Distribution Agreement

In presenting this thesis as a partial fulfillment of the requirements for a degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter now, including display on the World Wide Web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Julian McCarthy April 9th, 2021

Section 230: Big Tech's Legal Shield and the Ultimate Threat to Democracy

by

Julian McCarthy

Tanine Allison
Adviser

Film and Media Studies

Tanine Allison

Adviser

Katherine Vigilante

Committee Member

Beretta Smith-Shomade

Committee Member

2021

Section 230: Big Tech's Legal Shield and the Ultimate Threat to Democracy

By

Julian McCarthy

Tanine Allison

Adviser

An abstract of
a thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Arts with Honors

Film and Media Studies

2021

Abstract

Section 230: Big Tech's Legal Shield and the Ultimate Threat to Democracy
By Julian McCarthy

This thesis seeks to analyze Section 230 and its impact on the structure of the Internet and Web 2.0, the business models of today's information service providers (ISPs), and the current misinformation crisis. Subsection (c)1 of Section 230 states, "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." Jeff Kosseff has called Subsection (c)1 "The Twenty-Six Words That Created The Internet" because it prevents ISPs from being held liable for any harmful third-party content on their platforms and, subsequently, turn a blind eye to it. As a result, the information ecosystem has been poisoned by misinformation, disinformation, malinformation, and conspiracy theories. These fraudulent information variants have corrupted public opinion, undermined democracy, and relegated consumers to a hyperreality, where they are unable to discern fact from fiction.

I argue there has been a significant discrepancy between Section 230's intent versus its application. Subsection (c)2 of Section 230, also known as the "Good Samaritan" provisions, showcases that one of the law's primary goals was to give ISPs immunity for the third-party content on their platforms to encourage them to develop purposeful regulatory procedures for user-generated content. Instead, many ISPs have utilized Section 230's immunity for third-party content without enacting these procedures because of a profit-maximizing ideology. This work builds on the existing Section 230 scholarly literature by highlighting this discrepancy, analyzing Justice Clarence Thomas's recently released opinion about Section 230's wrongful application in *Zeran,* and explaining how Section 230 has influenced the structure of the digital sphere and contributed to the rise of dishonest content online.

Section 230: Big Tech's Legal Shield and the Ultimate Threat to Democracy

By

Julian McCarthy

Tanine Allison

Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Arts with Honors

Film and Media Studies

2021

Acknowledgements

I want to thank Dr. Tanine Allison for her unwavering support during this project. She truly took me under her wing and provided me with incredible feedback that greatly contributed to the final product of my thesis.

I would also like to thank Dr. Katherine Vigilante, who has been an invaluable mentor and resource throughout my entire academic career. As my first political science professor, she sparked an intellectual curiosity that I never knew I had and made me fall in love with media policy. It has been one of the greatest joys of my college experience to finish my journey at Emory with Dr. Vigilante just as I started it with her four years ago.

Lastly, I'd like to thank my parents for always telling me I could accomplish anything I set my mind to. I'm so grateful that I grew up in a loving family where it was acceptable to fail because it taught me how to pick myself up and the true value of resilience and grit. Thank you for giving me the opportunity to go to such an amazing school and making me feel like my voice matters.

Table of Contents

Introduction

There has been a significant disconnect between the original intent of Section 230 and what it has become today: Big Tech's legal shield and the ultimate threat to democracy. Subsection (c)1 of Section 230 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." The scholarly literature on Section 230 primarily focuses on Subsection (c)1 because it has allowed technology companies to avoid any liability for third-party content that they distribute, which has made it possible for the online industry to develop into the economic powerhouse it is today. Without Section 230, information service providers (ISPs) like Wikipedia, Facebook, and Google, could be accountable for any user-generated content that circulates on their platforms, potentially forcing them to adopt strict moderation practices to avoid legal suits, undoubtedly prohibiting economic growth and putting them out of business. Subsection (c)1 of Section 230 has given technology companies the freedom to evolve into innovative, social instruments that have defied informational norms and broken down social barriers.

