuine libels but also about insulting opinions, or about claims that are in reality accurate.

And, as the evidence I've gathered suggests, some of those demands would be backed by forgeries, fake witnesses, and barefaced lies. If people are willing to do that even in court proceedings, in front of government officials with the power to jail people for contempt or impose meaningful financial sanctions, they are likely to be much more willing to do so in informal notice-and-takedown proceedings where no government official is likely to intervene.

(A libel notice-and-takedown regime based on the DMCA might call on Google, WordPress, and the like to restore taken down material if the author challenges the takedown demand, unless the challenger promptly files suit against the author. But under such a DMCA-based regime, material would still stay down, based just on the takedown demand, until the lawsuit is done, which could be many years in the future—a powerful tool for censorship of any statements that are merely alleged to be libelous, and the analog of *ex parte* preliminary injunctions against libels, which are generally

---

[1] This example is borrowed from Mostafa El Manzalawy, *Data from the Lumen Database Highlights How Companies Use Fake Websites and Backdated Articles to Censor Google's Search Results*, LUMEN, Aug. 24, 2017, http://www.lumendatabase.org/blog_entries/800.

unconstitutional. The only way to avoid such censorship under this DMCA-based regime would be for Google, WordPress, and similar companies to examine such takedown demands and see if they seem to have enough substantive merit; and that raises all the factfinding concerns discussed in the text.)

To be sure, perhaps it's possible to design some effective notice-and-takedown procedure that would minimize the risk that constitutionally protected speech would be taken down by intermediaries who are afraid of liability. I certainly can't rule that out a priori. But any such system will create a massive incentive—a far greater incentive than under the current system—for complainants to cheat; and it would need to somehow be designed to deal with such cheating.

Of course, this is not by itself a categorical reason to reject notice-and-takedown systems. Perhaps they can be designed in a way that minimizes the risk of fraud; or perhaps their net benefit exceeds their net harm, even with the risk of fraud. But any such system needs to be considered with the risk of strategic misuse in mind.

Eugene Volokh

Remarks Concerning Communications Decency Act §230

Benjamin C. Zipursky
Professor of Law and James H. Quinn '49 Chair in Legal Ethics
Fordham Law School

United States Department of Justice Workshop on 230
Washington D.C.
February 19, 2020

Good morning. Knowledge of the common law of torts turns out to be vitally important to understanding the §230 of the Communications Decency Act. That is what I regard as my principal contribution to this panel.[1]

First and foremost, the common law of torts tends to place a great deal of weight on the distinction between bringing about harm and failing to stop others from bringing about harm. In negligence law, this is famously seen in the principle that carelessly running down a stranger with one's car will generate a negligence claim, but carelessly failing to pull a stranger from the path of another car will not. Negligence law of course has exceptions. A boarding school, for example, can be held liable for failure to protect its students from being assaulted in their dormitory; that is because a boarding school is said to have a special relationship to its students that generates an affirmative duty to protect them.

This "misfeasance/nonfeasance" distinction, as torts professors call it, plays at least an implicit role in virtually all torts. It is not generally enough to ask whether the plaintiff would have the injury in question if the defendant had engaged in a different course of conduct. What matters is whether a defendant is *doing* something – *punching a person in the nose* rather than *failing to stop someone else from punching him in the nose* or *owning the tavern in which the punch occurs*.

In defamation law, be it libel or slander, publication is normally an act. For example, the New York Times printed up millions of copies of the paper that contained the allegedly defamatory advertisement over which it was sued in *New York Times v. Sullivan*. Its act of printing the advertisement and marketing it to the public constitute publication. By contrast, a hotel's failure to throw out all of its copies of the defamatory New York Times would not count

[1] For more detailed versions of the analysis here, see Benjamin C. Zipursky, *Online Defamation, Legal Concepts, and the Good Samaritan*, 51 VAL. L. REV. 1 (2016); Benjamin C. Zipursky, *Thinking in the Box in Legal Scholarship: The Good Samaritan and Internet Libel,* 66 J. LEG. ED. 55 (2016-17); JOHN C.P. GOLDBERG AND BENJAMIN C. ZIPURSKY, RECOGNIZING WRONGS 319-39 (Harvard University Press 2020).

as publication, even if fewer people would have read the defamatory words had it done so. It is far less clear whether the common law of libel has real exceptions, and even if it does, it is even less clear what their parameters are and whether they would survive the *New York Times v. Sullivan* revolution in First Amendment law. Terminologically, the question is what will satisfy "the publication element" of the tort of libel.

