THE C. BOYDEN GRAY
Center *for the* Study
of the Administrative State
ANTONIN SCALIA LAW SCHOOL • GEORGE MASON UNIVERSITY

Defending the Indispensable: Allegations of Anti-Conservative Bias, Deep Fakes, and Extremist Content Don't Justify Section 230 Reform

Matthew Feeney

CSAS Working Paper 20-11

Should Internet Platform Companies Be Regulated – And If So, How?

GEORGE MASON UNIVERSITY | ANTONIN SCALIA LAW SCHOOL

Defending the Indispensable:

Allegations of Anti-Conservative Bias, Deep Fakes, and Extremist Content Don't Justify Section 230 Reform

Matthew Feeney
Director of the Cato Institute's Project on Emerging Technologies

Introduction

When President Clinton signed the Telecommunications Act of 1996 it's unlikely he knew that he was signing a bill that included what has come to be called the "Magna Carta of the Internet."[1] After all, the law was hundreds of pages long, including seven titles dealing with broadcast services, local exchange carriers, and cable. The Internet as we know it didn't exist in 1996. Facebook founder Mark Zuckerberg was 11 years old, and two Stanford University PhD students, Larry Page and Sergey Brin, had only just begun a project that would come to be known at Google. Some didn't even think that the Internet would last, with Ethernet co-inventor Robert Metcalfe predicting in 1995 that "the internet will soon go supernova and in 1996 will catastrophically collapse."[2]

The U.S. Supreme Court would rule much of Title V of the law, otherwise known as the Communications Decency Act, to be unconstitutional in 1997.[3] However, a small provision of the law – Section 230 – survived. This piece of legislation" stated that interactive computer services could not be considered publishers of most third-party content or be held liable for moderating content.

Despite providing the legal framework necessary for the development of some of America's most famous and innovative companies, Section 230 is currently under bipartisan attack. Lawmakers and activists from the left and the right have a supported amending Section 230 in order to tackle perceived anti-conservative bias, Deep Fakes, and extremist content.

None of these concerns warrant a Section 230 amendment. This paper will analyze the empirical basis for the claims and explain why addressing them via Section 230 reform would result in a less competitive and less liberal market for venues of online speech.

Section 230

Section 230 of the Communications Decency Act solved a dilemma that emerged in the wake of two court cases from the 1990s. In the 1990s websites that hosted comment sections, fora, bulletin boards, and discussion groups were becoming increasingly popular. CompuServe, America Online, Prodigy Services, and other online service providers hosted venues for such commentary. It was only a matter of time before courts would have to consider how to handle questions about who should be held liable for content at such venues. The judicial response to

[1] Alan Rozenshtein, "Silicon Valley's Regulatory Exceptionalism Comes to an End," Lawfare, March 23, 2018. https://www.lawfareblog.com/silicon-valleys-regulatory-exceptionalism-comes-end

[2] Luciano Floridi, "Should we be afraid of AI? Machines seem to be getting smarter and smarter and much better at human jobs, yet true AI is utterly implausible. Why?" Aeon, May 9, 2016. https://aeon.co/essays/true-ai-is-both-logically-possible-and-utterly-implausible

[3] *Reno v. American Civil Liberties Union* (1997) 521 U.S. 844

these inevitable questions prompted Reps. Ron Wyden (D-OR) and Christopher Cox (R-CA) to write what became Section 230.

At first glance it might seem odd that members of Congress would feel the need to address questions of Internet content liability. After all, there was and still is a long-standing, well-developed body of law governing liability questions associated with book distributors and newspaper publishers. Why was new legislation required?

When Judge Peter Leisure of the United States District Court for the Southern District of New York considered a libel claim associated with an online service provider he took the traditional approach. At question in the case *Cubby, Inc. v. CompuServe Inc.* (1991) was whether Cubby Inc. could sue CompuServe for defamatory content that appeared on a newsletter available to subscribers of a CompuServe product.[4]

CompuServe developed the product CompuServe Information Service ("CIS"). CIS subscribers could access dozens of bulletin boards and databases, including the Journalism Forum. The Journalism Forum included a daily newsletter named Rumorville USA, published by Don Fitzpatrick Associates of San Francisco (DFA).

Cameron Communications (CCI) contracted with CIS, allowing it to "manage, review, create, delete, edit and otherwise control the contents" on the Journalism Forum. CCI also had a contract with DFA, which stipulated that DFA "accepts total responsibility for the contents" of Rumorville.[5]

Cubby, Inc. and Robert Blanchard developed the Rumorville competitor Skuttlebut. They claimed that Rumorville published defamatory content related to Scuttlebutt and brought a libel claim against CompuServe and DFA.

In his ruling in favor of CompuServe, Judge Leisure held that CompuServe had no more editorial control over Rumorville's content than a book store or public library.[6] He went on, writing that holding CompuServe to a liability standard higher than those appropriate for book stores would "impose an undue burden on the free flow of information."[7]

[4] Cubby, Inc. v. Compuserve, Inc. 776 F. Supp. 135 (S.D.N.Y. 1991).
[5] Ibid.
[6] "CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so. […] A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information."
Ibid.
[7] Ibid.

Although a win for the burgeoning Internet industry, the *Cubby* case only addressed defamation liability claims.[8] It did not exclude the possibility of a "Heckler's Veto," with illegitimate allegations of defamation being sufficient for the removal of content.[9]

A few years later, the New York Supreme Court considered a defamation case, *Stratton Oakmont, Inc. v. Prodigy Services Co.* (1995).[10] Prodigy Services, an online service provider, hosted a bulletin board run by Charles Epstein named Money Talk. An unidentified user posted content Stratton Oakmont considered defamatory. Stratton Oakmont sued for $100 million.[11] The Court considered the *Cubby, Inc. v. CompuServe Inc.* holding, but found that the *Stratton Oakmont* case was different in two important ways: 1) Prodigy presented itself as the controller of message board content, and 2) Prodigy used software to automatically screen and sometimes remove content deemed to violate its guidelines.[12] The Court stated that service providers such as CompuServe and Prodig*y* should generally be considered in the same way as bookstores.[13] However, the *Stratton Oakmont, Inc. v. Prodigy Services Co.* holding went on to state that Prodigy's decision to use technology to filter and remove content mandated that it be considered a publisher.[14]

The *Stratton Oakmont* and *Cubby* rulings put online service providers into the "Moderator's Dilemma." Providers were presented with a choice: use *Cubby* for guidance and take a hands-off approach to third party content or turn to *Stratton Oakmont*'s example and engage in content moderation but risk being considered a publisher of third party content.

Rep. Chris Cox (R-CA), a CompuServe and Prodigy customer, read a newspaper article about the *Stratton Oakmont, Inc. v. Prodigy Services Co.* case and discussed it with his colleague Rep. Ron Wyden (D-OR).[15] Wyden could see that *Stratton Oakmont* risked hampering technological innovation by exposing Internet service providers to multi-million-dollar lawsuits if they engaged in content moderation. The lawmakers were also aware of legislative efforts to deal with online pornography that risked stifling free speech. Sen. James Exon (D-NB) had introduced legislation co-sponsored by Sens. Daniel Coats (R-IN), Robert Byrd (D-WV), and Howell Heflin (D-AL) that would've prohibited the use of telecommunication devices to make "indecent" images available to minors.[16] Both Wyden and Cox pondered legislation that could prevent *Stratton Oakmont* becoming the national standard for online service providers and head off the Exon legislation.