However, that is only part of Section 230's story. The law has allowed technology companies to turn a blind eye to the poisoning of the information ecosystem with misinformation, disinformation, and conspiracy theories. Under Section 230, the responsibility of regulating content on the Internet is placed solely on the ISPs. It is up to the ISPs, not the government or any independent regulatory organization, to moderate this digital landscape and remove harmful third-party content. But why would ISPs take down so-called "harmful" content when it generates user-activity and provides them with meaningful, consumer information they

can sell to advertisers? In other words, because Section 230 has given ISPs immunity from any third-party content suit, why would ISPs take down highly engaging, third-party content if they are abiding by a profit-maximizing ideology? It is in the technology company's economic interest to not only let harmful user-generated content exist on their platforms but to actively promote it.

This thesis seeks to fill in the gaps of Section 230's story through an analysis of the disconnect between Section 230's purpose and its application, how it has shaped the business models of major ISPs and technology companies, and the potential impact it has had on the misinformation crisis and the spread of conspiracy theories online. There is limited scholarly literature on how Section 230 has possibly contributed to the rise of digital conspiracy theories and its subsequent effects on the public's perception of reality. Chapter 1 examines Section 230's history, "Internet exceptionalism," Justice Clarence Thomas's recent opinion on the court's "dubious" interpretation of Section 230, and the law's failure to accomplish what its writers intended, as demonstrated by Section 230's "Good Samaritan" provisions.

Chapter 2 analyzes how Section 230 impacted the growth of the Internet, the rise of Web 2.0, and the business models of today's ISPs. Chapter 3 explores the different types of malignant content infecting the body of information online and how Section 230 has potentially contributed to the rise of conspiracy theories on digital media. The chapter will conclude with an in-depth examination of the 'birther' conspiracy theory and 2020 election fraud misinformation campaigns and an investigation into the potential impact of the removal of President Donald Trump and his allies from social media on the amount of misinformation and disinformation online and the public's acceptance of this content.

I argue Section 230 has structured the current digital media landscape and contributed to the misinformation crisis. While Section 230 has tremendously benefited the online space, it has

also contributed to the deterioration of the information ecosystem and exposed countless consumers to fraudulent content. I claim ISPs were granted immunity for all the third-party content on their platforms in exchange for their institution of the meaningful third-party content moderation practices outlined by Subsection (c)2 of Section 230, also known as the "Good Samaritan" provisions. Many ISPs like Twitter, Facebook, and Reddit have failed to fulfill this requirement, resulting in the proliferation of dishonest content and immeasurable harm to society at large.

Chapter 1: The History of Section 230

Introduction

The upcoming chapter will examine the history of Section 230, the context in which the law arose, and its primary intentions. Understanding the history of Section 230 and the aims of its authors, Representatives Ron Wyden (D. Oregon) and Chris Cox (R. California), reveals a colossal disparity between the intentions of the law and its application today. I argue Cox and Wyden granted ISPs immunity for all the third-party content on their platforms in exchange for developing and actively engaging in regulatory actions like removing and filtering harmful user-generated content. I make the case that Section 230 was a privilege granted to ISPs under the assumption that they would fulfill their moderation responsibilities, but, as I will prove in the later chapters, they have failed to do so.

I further contribute to the existing scholarly literature on Section 230 by examining Supreme Court Justice Clarence Thomas's recently released opinion that argues Section 230 was wrongly interpreted in *Zeran v. American Online*. I also build on Jeff Kosseff's analysis of Section 230's origins by offering additional support for his claim that "Internet exceptionalism" is at the core of Section 230, its interpretation in the courts, and the laws that govern the digital landscape (96-102). Internet exceptionalism centers on the premise that the Internet is fundamentally different from other media platforms and, as a result, should not be regulated in the same way. It's essential to remember that at the time of Section 230's creation, the Internet was breaking down informational and communal barriers as no other medium had before. This caused individuals to believe the Internet should be subject to a different set of rules and regulations. Whether they knew it or not at the time, Cox and Wyden were proponents of Internet exceptionalism. Ultimately, this chapter aims to give an in-depth explanation of the history of

Section 230 in order to make sense of the current state of the Internet and how it has enabled ISPs and technology companies to forego meaningful moderating practices.