There are a few cases ruling that the act of selling what someone else has published can satisfy the publication element if one has notice. And a couple of flimsy cases suggest that the owner of a wall on which someone else has placed a defamatory message has a duty to remove the message; in saying this – which is far from uncontroversial – courts have meant that the property owner's failure to remove the defamatory posting after notice is given will satisfy the publication element. On the other hand, no court has been willing to say that the provider of telephone lines and service can be held liable for the slanderous words spoken by third parties over the telephone.

In the early 1990s, legal scholars began writing articles and law review notes about how internet service providers would fit into this framework. Bear in mind that the 1980s and the early 1990s were a time when tort scholars and courts were increasingly skeptical about the normative relevance of a misfeasance/nonfeasance distinction, and many were increasingly interested in extending liability to deep pockets regardless of where their conduct fit into a framework of doing or preventing. Some scholars advocated for the expansion of the aforementioned categories to ISP's. The judge in *Cubby v. CompuServe*[2] did not impose liability on CompuServe, but in dicta he indicated that an ISP serving as a sort of library for content providers might indeed satisfy the publication element if it had been provided with notice of the defamatory content of material it was making accessible to its subscribers.

The plaintiff's lawyers in *Stratton Oakmont*[3] expressly drew upon the affirmative duty logic of negligence law in crafting their argument that Prodigy satisfied the publication element for an anonymous poster's allegedly defamatory post. One of the exceptions in negligence law is that one who has undertaken to protect someone from the harm that an external source or a third party is causing *does* have a duty to protect them. The misfeasance/nonfeasance distinction fails to protect the defendant who has made such an undertaking. The plaintiff argued that because

[2] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 2d 135 (S.D.N.Y. 1991).
[3] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

Prodigy had undertaken to its consumers and to the public to engage in screening and filtering, it should be treated as satisfying the publication element; it should be treated as a publisher. The New York trial judge in *Stratton Oakmont* accepted this argument, and Prodigy was on the hook.

The internet industry was predictably outraged by this decision, and it sensibly went to Washington to argue that this New York trial court was standing in the way of what federal lawmakers wanted. No company would now volunteer to filter or screen content, because doing so would count as satisfying the publication element in a libel claim. The undertaking-therefore-affirmative duty argument was a recipe for plaintiff's lawyers, and the industry now knew it. Federal lawmakers wanted to incentivize the nascent ISPs to screen content because federal agencies could not possibly do it all themselves. *Stratton Oakmont*'s ruling implied that screening content was the one thing ISPs should *not* do. It had things exactly backwards, and Congress needed to fix it.

It turns out that state legislatures across the country have faced a nearly analogous policy problem with negligence law. Negligence law's misfeasance/nonfeasance distinction, left on its own, tells highway motorists that they will face no liability for failure to offer roadside assistance to someone in a medical emergency situation if that person is a stranger; we say there is no duty to rescue. However, if one undertakes to help, and then things go awry, the volunteer is said to have a duty of care and to face liability for the ensuing injuries. Every state legislature has decided that such a combination of rules would provide a pathological set of incentives for doctors, nurses, and others to stop and be Good Samaritans, and has therefore passed a statute for them called a "Good Samaritan Statute." These statutes say that undertaking to rescue someone in an emergency does not create liability for injuries flowing from the negligent conduct of the rescuer, so long as the rescuer is acting in good faith. It thereby eliminates the disincentive presented by the unadorned common law principles, and clears the way for Good Samaritan volunteering.

It is no coincidence that §230 is called Protection for "Good Samaritan" blocking and screening of offensive material. It was enacted to reverse the pathological set of incentives that the internet industry pointed out in *Stratton Oakmont*. The language of §230(c)(2) is as clear as the Good Samaritan label itself: "No provider or user of an interactive service shall be held liable on account of action voluntarily taken in good faith to restrict access to material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent . . . ."

The Good Samaritan connection here are unmistakable, so one wonders why courts have not paid more attention to it or expressly seen this connection. Part of the answer is that §230(c)(2) is not the part of §230 that has caused so much interpretive confusion. What has troubled courts and advocates is §230(c)(1), which does not discuss voluntary undertakings at all. So how does this background help us?