[8] Professor Eric Goldman, "Internet Law: Cases and Materials," Santa Clara University. July 2019 Version.
[9] Ibid.
[10] Stratton Oakmont, Inc. v. Prodigy Services Co. 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
[11] Goldman "Internet Law: Cases and Materials"
[12] Stratton Oakmont, Inc. v. Prodigy Services Co. 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
[13] Ibid.
[14] Ibid.
[15] Jeff Kosseff, "The Twenty-Six Words That Created the Internet," Cornell University Press, April 15, 2019.
[16] 141 Cong. Rec. 8386 (June 14, 1995)

At the time, members of Congress were considering a revamp of the Communications Act of 1934. Cox and Wyden's solution to the Moderator's Dilemma and alternative to the Exon proposal eventually made its way into this overhaul effort as Section 230 of the Communications Decency Act.

Section 230 solved the Moderator's Dilemma by providing "interactive computer services" such as CompuServe and Prodigy with two key protections, which Sen. Wyden sometimes refers to as 230's sword and shield provisions.[17] The shield is Section 230(c)(1), which reads:

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.[18]

This provision is a repudiation of *Stratton Oakmont*. It states that online providers such as Prodigy and CompuServe (interactive computer services) shall not be treated as the publisher of content posted by a member of forums, bulletin boards, or comments sections (information content providers). Today, this provision ensures that Facebook, Yelp, Google, and Twitter cannot be considered the publisher of content users post. It also protects companies that are treated as publishers in other contexts. For example, *The New York Times* is a publisher of articles and opinion pieces. If someone believes they have been defamed in a *New York Times* opinion article they can sue not only the author of the article but also The New York Times Company, which publishes *The New York Times*. However, if someone posted defamatory content in the comments section of a *New York Times* article it could not be held liable. This is because the *New York Times'* comments section is an "interactive computer service" as defined by Section 230.[19]

Section 230's sword provision is 230(c)(2)(A):

No provider or user of an interactive computer service shall be held liable on account of […] any action voluntarily taken in good faith to restrict access to or availability of material that the

[17] 47 U.S.C §230(f)(2): The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

Emily Stewart, "Ron Wyden wrote the law that built the internet. He still stands by it — and everything it's brought with it.," *Vox*, May 16, 2019. https://www.vox.com/recode/2019/5/16/18626779/ron-wyden-section-230-facebook-regulations-neutrality

Colin Lecher, "Sen. Ron Wyden on Breaking Up Facebook, Net Neutrality, and the Law that Built the Internet," *The Verge*, July 24, 2018. https://www.theverge.com/2018/7/24/17606974/oregon-senator-ron-wyden-interview-internet-section-230-net-neutrality

[18] 47 U.S.C §230(c)(1)

[19] 47 U.S.C §230(f)(2)

provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected[20]

This provision allows companies to codify their own content moderation standards and remove content without fear of litigation. It makes clear that companies are free to remove content they consider objectionable, even if that content is protected by the First Amendment.[21] Pornography and footage of beheadings are legal and protected under the Constitution, but Section 230(c)(2)(A) allows companies such as Twitter and Facebook to restrict such content from their services.

While Section 230 provides interactive computer services broad liability protections these protections are not absolute. Section 230 includes exceptions for prosecutions of federal crimes, intellectual property claims, claims under the Electronic Communications Privacy Act of 1986 or state law equivalents, and content associated with sex trafficking.[22]

Hard as it might be to believe amid current furious debates about online content moderation, Section 230 passed with relatively little debate or input from industry.[23] Only nine members took part in House floor debate on Section 230, and the House voted 420-4 to add it to the telecommunications reform bill, which did not include Sen. Exon's proposal.[24]

Why Not Adopt a European Model?

The American government's jurisdiction over the Internet is restricted to the United States. But social media crosses national boundaries. Social media firms thus have to comply with a vast array of different liability laws and regulations. That residents of every continent use Facebook and Twitter is perhaps evidence that Section 230 is not a necessary condition for online social media. However, a review of Internet third party liability regimes in some of the largest markets outside the U.S. reveals that they are inferior to Section 230 and serve as a poor template for Section 230 reforms.

One of the largest non-U.S. social media markets is the European Union (EU). In 2000, the European Parliament passed the EU Directive on Electronic Commerce 2000/31/EC, imposing a duty of care on intermediary service providers (ISPs) such as Facebook and Twitter.[25] Article 12(1) of the directive states that ISPs are not liable for third party content. This immunity is

[20] 47 U.S.C §230(c)(2)(A)
[21] U.S. Const. Amend I
[22] 47 U.S.C §230(e)
[23] Jeff Kosseff, "The Twenty-Six Words That Created the Internet," Cornell University Press, April 15, 2019.
[24] Ibid.
[25] Directive 2000/31/EC, of the European Parliament and the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (178) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN.

conditioned on three requirements: the ISP "(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."[26]

Article 12(3) allows for the EU's member states to require IPSs to remove or block content consistent with state laws.[27] A number of members have done so.

There are similarities between America's Section 230 and the Internet governance regimes in Europe. Lawmakers on both sides of the Atlantic have embraced some kind of third party liability protection for internet service providers. However, Section 230's immunity shield is stronger than those seen in Europe, and the European model is associated with higher costs for Internet users.

For example, under French law ISPs risk liability if they don't remove objectionable content after notice. French law also requires ISPs make filtering software available to users.[28] In the United Kingdom, ISPs can use an "innocent dissemination" defense in liability suits if it was unaware of the offending content, but the defense is conditioned on taking reasonable care in publishing the content.[29] In *Godfrey v. Demon Internet*, an English court found that Demon Internet could not use the "innocent dissemination" defense after taking two weeks to remove content a physics professor alleged to be defamatory.[30] Under Section 5(2) of the German Teleservices Act ISPs are potentially liable for third party content if the ISP is aware of the content and blocking the content is feasible.[31]

The European regime is associated with legal uncertainty and financial costs American ISPs are fortunate enough to avoid.[32] As Suffolk University Law School professor Michael L. Rustad and Northeastern University's Professor Thomas H. Koenig have noted, "[European] ISPs, for example, need to bear the expenditures of investigating complaints, tracking down wrongdoers, and making nuanced takedown and put-back decisions under European law. These higher costs are passed on to computer users and other consumers in Internet access charges."[33]

It's true that the Internet is global, but its governance is not. Countries across the world take different approaches to liability for third party content. A reform to Section 230 that embraces the duty of care seen in Europe would help well-resourced market incumbents - which would be

[26] Ibid.
[27] Ibid.
[28] Law No. 2000-719 of Aug. 1, 2000, J.O., Aug. 2, 2000, pp. 11903, 11922; JCP 2000 No. 39, p. 1739, http://www.juriscom.net/txt/loisfr/l20000801.htm
[29] Schruers, Matthew, The History and Economics of ISP Liability for Third Party Content. Virginia Law Review, Volume 88, No. 1, pp 205-64, March 2002, pp. 227.
[30] Ibid.
[31] Ibid. at 228.
[32] Michael L. Rustad & Thomas H. Koenig, Rebooting Cybertort Law, 80 Wash. L. Rev. 335 (2005). Available at: https://digitalcommons.law.uw.edu/wlr/vol80/iss2/3, pp. 394.
[33] Ibid.

best positioned to incur the associated costs - and prompt firms to err on the side of caution, resulting in less legal content appearing online.

Bias

Section 230 is a prominent feature of modern political debate in large part because of concerns associated with alleged anti-conservative bias in Silicon Valley. Specifically, these concerns are centered around the largest "interactive computers services" including Facebook, Twitter, and YouTube, which is owned by Alphabet subsidiary Google. These concerns have motivated some lawmakers to call for Section 230 amendments that would significantly alter how the Internet as we know it functions. Such a dramatic change in legislation and modern culture should be grounded in empirical facts. Yet an analysis of the most prominent allegations of anti-conservative bias influencing "Big Tech" social media companies' content moderation policies reveals that they are not based on persuasive evidence. Even if they were, evidence of anti-conservative bias it wouldn't justify amending Section 230.