Hypothetical

Imagine this scenario: Dr. Anderson is a new adjunct professor at Springfield University. After a successful first semester of teaching Creative Writing, she is excited to return to campus and continue working with students. One week before the semester commences, she receives a call from the head of the English department notifying her that only three students have signed up for her 50-person Intro to Creative Writing class. Dr. Anderson is shocked by the news, considering the popularity of the course the previous semester. The department head suggests the cause for such low registration is an extremely defamatory post circulating about her teaching style and Creative Writing class on *RateMyProfessors.com*. Dr. Anderson frantically googles herself on *RateMyProfessors.com* to find a page filled with comments about her, most of which are positive. However, the top comment that has been rated the most helpful comment by users says: "Dr. Anderson's Creative Writing Class is the most failed course at Springfield University. She goes out of her way to make her students fail. Do NOT take this class unless you want an F on your transcript." Dr. Anderson, appalled by the demonstrably false comment, immediately flags the post and puts in a request for it to be deleted by content moderators.

She looks up *RateMyProfessors'* policies for third-party content regulation. She finds that content moderators will review the content and remove the post only if it violates site guidelines. Dr. Anderson reaches out to *RateMyProfessors* and asks them to take down the comment. When she finally connects with a representative, they assure her that the comment will be taken down. However, three weeks pass, and the comment is still on the website. Dr. Anderson, outraged by *RateMyProfessors's* failure to take down a patently false and harmful comment that was clearly

in violation of the community guidelines, wants to sue the company for defamation. After consulting legal counsel, she discovers that the current law explicitly prohibits any such legal action from being taken. Under subsection (c)1 of Section 230, "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." In other words, Dr. Anderson cannot sue *RateMyProfessors* for the defamatory comment that was distributed on its platform because doing so would treat the company as the author of the defamatory post.

That being said, Dr. Anderson can still sue the original post's creator, but such action would be extremely arduous. Since users post their comments anonymously, Dr. Anderson would have to reach out to *RateMyProfessors* to get the author's information. An information service provider (ISP) is only obligated to release said anonymous information if the plaintiff's case could withstand summary judgment, meaning a determination could be "made on the claims involved without holding a trial" (Legal Information Institute, sec. 1; par. 1). Dr. Anderson, unequipped with the proprietary means or legal resources to make such a case, cannot repair her reputation or seek financial compensation for its damage.

The hypothetical described above is not uncommon. Countless individuals have had their reputations and livelihoods ruined because of user-generated content distributed by ISPs online. Due to Section 230, ISPs cannot be held liable for the third-party content that proliferates on their forums. In Dr. Anderson's case, *RateMyProfessors* could not be sued for its involvement in distributing the extremely damaging post. Treating *RateMyProfessors* as the author of user-generated content would be in clear violation of Section 230.

Without Section 230, all ISPs could be treated as the publisher/author of the user-generated content on their platforms. It is difficult to imagine a world where ISPs like Facebook,

Twitter, Google, Yelp, and Wikipedia could be held liable for every piece of third-party content on their platforms. If they were, they would not have grown into the tech behemoths they are today. This offers an explanation as to why Jeff Kosseff has referred to Section 230 as "The Twenty-Six Words That Created the Internet." In order to understand how Section 230 has impacted the Internet and the current digital landscape, we must examine the law's history.

The History of Section 230

In 1990, three privately-owned companies dominated the digital landscape: CompuServe Inc., Prodigy Services, and America Online (AOL). Like many modern technology companies, these ISPs supplied “curated information in the electronic versions of newspapers, newsletters, and financial advice” to a paying subscriber base (Kosseff, 37). All of the platforms, to some degree, possessed the innovative and defining participatory features associated with today’s digital landscape. Today’s social media companies like Twitter and Facebook have built their business models around the distribution of content created by users.