The answer is that §230(c)(1) makes sense only when one sees it in light of §230(c)(2). These provisions need to be understood as a package, and against the background of affirmative duty law in negligence. State Good Samaritan statutes basically say that volunteering to help does not alter the baseline no-duty-to-rescue-strangers rule. Section 230(c)(2) basically states that good faith volunteering to protect and filter against offensive content posted by third parties will not generate a full-fledged duty to protect others against defamatory postings. The irony is that it was simply not clear whether there was any baseline rule of no duty to protect people against the offensive content put on the internet by others. This was an open question under state law; as indicated above, scholars were beginning to discuss it, and two courts had weighed in on it a bit. Congress took the opportunity in §230(c)(1) to lay down a baseline rule that there is no duty to protect people against such language (and entrenched it further with the preemption provisions of §230(e)(3)). To say that providers and users *shall not be treated as publishers or speakers* of the posts or content of others is simply to say that the publication element of defamation shall not be deemed satisfied by them simply by virtue of their being the internet service provider (like Prodigy or CompuServe) who had the power to remove it and through whose medium it was posted.

Four conclusions and a more general observation follow from this analysis. One conclusion is that *Zeran v. America Online, Inc.*[4] was correctly decided. Zeran's lawyer cleverly argued in that case that Congress meant to preclude treating ISPs as newspaper publishers, but left open the possibility of treating them as distributors. In this case, argued plaintiff's counsel, AOL would have incurred affirmative duties to remove defamatory postings if they had been provided with prior notice, as AOL had. But the text of §230(c)(1), read in light of its combination with §230(c)(2) and the name and history of the statute, indicate that the statute creates a baseline under which courts may not treat an ISP as satisfying the publication element by virtue of its failure to screen or remove postings by others, with notice or otherwise.

[4] 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

A second is that the Ninth Circuit made a serious error in its widely followed 2003 decision in *Batzel v. Smith*[5] when it stated that the active/passive distinction is irrelevant to §230, and ruled that reposting what someone else wrote is immunized by §230. It is not. The principal point of §230 was to firm up the active/passive distinction and say that if you are not the one who placed it there, you normally cannot be said to satisfy the publication element. It says nothing about what should happen if the defendant did place a defamatory statement on the internet by reposting it. In failing to see this, the Ninth Circuit effectively interpreted CDA as abrogating the republication rule for the internet. More generally, nothing in §230 prohibits liability for content *created* by third parties; it is about who placed it on the internet, not who created it. "He said it first" does not work in defamation law as a defense, but after *Batzel*, it often works for the internet. That was a mistake and it needs to be undone.

Third, the text and history of §230(c)(1) indicate a focus on the publication element of defamation claims. It is far less clear what – if anything -- it should be interpreted to say about the range of legal wrongs to which it has been applied. A variety of considerations (including, but not just limited to, the breadth of the legislative findings and the need to see through artful pleading) arguably weigh in favor of a somewhat broader reading, and I think at this stage it is sensible for figures on all side to recognize that. But it is a mistake to see the text itself as eliminating liability for a hugely broad range of legal wrongs.

Fourth, the text of §230(c)(2), like the classic state Good Samaritan statutes upon which it was modeled, envisions only a *qualified* immunity for those who engage in screening. Its protection expressly precludes imposing liability for "action voluntarily taken in *good faith*" (emphasis added). In answering the calls of a talented defense bar for an absolute immunity, courts have largely overlooked this crucial qualification at the core of the text itself.

Finally, my own view is that Congress was well motivated and sensible when it passed §230 in response to *Stratton Oakmont* case a quarter century ago, just as states have been sensible to enact Good Samaritan laws. In both cases, legislatures have been alert to perverse incentives stemming from the law's awkward efforts to distinguish causing harm from failing to prevent it. But courts have never read such statutes as obstacles to the reasonable allocation of responsibility for harm; their very point is to allow our legal system to accommodate common

[5] 333 F.3d 1018 (9th Cir.), *reh'g denied*, 351 F.3d 904 (9th Cir. 2003), *cert. denied*, 541 U.S. 1085 (2004).

sense judgments about the duties owed to others to protect them from harm. To the extent that judicial interpretation of §230 has taken a different turn, Congress should steer it back on course.