Before examining contemporary accusations of anti-conservative bias, it is worth putting them in a historical context. Accusations of "Big Tech" bias are not unique to our present political climate. While today we are used to such accusations coming from self-identified conservatives, similar complaints have been leveled by left-wing and progressive groups.

In 2017, the Chairperson of the International Editorial Board of the World Socialist Web Site (WSWS) wrote a letter to executives at Alphabet and Google, which is an Alphabet subsidiary.[34] The letter claimed:

> "Google, and by implication, its parent company Alphabet, Inc., are now engaged in political censorship of the Internet.[…] Google is manipulating its Internet searches to restrict public awareness of and access to socialist, anti-war and left-wing websites. […] Whatever the technical changes Google has made to the search algorithm, the anti-left bias of the results is undeniable. The most striking outcome of Google's censorship procedures is that users whose search queries indicate an interest in socialism, Marxism or Trotskyism are no longer directed to the World Socialist Web Site. Google is "disappearing" the WSWS from the results of search requests."[35]

The same year WSWS official sent his letter, ProPublica accused Facebook of an inconsistent content moderation policy that favored white politicians over racial justice activists.[36] Activists

[34] David North , "An open letter to Google: Stop the censorship of the Internet! Stop the political blacklisting of the World Socialist Web Site!" World Socialist Web Site, August 25, 2017. https://www.wsws.org/en/articles/2017/08/25/pers-a25.html
[35] Ibid.
[36] Julia Angwin and Hannes Grassegger, "Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children," ProPublica, June 28, 2017. https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms

have also criticized Facebook for complying with requests from law enforcement to remove content associated with police brutality.[37] A 2016 petition on Change.org demanding that Facebook stop "censoring and restricting the voices of people of color and individuals from the trans community" received almost 16,000 signatures.[38] Conservatives who believe that their opinions are being systematically stifled by "Big Tech" should consider that left-wing groups and activists have lodged similar complaints.

Accusations of anti-conservative bias are varied, as are the proposed remedies. Critics see three kinds of bias against conservatives: demonetization, algorithmic suppression, and politically motivated removal. Conservative activists and lawmakers have proposed judicial and legislative responses to these claims, including amendments to Section 230. Many of these proposals are motivated by concerns about YouTube.

YouTube is a video-sharing website. Visitors can use YouTube's search function to find videos on a vast array of topics. Content creators can upload videos to YouTube and moderate an optional comments section for each video. Those who visit YouTube to view videos do not need a YouTube account, although some content is restricted to adults. YouTube visitors can generate a free account and voluntarily put themselves into "Restricted Mode," which blocks content that features violence, expletives, discussions of sex, drugs, and alcohol, as well as content that YouTube considers demeaning or incendiary.[39] This "Restricted Mode" is at the heart of one of the most prominent conservative allegations of Silicon Valley bias popularized by Dennis Prager.

Dennis Prager is a conservative commentator and the founder of Prager University (often abbreviated to PragerU). Despite its name, PragerU is not an accredited academic institution. Rather, it's a website that features videos and podcasts that seek to educate visitors on a variety of issues from a conservative perspective. PragerU has a YouTube channel where users can watch PragerU's videos. Some of the most popular of these videos feature a guest speaker discussing one issue in an animated video that lasts for around five minutes. At the time of writing PragerU has 2.44 million subscribers.

PragerU claimed in a 2017 complaint filed with the United States District Court for the Northern District of California that YouTube was censoring its videos.[40] Specifically, PragerU claimed that YouTube engaged in "demonetization" and put some of its videos in "Restricted Mode" in

[37] Coalition letter to Mark Zuckerberg, August 22, 2016..
https://s3.amazonaws.com/s3.sumofus.org/images/FinalLetter-MarkZuckerberg_1.pdf
[38] Change.org petition "Facebook: Stop Censoring and Banning the Accounts of Black and Trans Activists."
https://www.change.org/p/facebook-stop-censoring-and-banning-the-accounts-of-black-and-trans-activists
[39] Google's explanation of YouTube's restricted mode:
https://support.google.com/YouTube/answer/7354993?hl=en
[40] Complaint for Damages, Injunctive Relief, and Declaratory Judgment & Jury Trial Demand, Prager Univ. v. Google LLC, No. 17-CV-06064-LHK (N.D. Cal. Oct. 23, 2017).
http://www.bgrfirm.com/wp-content/uploads/2017/10/PRAGER_U-_v_GOOGLE-YOUTUBE_complaint_10-23-2017_FILED.pdf

order to limit access to PragerU's conservative content.[41] If true, such activities would be legal under Section 230(c)(2)(A).[42]

Unfortunately for Prager, PragerU's claims don't withstand scrutiny. It is true that a portion of PragerU's YouTube videos are blocked to users who opt into Restricted Mode. However, it's far from obvious that this is blocking is politically motivated. NetChoice analyzed the number of PragerU videos placed in Restricted Mode and found that 12 percent of its videos were in that category.[43] That compares to 71 percent of Young Turks videos and 54 percent of Daily Show videos.[44] In a declaration before the United States District Court for the Northern District of California Alice Wu, a senior YouTube trust and safety manager, showed that the History Channel, BuzzFeed, Vox.com, Democracy Now, and Al Jazeera all have a higher portion of their YouTube videos put in Restricted Mode than PragerU's.[45] That progressive and non-partisan channels have a higher portion of their videos in Restricted Mode than PragerU flies in the face (JS: refutes? falsifies?) of PragerU's claim that YouTube puts some of its videos in Restricted Mode because of an anti-conservative bias.

PragerU's "demonetization" claims are also unfounded. It's true that YouTube does limit advertising from certain videos including not only violent and hateful content but also content associated with firearm purchases and recreational drugs.[46] PragerU is hardly alone when it comes to having some content demonetized, but such demonetization is hardly evidence of a concerted anti-conservative campaign. In the wake of YouTube revising its policies related to advertising a wide range of content creators complained about a drop in advertising revenue, including progressive commentator David Parkman.[47]

[41] Ibid.
"As applied to PragerU, Google/YouTube use their restricted mode filtering not to protect younger or sensitive viewers from "inappropriate" video content, but as a political gag mechanism to silence PragerU. And Google/YouTube do this not because they have identified video content that violates their guidelines or is otherwise inappropriate for younger viewers, but because PragerU is a conservative nonprofit organization that is associated with and espouses the views of leading conservative speakers and scholars. This is speech discrimination plain and simple: censorship based entirely on the perceived identity and political viewpoint of the speaker not on the content of the speech."
[42] 47 U.S.C §230(c)(2)(A)
[43] Steve DelBianco, "Re: Hearing to Examine Google and Censorship through Search Engines," letter to Senator Ted Cruz, July 16, 2019, HYPERLINK "https://netchoice.org/wp-content/uploads/NetChoice-comment-for-Sen-Judiciary-hearing-16-Jul-2019.pdf."https://netchoice.org/wp-content/uploads/NetChoice-comment-for-Sen-Judiciary-hearing-16-Jul-2019.pdf.
[44] Ibid.
[45] Declaration of Alice Wu in Support of Defendants' Opposition to Motion for Preliminary Injunction, Prager Univ. v. Google LLC, No. 17-CV-06064-LHK (N.D. Cal. Feb. 9, 2018).
https://www.documentcloud.org/documents/4405479-2018-02-09-38-Declaration-of-Alice-Wu-ISO.html
[46] Google's advertising guidelines.
https://support.google.com/YouTube/answer/6162278?hl=en&ref_topic=9153642
[47] Geoff Weiss, "Here's How The YouTube 'Adpocalypse' Is Affecting Top Creators," tubefilter, May 4, 2017.
https://www.tubefilter.com/2017/05/04/how-YouTube-adpocalypse-affected-top-creators/

Accusations of political censorship and demonetization are not the only complaints leveled against Google and its subsidiaries. Some conservative organizations have claimed that Google employees deliberately interfere with Google's search function in order to limit access to conservative content. Among the most notable of these organizations is the conservative activist group Project Veritas, which in August 2019 released documents leaked by a Google insider.[48] The documents, many of which include photos of emails from Google employees, do not reveal an attempt to reduce access to conservative content.[49] In fact, the supposed revelation discussed far less about algorithmic bias and how Google's search function works than Google itself voluntarily discloses.[50] [51]

Another accusation leveled at Google is that the company's search function is biased towards left-of-center political candidates. Perhaps the most cited piece of research in support of this claim is by Robert Epstein of the American Institute for Behavioral Research and Technology. Epstein claims that in the months leading up to the 2016 presidential election Google's search results were biased in favor of Democratic Party nominee Hillary Clinton.[52] However, the study that supposedly supports the claim includes the search queries of an unrepresentative sample of only 95 people from 24 states, used crowdsourcing to rank bias, and rejected data received from Gmail addresses.[53] In addition, the study did not force respondents to use identical devices, a serious flaw given that search results can vary depending on the specific device used. Epstein went so far as to wonder whether Google was deliberately seeking to interfere with his research.[54] Despite the study's poor methodology, Sen. Cruz (R-TX) invited Epstein to testify before the United States Senate Judiciary Subcommittee on the Constitution.[55]

The Economist, citing Epstein's research as among the work associated with alleged bias, conducted an experiment on Google search results to test for anti-conservative discrimination.

[48] Landing page for Project Veritas' "Google Document Dump." https://www.projectveritas.com/google-document-dump/

[49] For a more in-depth examination of Project Veritas' claims see:
Matthew Feeney, "Misleading Project Veritas Accusations of Google "Bias" Could Prompt Bad Law," Cato Institute's Cato At Liberty blog, July 15, 2019.
https://www.cato.org/blog/misleading-veritas-accusation-google-bias-could-result-bad-law

[50] Ibid.

[51] Sean Moran, "Watch: Ted Cruz Grills Google on its Political Bias," Breitbart, June 25, 2019. https://www.breitbart.com/tech/2019/06/25/watch-ted-cruz-grills-google-on-its-political-bias/

[52] Robert Epstein and Ronald Robertson, "A Method for Detecting Bias in Search Rankings, with Evidence of Systematic Bias Related to the 2016 Presidential Election," American Institute for Behavioral Research and Technology, June 1, 2017. https://aibrt.org/downloads/EPSTEIN_&_ROBERTSON_2017-A_Method_for_Detecting_Bias_in_Search_Rankings-AIBRT_WP-17-02_6-1-17.pdf

[53] Ibid.

[54] Ibid:
"Perhaps Google identified our confidants through its gmail system and targeted them to receive unbiased results; we have no way to confirm this at present, but it is a plausible explanation for the pattern of results we found."

[55] Testimony by Robert Epstein Before the United States Senate Judiciary Subcommittee on the Constitution Tuesday, June 16, 2019. https://www.judiciary.senate.gov/imo/media/doc/Epstein%20Testimony.pdf

The program *Economist* researchers used revealed that Google did not favor left-wing news outlets.[56]

Accusations of anti-conservative bias have prompted a number of legislative and judicial proposals. In their complaint against YouTube, PragerU argued that YouTube is conducting a public function by regulating speech in a public forum and behaves like a state actor.[57] As a state actor, Prager University argued, YouTube is not permitted to engage in viewpoint discrimination.[58] To buttress this claim, Prager University cited *Marsh v. Alabama* (1946), which held that the free speech protections under the First and Fourteenth Amendments are applicable in a town owned by a private entity.[59] Judge Koh, who dismissed Prager University's motion for preliminary injunction at the United States District Court for the Northern District of California, correctly noted that the comparison between YouTube and the company town at issue in *Marsh* was inappropriate: "Marsh's holding stands for the proposition that a private entity that owns all the property and controls all the municipal functions of an entire town is a state actor that must run the town in compliance with the Constitution. Thus, contrary to Plaintiff's position, Marsh does not compel the conclusion that Defendants are state actors that must comport with the requirements of the First Amendment when regulating access to videos on YouTube."[60] This should hardly be a controversial holding. Local governments have no traditional role as video publishers, and YouTube does not collect taxes, pave roads, or enforce laws.

First Amendment cases since *Marsh* are of little help to Dennis Prager and his allies. For example, in *Lloyd Corp. v. Tanner* (1972) the Supreme Court held that a shopping mall did not constitute a public forum.[61] Prager appealed the case to the United States Court of Appeals for the Ninth Circuit. In a unanimous opinion written by Judge McKeown the court agreed with

[56] "Google rewards reputable reporting, not left-wing politics," *The Economist*, June 8, 2019. https://www.economist.com/graphic-detail/2019/06/08/google-rewards-reputable-reporting-not-left-wing-politics

[57] Complaint for Damages, Injunctive Relief, and Declaratory Judgment & Jury Trial Demand, Prager Univ. v. Google LLC, No. 17-CV-06064-LHK (N.D. Cal. Oct. 23, 2017).
[58] Ibid.
[59] *Marsh v. Alabama* (1946) 326 U.S. 501
[60] *Prager Univ. v. Google LLC* United States District Court for the Northern District of California, San Jose Division March 26, 2018, Decided; March 26, 2018, Filed Case No. 17-CV-06064-LHK https://www.courtlistener.com/recap/gov.uscourts.cand.318491/gov.uscourts.cand.318491.54.0.pdf

See also (from same citation):

"Defendants do not appear to be at all like, for example, a private corporation that governs and operates all municipal functions for an entire town […] or one that has been given control over a previously public sidewalk or park […]or one that has effectively been delegated the task of holding and administering public elections[…] Instead, Defendants are private entities who created their own video-sharing social media website and make decisions about whether and how to regulate content that has been uploaded on that website."
[61] *Lloyd Corp. v. Tanner* (1972) 407 U.S. 551

Judge Koh, holding that as a private company, YouTube is not subject to judicial scrutiny under the First Amendment.[62]

Public forum arguments as a means to address supposed anti-conservative bias in "Big Tech" are unlikely to persuade the federal judiciary. However, litigation is only one of the arrows in the conservative anti-Section 230 quiver. Legislation is another option, and conservative lawmakers in both houses of Congress have introduced legislation that seeks to tackle supposed political bias.

In June 2019 Sen. Joshua Hawley (R-MO) introduced the Ending Support for Internet Censorship Act.[63] The legislation targets "interactive computer services" as defined by Section 230 with either more than 30,000,000 active monthly users in the United States; more than 300,000,000 active monthly users worldwide; or more than $500,000,000 in global annual revenue. Under Hawley's bill, such services would only enjoy Section 230 liability protections if they received a two-year certification from the Federal Trade Commission (FTC). Such a certification would be dependent on the interactive computer service (such as Google or Facebook) providing the FTC with "clear and convincing evidence that the provider does not […] moderate information provided by other information content providers in a politically biased manner."[64]Neutrality would be determined by a majority of the FTC plus one, not covered firms. Such a proposal could raise issues associated with bans on material support for foreign terrorist organizations.[65] Under Sen. Hawley's bill, any large Internet company that uses content moderation "to negatively affect a political party, political candidate, or political viewpoint" risks losing its FTC certification.

The bill does include a "business necessity" exception, which allows for interactive computer services to restrict access to political content if such restrictions are "necessary for business," the censored content is not protected by the First Amendment, "there is no available alternative that has a less disproportionate effect," and the content moderation is not intended to discriminate against "political affiliation, political party, or political viewpoint."[66] But this exception is potentially one that swallows the rule. Any business could claim that removing Ku Klux Klan members from its platform is necessary for business. Even if the "business necessity" exception only prohibited covered firms from excluding recognized political parties there is content that might be bad for business. A social media site that caters to racial minorities might view it as a

[62] Prager Univ. v. Google LLC, No. 18-15712 (9th Cir. Feb. 26, 2020), https://cdn.ca9.uscourts.gov/datastore/opinions/2020/02/26/18-15712.pdf.

[63] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2019). https://www.hawley.senate.gov/sites/default/files/2019-06/Ending-Support-Internet-Censorship-Act-Bill-Text.pdf
[64] Ibid.
[65] Kathleen Ann Ruance, "The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes," Congressional Research Service, September 8, 2016. https://fas.org/sgp/crs/terror/R44626.pdf
[66] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2019). https://www.hawley.senate.gov/sites/default/files/2019-06/Ending-Support-Internet-Censorship-Act-Bill-Text.pdf

business necessity to remove images of the Confederate flag, which sitting Rep. Steve King (R-IA) displayed on his desk.[67] But in order to satisfy Sen. Hawley's "business necessity" criteria a firm would also have to demonstrate that there is no alternative action that would result in a less disproportionate effect. What is considered an alternative action that satisfies the "business necessity" exception would have to be litigated. Such litigation could result in firms taking steps to hide all content outside the political mainstream.

Hawley's fellow Republican Rep. Paul Gosar (R-AR) has also introduced Section 230 reform legislation.[68] Like Sen. Hawley, Rep. Gosar was motivated to introduce the bill because of perceived anti-conservative bias.[69] Rep. Gosar's bill would gut the provisions of Section 230 that protect Internet companies from moderating content considered "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[70] Under Rep. Gosar's bill, companies such as Google and Facebook would only enjoy liability protection for activities related to takedowns of illegal and not necessarily offensive content.[71]This would do significant damage to many social media businesses, which rely on the ability to remove offensive comment in order to make their service attractive.

Rep. Gosar's bill reveals a misunderstanding of how Section 230 litigation tends to develop. While it targets Section 230(c)(2)(A), which protects interactive computer services from being held liable for content they choose to remove, interactive computer services rarely rely on its protections.[72]

Legislative proposals such as Hawley's and Gosar's rest on dubious evidence. Claims that some of the best-known "Big Tech" companies are waging a campaign to limit or eliminate access to conservative content rest on shaky empirical foundations. Yet even if there was proof that these companies were conducting such a campaign it wouldn't justify the legislative proposals suggested by Hawley and Gosar. "Big Tech" companies such as Google, Facebook, YouTube,

[67] Brianne Pfannenstiel, "Steve King provokes criticism for displaying Confederate flag," *Des Moines Register*, July 11, 2016. https://www.desmoinesregister.com/story/news/politics/2016/07/11/steve-king-provokes-criticism-displaying-confederate-flag/86947746/

[68] Stop the Censorship Act, H.R. 4027, 116th Cong. (2019). https://www.congress.gov/bill/116th-congress/house-bill/4027/cosponsors?q=%7B%22search%22%3A%5B%22Stop+the+Censorship+Act%22%5D%7D&r=1&s=1

[69] Press release from Rep. Gosar's office:
Rory Burke, "Congressman Gosar Introduces Legislation to Stop Big Tech Censorship," July 25, 2019. https://gosar.house.gov/news/documentsingle.aspx?DocumentID=3854

[70] Ibid.

[71] Ibid.

[72] Eric Goldman, "Comments on Rep. Gosar's '"Stop the Censorship Act,"' Another '"Conservative"' Attack on Section 230," Technology & Marketing Law Blog, August 15, 2019. https://blog.ericgoldman.org/archives/2019/08/comments-on-rep-gosars-stop-the-censorship-act-another-conservative-attack-on-section-230.htm

and Twitter are private companies with no obligation to host content that they consider contrary to their values or priorities.

Deep Fakes

Calls for Section 230 reform are not reserved to one side of the political spectrum. In the wake of President Donald Trump's election and increased use of "Deep Fake" technology some Democrats have suggested amendments to Section 230. These proposals seek to secure the integrity of elections and protect dignity. While such content and assaults on democratic institutions are disturbing, they don't in and of themselves justify Section 230 reform.

"Deep Fake" is a term applied to content created with Artificial Intelligence techniques – specifically deep learning - to make fake video and audio content. One of the most popular Deep Fake applications is the production of videos that make it appear as if someone is saying or doing something they never said or did.

Not all altered videos are Deep Fakes. In May 2019 altered footage of House Speaker Nancy Pelosi (D-CA) speaking at a Center for American Progress event spread across popular social media platforms.[73] The footage had been edited to make it appear as though Speaker Pelosi was drunk, her speech appearing slurred and garbled.[74]In November 2018 then-White House Press Secretary Sarah Sanders shared a video on Twitter allegedly showing CNN reporter Jim Acosta being aggressive with a White House intern during an event with President Trump at the White House. The intern was trying to take the microphone Acosta was using away.[75] Although Acosta had resisted the intern's efforts, the footage Sanders shared had been altered to make it appear as if Acosta had been more aggressive than he actually had been.[76] The Pelosi and Acosta videos certainly serve a political purpose and are edited, but they are not Deep Fakes. Neither video relied on the deep learning techniques that are a necessary condition for Deep Fakes.

Fake audio also poses risks. Scammers have used AI techniques to facilitate fraud transfers.[77] In 2019 scammers used commercially available voice generation software to target the CEO of a UK-based energy firm. The software allowed the scammers to impersonate the voice of the German head of the firm's parent company, directing the CEO to send $243,000 to Hungarian

[73] Drew Harwell, "Faked Pelosi videos, slowed to make her appear drunk, spread across social media," *The Washington Post*, May 24, 2019. https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/
[74] Ibid.
[75] David Bauder and Calvin Woodward, "Expert: Acosta video distributed by White House was doctored," Associated Press, November 8, 2018. https://apnews.com/c575bd1cc3b1456cb3057ef670c7fe2a
[76] Ibid.
[77] Catherine Stupp, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *The Wall Street Journal*, August 30, 2019, Pro Cyber News, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrimecase-11567157402.

suppliers.[78] The scammers scattered the illegally obtained funds to accounts across the globe.[79] While not every attack of this kind will use Deep Fakes techniques, such techniques will make these kind of attacks easier to carry out.

Deep Fake content can have valuable satiric and educational applications but can also be used to harm someone's reputation by making it look as if they're engaged in pornography, racist behavior, or criminal conduct. There are also potential political implications. If someone or a group of people sought to interfere in an election, they could choose to use Deep Fake technology to make it appear as if their political opponent said something offensive or embarrassing.

The potential to make it look as if a political opponent behaved poorly is an often-cited concern associated with Deep Fakes. Yet there are other political applications, such as making it appear that you or a political ally have skills they in fact do not possess. For example, a politician in India recently used Deep Fake technology to make it appear as if he spoke languages he could not speak in an attempt to be able to communicate with more potential voters.[80]

Lawmakers at the federal and state level have taken steps in order to address concerns associated with Deep Fake content. Lawmakers in Virginia passed a law banning the use of deep fake technology in order to distribute nonconsensual pornography.[81] California and New York lawmakers have considered similar legislation.[82] Texas passed a bill targeting the use of deep fakes to create damaging portrayals of political candidates.[83] Congressional bills associated with Deep Fakes have mostly been focused on research, including proposals mandating the study of the impact Deep Fakes on national security and disinformation.[84]

While the risks associated with Deep Fakes are worth taking seriously it's not obvious that they necessarily warrant Section 230 reform. We may be exaggerating the risks and underappreciating potential responses.

[78] Ibid.
[79] Ibid.
[80] Kim Lyons, "An Indian politician used AI to translate his speech into other languages to reach more voters," *The Verge*, February 18, 2020. https://www.theverge.com/2020/2/18/21142782/india-politician-deepfakes-ai-elections
[81] Virginia, VA. Code Ann. §18.2-386.2
[82] Assemb. B. 1280, Leg., 2019-20 Reg. Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1280.; Assemb. B. 602, Leg., 2019-20 Reg. Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB602.; Assemb. B. No. A08155-B, 2018 Leg., 241st Sess. (N.Y. 2018) (as amended June 5, 2018), https://nyassembly.gov/leg/?default_fld=&bn=A08155&term=2017&Summary=Y&Actions=Y&Text=Y&Committee%2526nbspVotes=Y&Floor%2526nbspVotes=Y.
[83] S.B. 751, 86th Leg., Reg. Sess. (Tx. 2019), https://www.legis.state.tx.us/tlodocs/86R/billtext/html/SB00751F.HTM.
[84] Matthew F. Ferraro, "Deepfake Legislation: A Nationwide Survey – State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media," WilmerHale, September 25, 2019. https://www.wilmerhale.com/en/insights/client-alerts/20190925-deepfake-legislation-a-nationwide-survey

The concerns associated with Deep Fakes are, broadly speaking, about skepticism. One category of concerns focusses on how Deep Fakes might make society increasingly skeptical. The claim made by those with this concern is that in a world where Deep Fake content is ubiquitous, people will be more on guard, hesitant to believe content shared online. Another set of concerns revolves around the widespread use of Deep Fakes prompting more people to believe everything they see online. The ideal amount of skepticism in any society is not 100 percent or 0 percent, and there are worries that the proliferation of Deep Fake technology will drag society toward of one of these extremes.

But non-government responses to Deep Fake content will emerge. Indeed, although Deep Fake content is still in its relative infancy there have already been numerous examples of robust responses to the spread of realistic-looking fake content.[85]

In 2019 Facebook, the Partnership on AI, Microsoft, and a team of academics from across the U.S. announced the "Deepfake Detection Challenge" aimed at developing technologies that can identify Deep Fake content.[86] In September, 2019 Google submitted thousands of Deep Fake videos featuring consenting actors to researchers to FaceForensics benchmark, a Deep Fake detection effort run by the Technical University of Munich and the University Federico II of Naples.[87] These are only two examples of efforts from across the world to develop Deep Fake detection technology. In addition to contributing to developments in Deep Fake detection, Silicon Valley firms have taken steps to prohibit some categories of "manipulated media"[88]

Deep Fake detection technology is not perfect, and we should expect some damaging Deep Fake content to spread between popular sites. However, we should make sure to put Deep Fake content into a historical context. We have seen discussions about media manipulation in the past. As the R Street Institute's Jeffrey Westling mentioned in his paper on response to Deep Fakes, the emergence of Adobe Photoshop in 1990 prompted *Newsweek* to speculate about the technology allowing authoritarian regimes to deny evidence of atrocities.[89] Fraudsters and

[85] See Westling, Jeffrey, Are Deep Fakes a Shallow Concern? A Critical Analysis of the Likely Societal Reaction to Deep Fakes (July 24, 2019). Available at SSRN: https://ssrn.com/abstract=3426174 or http://dx.doi.org/10.2139/ssrn.3426174

[86] Mike Schroepfer, "Creating a data set and a challenge for deepfakes," Facebook Artificial Intelligence, September 5, 2019. https://ai.facebook.com/blog/deepfake-detection-challenge/

[87] Nick Dufour, "Contributing Data to Deepfake Detection Research," Google AI Blog, September 24, 2019. https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html

[88] Betsy Morris, "Facebook Bans Deepfakes but Permits Some Altered Content," *The Wall Street Journal*, January 7, 2020. https://www.wsj.com/articles/facebooks-deepfake-video-ban-permits-some-altered-content-11578384519.

Shirin Ghaffary, "Twitter is finally fighting back against deepfakes and other deceptive media," Vox, February 4, 2020. https://www.vox.com/recode/2020/2/4/21122653/twitter-policy-deepfakes-nancy-pelosi-biden-trump

[89] Westling, Jeffrey. Citing:
"When Photographs Lie," *Newsweek*, July 29, 1990. https://bit.ly/2Xt8dPK

criminals have used Photoshop in the years since 1990, but the benefits of the technology far outweigh the costs. Fears such as those outlined in *Newsweek* in 1990 have not been realized. When images of atrocities from the conflict in Syria emerge widespread skepticism of their veracity is rare, and few find authoritarian regime's claims of media manipulation persuasive. Few doubt that the plethora of images showing the ongoing persecution of the majority-Muslim Uyghur population in Western China is authentic.

Nonetheless, there are those who want to address the emergence and proliferation of Deep Fake technology with Section 230 reform. One of the Democratic lawmakers most prominent in Section 230 reform discussions is Sen. Mark Warner (D-VA). In 2018 news organizations shared copies of Sen. Warner's technology policy white paper.[90] The paper did not include texts of bills, thought it did outline potential policies to pursue. Among those policies was a reform to Section 230 aimed at addressing Deep Fake content. Sen. Warner's proposal would remove Section 230 liability protections for Deep Fake content that a judge has found to be a dignitary tort violation.

Danielle Citron of the Boston University School of Law and Benjamin Wittes of the Brookings Institution have also proposed Section 230 reforms that they argue could be used to limit the spread of degrading content.[91] Under Citron and Wittes' proposal Section 230(c)(1) would be amended as follows (Citron and Wittes additions in italics):

"No provider or user of an interactive computer service *that takes reasonable steps to prevent unlawful uses of its services* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider*."[92]

What constitutes "reasonable steps" would be up to courts. Recent Section 230 cases provide some examples of the issues courts would have to consider. In *Herrick v. Grindr* the plaintiff argued that Grindr, a dating app for the homosexual, bisexual, and transsexual community, was negligent in designing its app. Matthew Herrick had ended a relationship with a man he met on Grindr. After the relationship ended his former partner used Grindr to set up an account impersonating Herrick. The fake account told potential matches that Herrick was interested in rape fantasies. As a result, numerous men visited Herrick's home and place of work. Herrick alleged that Grindr's lack of identification verification was negligent: "Grindr could identify and ban the impersonating accounts through the language used in the direct messages. But it

[90] Hanna Kozlowska, "This paper shows just how unprepared the US is to deal with the problems technology has created," Quartz, August 1, 2018. https://qz.com/1345888/mark-warners-white-paper-outlines-how-unprepared-the-us-is-to-deal-with-problems-created-by-technology/

[91] Citron, Danielle Keats and Wittes, Benjamin, The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity (July 24, 2017). Fordham Law Review, Forthcoming; U of Maryland Legal Studies Research Paper No. 2017-22. Available at SSRN: https://ssrn.com/abstract=3007720

[92] Ibid.

intentionally, knowingly, and negligently refuses to. Upon information and belief, common software could be used to flag the specific phrases used repeatedly in the offending accounts."[93]

In 2019, the Wisconsin Supreme Court considered a case involving Armslist, an online marketplace for firearms and firearm equipment.[94] In 2012 court granted Zina Daniel Haughton a restraining order against her husband, Radcliffe Haughton.[95] One of the conditions of the restraining order was that Haughton not be in possession of firearms. Houghton nonetheless arranged a firearm purchase on Armslist.[96] The purchase took place at a McDonald's parking lot. The next day, Haughton shot and killed Zina Daniel Haughton, two others, and then himself. Four others were injured. Yasmeen Daniel, Zina's daughter, witnessed the shooting.[97] Daniel alleged that Armslist exploited the background check exception to private firearm sales and should have known that people banned from possessing firearms would turn to Armslist.[98] The Wisconsin Supreme Court dismissed the case, holding that Section 230 provides Armslist with a liability shield.[99]

If the Citron and Wittes Section 230 amendment were implemented courts would have to consider whether Grindr and Armslist failed to take "reasonable steps." Citron and Wittes claim that "[S]uch a determination would take into account differences among online entities. ISPs and social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two."[4] Citron and Wittes also accept that the duty of care will evolve alongside technology.[5] In a paper focusing on Deep Fakes, Citron and her co-author University of Texas School of Law's Robert Chesney cite the Citron/Wittes Section 230 proposal, noting that it could deter sites from hosting abusive Deep Fake content posted by users.[100]

While perhaps initially attractive, the Citron/Wittes proposal is not without issues that should give lawmakers pause. One issue to consider is the potential for unintended consequences. The duty of care could evolve in such a way that it stifles legal and valuable speech. If found liable for hosting illegal content under a Citron/Wittes regime an Internet company could potentially face crippling penalties handed down by zealous juries. In order to avoid such penalties an Internet companies' tolerance of false positives would be justified.

93 First Amended Complaint & Demand for Jury Trial at #, Herrick v. Grindr, LLC, 306 F. Supp. 3d 579 (S.D.N.Y. 2017) (No. 17-CV-932), https://www.cagoldberglaw.com/wp-content/uploads/2019/06/First-Amended-Complaint-2017.pdf.
94 Daniel v. Armslist, LLC, 2019 WI 47 (2019), https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=240009.
95 Ibid.
96 Ibid.
97 Ibid.
98 Ibid.
99 Ibid.
100 Chesney, Robert and Citron, Danielle Keats, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security (July 14, 2018). 107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21. Available http://dx.doi.org/10.2139/ssrn.3213954

As Santa Clara law professor Eric Goldman has explained, a "reasonableness" standard would make litigation less predictable and more costly.[101] The "reasonableness" standard could evolve to the point that only large and wealthy market incumbents are able to comply, putting some of the best-known Internet companies at risk. Although one of the most famous websites in the world, Wikipedia does not have nearly the number of staff (including lawyers) as Google and Facebook do. As such, a "reasonableness" standard could harm very popular websites as well as small startups. It would also eliminate Section 230's procedural benefits, making Section 230 litigation far less predictable.[102]

Chesney and Citron outline four ways to ensure that the Citron/Wittes proposal would not hamper innovation: 1) adding a sunset provision and data-gathering requirement that would allow Congress to reassess every few years, 2) damage caps, 3) linking the Section 230 changes to a federal anti-SLAPP provision, and 4) an exhaustion of remedies requirement, thereby allowing Internet sites to tackle illegal content before a plaintiff sues.[103]

It is unclear that these provisions would prevent large and wealthy incumbents from entrenching their market positions. A sunset requirement may require Congress to renew the proposed Section 230 provisions, but that hardly means that Congress will be in the habit of critically assessing the impact of these Section 230 reforms. In their discussion of this provision Citron and Chesney cite the history of Section 702 of the US Foreign Intelligence Surveillance Act.[104] Yet history of Section 702 reveals that despite widespread outcry over legitimate civil liberty concerns Congress renewed the provision.

The history of Section 702 is also rife with heated debate pre-reauthorization, with lawmakers engaged in predictable and misleading commentary.[105] Commentators and public policy professional have also weighed in on Section 702 debates, with Benjamin Wittes and Susan Hennessey writing in 2017, "The trouble is that sunset provisions presume a level of congressional functionality that is not evident today. Specifically, they presume that Congress wouldn't play chicken with an important national security authority. If 702 did not include a sunset provision, we would not be pondering changes to 702 so utterly unsupported by anything like evidence."[106] If Section 230's liability shield was up for reauthorization every two years we should expect for the content moderation debate to yield similar commentary and rhetoric.

[101] Goldman, Eric, Why Section 230 Is Better Than the First Amendment (November 1, 2019). Notre Dame Law Review, Vol. 95, No. 33, 2019.
[102] Ibid.
[103] Ibid.
[104] 50 U.S.C. sec. 1881a
[105] Jake Laperruque, "Facts on FISA: Correcting the Record on the Section 702 House Floor Debate," Just Security, January 17, 2018. https://www.justsecurity.org/51110/facts-fisa-correcting-record-section-702-house-floor-debate/
[106]Benjamin Wittes and Susan Hennessey, "Congress Wants to Tie the Intelligence Community's Hands for No Reason," *Foreign Policy*, October 13, 2017. https://foreignpolicy.com/2017/10/13/congress-wants-to-tie-the-intelligence-communitys-hands-for-no-reason/

The introduction of a sunset provision may help market incumbents because many will have more resources than competitors to adapt to developing standards of care. In the wake of this Section 230 amendment a standard of what constitutes adequate care would emerge. Complying with such a standard could be costly, and young and smaller firms seeking venture capital would have to spend resources adhering to the standard. If the data reveal that these costs are anti-competitive or resulting in excessive takedowns of legal content Congress could choose not to renew the Section 230 standard of care amendment. Such a move from Congress would result in potentially significant sunk costs for firms who invested in complying with the standard of care. Content moderation policies can be costly to implement, and not all companies are equally financially equipped to weather an environment with evolving standards of care.

Damage caps would address the risk of zealous juries discussed above. However, this would also unfairly benefit market incumbents. It would also hamper the goal of the amendment to Section 230. Large market incumbents are best positioned to pay damages. If the cap is very large it will risk stifling the growth of competitors to the benefit of large companies. If the cap is relatively small, it won't provide an adequate disincentive for companies to remove the content the Section 230 amendment is aimed at tackling.

Extremism

One category of content that has also prompted criticism of Section 230 is extremist political content. Among the most discussed of such content are associated with Islamic terrorism and white supremacy. Concerns about such content are more pronounced than they were decades ago thanks in large part to the fora for such content that have proliferated, and the strategies criminals motivated by violent ideologies have employed. Although perhaps tempting to take aim at Section 230 amid the spread of violent online content, such content does not justify Section 230 reform.

On October 27, 2018 a shooter murdered eleven people and wounded six others at the Tree of Life synagogue in Pittsburgh, Pennsylvania. The suspect, Robert Gregory Bowers, was arrested at the scene and is currently facing a host of federal charges, including hate crimes. Shortly before the attack a Gab account allegedly associated with Bowers posted, ""HIAS [Hebrew Immigrant Aid Society] likes to bring invaders in that kill our people. I can't sit by and watch my people get slaughtered. Screw your optics, I'm going in."[107] Gab is a social media website known for its far-right, white supremacist, and conspiracy theory content.

[107] Miriam Jordan, "HIAS, the Jewish Agency Criticized by the Shooting Suspect, Has a History of Aiding Refugees ," *The New York Times*, October 28, 2019. https://www.nytimes.com/2018/10/28/us/hias-pittsburgh-robert-bowers.html

In the wake of the attack, Senator Warner (D-VA) said the following: "I have serious concerns that the proliferation of extremist content — which has radicalized violent extremists ranging from Islamists to neo-Nazis — occurs in no small part because the largest social media platforms enjoy complete immunity for the content that their sites feature and that their algorithms promote."[108]

Less than a year later another shooter who frequented white supremacist websites murdered 51 people and wounded 49 others in an attack on two mosques in Christchurch, New Zealand. The shooter livestreamed the atrocity to a Facebook account via a camera attached to his helmet.

The footage of the Christchurch shootings proliferated across the Internet. Sen. Richard Blumenthal (D-CT) criticized some of Silicon Valley's best-known firms for not doing enough to halt the spread of racist content, saying that they have "turned a blind eye to hate & racism on their platforms for a decade."[109] He added, "Facebook & other platforms should be held accountable for not stopping horror, terror, & hatred—at an immediate Congressional hearing." Rep. Bennie Thompson (D-MS) wrote a letter to the chief executives of Facebook, Twitter, YouTube, and Microsoft stating, "You must do better. […] If you are unwilling to do so, Congress must consider policies to ensure that terrorist content is not distributed on your platforms."[110]

Amid the plethora of legal and unremarkable information uploaded to social media sites footage of atrocities and comments made by murderers is likely to be the content that makes headlines. As such content proliferates like a digital hydra criticism of the most popular social media sites is understandable. But it's not at all clear that the spread of extremist content is evidence that interactive computer services should lose Section 230 liability protection or that attempts by Silicon Valley's most famous firms to counter extremist content are the equivalent of turning a blind eye.

In discussions about extremist content we should begin by conceding that it will continue to be a presence on the Internet as long as there is demand for it. We should also note that the Internet is much more than Silicon Valley. Even if household name companies such as YouTube, Facebook, and Twitter were able to eliminate 100% of extremists content it would still exist on sites such as Gab, encrypted messaging apps, foreign services, sites hosted on the "Dark Web," and on decentralized file sharing networks.

[108] Tony Romm, "Hate speech tied to suspect in synagogue massacre rekindles calls for regulating social media," *The Washington Post*, 10/29/2018. https://www.washingtonpost.com/business/economy/hate-speech-tied-to-suspect-in-synagogue-massacre-rekindles-calls-for-regulating-social-media/2018/10/29/38235396-dbd1-11e8-b732-3c72cbf131f2_story.html

[109] Senator Richard Blumenthal, Twitter Post. March 16, 2019, 2:52PM. https://twitter.com/SenBlumenthal/status/1106991693860089856

[110] Rep. Bennie Thompson, "Chairman Thompson: Tech Companies Must Work to Stop Spread of Terrorist Content," letter to Mark Zuckerberg, Susan Wojcicki, Jack Dorsey, and Satya Nadella, March 19, 2019, https://homeland.house.gov/news/correspondence/chairman-thompson-tech-companies-must-work-to-stop-spread-of-terrorist-content.

Fortunately, the vast majority of the billions of people who use the Internet are not seeking such content, and the largest social media firms have outlined content policies that prohibit it. These policies do not enforce themselves, and a coalition of human moderators, AI tools, and user reporting features combine to form content moderation enforcement efforts. These efforts are not perfect, but they seek to enforce the firms' prohibitions on legal speech (e.g. hate speech, pornography, beheading videos) and police the platforms for illegal content (e.g. child pornography, improperly shared copyrighted content).

The task is gargantuan. In one day, Facebook's 2.4 billion users send about 100 billion messages.[111] YouTube users upload more than 400 hours of video to the platform every minute.[112] In such an environment it's inevitable that some content that runs afoul of the law and these companies' content moderation policies will make it through the collection of human moderators and AI screenings. Critics of "Big Tech" should not let the perfect be the enemy of the good.

As footage of the Christchurch shooting spread around the world YouTube removed human moderators from the process, using AI tools to identify and remove copies of the footage.[113] Amid the global outrage directed at the shooter and his video YouTube were willing to run the risk of many false positives as it attempted to purge its platform of the video.[114] YouTube's AI content moderation tools were up against users who were attempting to avoid detection by altering the video.[115] Although YouTube declined to give detailed data related to the Christchurch shooting it did confirm that tens of thousands of videos were removed as part of its Christchurch take-down effort.[116]

Facebook claimed that it removed 1.5 million videos of the attack within 24 hours of the shooting, adding that 1.2 million were removed "at upload."[117]

Facebook's and YouTube's efforts to remove the Christchurch shooter's footage is hardly evidence that they have "turned a blind eye" to racist content. Today, it is still possible to find the

111 Facebook, "Company Info | About Facebook," https://about.fb.com/company-info/.
112 YouTube, "Official YouTube Blog: An Update on Our Commitment to Fight Terror Content Online," August 1st, 2017. https://YouTube.googleblog.com/2017/08/an-update-on-our-commitment-to-fight.html.
113 Isobel Asher Hamilton , " YouTube's human moderators couldn't stem the deluge of Christchurch massacre videos, so YouTube benched them," Business Insider, March 18, 2019. https://www.businessinsider.com/YouTube-benched-humans-and-used-ai-to-deal-with-christchurch-massacre-2019-3
114 Ibid.
115 Ibid.
116 Ibid.
117 Andrew Liptak " Facebook says that it removed 1.5 million videos of the New Zealand mass shooting," The Verge, March 17, 2019. https://www.theverge.com/2019/3/17/18269453/facebook-new-zealand-attack-removed-1-5-million-videos-content-moderation

Christchurch shooter's video. Indeed, thanks to the nature of decentralized file sharing systems there are many people around the globe who are storing pieces of copies of the video without realizing it.

Shortly after the Pittsburgh Tree of Life synagogue shooting many companies terminated their relationships with Gab, including PayPal, Stripe, and Blackblaze. Gab's hosting provider, Joyent, ceased hosting Gab after the shooting, and the site went down until Epik, a registrar known for hosting white supremacist content, allowed Gab back online.

The history of Gab in the wake of the Tree of Life shooting highlights two important facts that Section 230 critics must address.

First, the Internet is much more than Silicon Valley. While some Silicon Valley firms have become household names, they own platforms that are part of a larger ecosystem of competing sites operating on the Internet's infrastructure. For the foreseeable future YouTube and Facebook will remain among the most popular venues for people to upload content, but sites that cater to specific ideologies will continue to function.

Second, firms operating in a market can respond to preserve reputations. Large companies cut ties with Gab after the Tree of Life shootings. Faced with choosing between association with well-known white supremacists and losing a customer many firms chose the latter. In addition, some of Silicon Valley's best-known companies have funded efforts to tackle extremism. For example, Google's Jigsaw aims to identify those becoming radicalized by white supremacists and Islamic extremists.

Section 230 amendments motivated by Silicon Valley's perceived failures to remove extremist content will result in platforms engaging in over-moderation and risk entrenching market incumbents into their dominant positions.

Conclusion

Section 230 of the Communications Decency Act is an elegant solution to a dilemma that risked hampering the growth of the Internet. Despite its elegance it is not without critics, many of whom are seeking to address online content that is offensive and an affront to people's dignity. Other critics are concerned about the role of "Big Tech," which they perceive to be one part in a wider political and cultural conflict.

These sets of concerns do not justify amendments to Section 230. While perhaps tempting,

changes to Section 230 risks stifling speech and competition. Those seeking to address the issues outlined above should look beyond Section 230 reform.