Prodigy Services, CompuServe Inc., and AOL were ahead of their time in the sense that subscribers could post content in the designated areas of each respective forum and interact with other users. Back then, these technological aspects were revolutionary and came with staggering communal benefits, along with an unprecedented set of consequences. ISPs had to figure out how and to what extent they would edit, remove, or promote the content posted by their users. They were in uncharted territory, and with no defining technological or legal precedent, these three platforms adopted different strategies to moderate the third-party content on their forums.

Robert Blanchard was the earliest person to file a defamation suit against an ISP for content posted by a third-party in *Cubby, Inc. v. CompuServe Inc*. He was distraught when an article published by *Rumorville* circulated on CompuServe, alleging he had been fired from his

most recent job at WABC for journalistic malpractice. Instead of pressing charges against the anonymous user, he chose to sue CompuServe Inc. for distributing and promoting the damaging article. Peter K. Leisure, the District Court Judge for the Southern District of New York, ruled:

> "Plaintiffs have not set forth any specific facts showing that there is a genuine issue as to whether CompuServe knew or had reason to know of Rumorville's contents. Because CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements, summary judgment in favor of CompuServe on the libel claim is granted" (U.S. District Court, Southern District of NY, 6).

In other words, Judge Leisure ruled that CompuServe Inc. was merely a distributor of the defamatory content, not the author. Therefore, CompuServe Inc. could only be held liable if the company "knew or had reason to know" about the defamatory content. Due to the plaintiff's inability to provide sufficient evidence that CompuServe Inc. "knew or had reason to know" about the defamatory content, Judge Leisure ruled that they could not be held liable for it (U.S. District Court, Southern District of NY, 5). He pointed out CompuServe had "little or no editorial control over that publication's contents" and, therefore, had no reason to know about the defamatory content (U.S. District Court, Southern District of NY, 5). In other words, CompuServe Inc.'s hands-off moderation approach effectively shielded it from legal liability because it was simply a distributor of content and exercised little to no regulatory control over the content posted on its forum.

Four years later, Prodigy Services would face a similar suit and receive a different outcome due to the contrast in its third-party content moderation practices. Unlike CompuServe Inc., Prodigy Services adopted a more intense moderation approach where it had substantial

regulatory control over what was published on its forum. Prodigy Services marketed its platform as a family-oriented alternative to other ISPs like CompuServe Inc. that exercised no regulatory control over the content posted on its forum. On its website, Prodigy Services made a commitment to “not carry messages that are obscene, profane or otherwise offensive” (Kosseff, 44). As a result, users of the platform had a different set of expectations regarding the degree to which Prodigy Services would regulate third-party content. One of those users was Daniel Porush, the president of Stratton Oakmont, a New York banking firm. When he noticed harmful, defamatory material circulating on the platform about him and his company, he sued Prodigy Services.

Prodigy Services moved to dismiss the case on the grounds of the *Cubby Inc. v. CompuServe Inc.* precedent. The *Cubby Inc. v. CompuServe Inc.* precedent established that ISPs were distributors of third-party content, not publishers/authors. Therefore, ISPs could only be held liable if the plaintiff proved the company "knew or had reason to know" about the harmful material. However, Daniel Porush's legal team pointed out the "knew or had reason to know" standard that had effectively vindicated CompuServe Inc. from accountability did not apply to Prodigy Services because of the difference in how the company moderated third-party content. Whereas CompuServe Inc. adopted a hands-off moderation approach to user-generated content, Prodigy Services could screen and filter the third-party content on its forum and made a commitment to do so. New York Supreme Court Justice Stuart L. Ain ruled, "Prodigy's 'conscious choice,' to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice" (New York Supreme Court).

In other words, Justice Ain ruled Prodigy Services' effort to create a family-friendly digital environment and ability to exercise "editorial control" over third-party content made it a publisher/author of the damaging content, not a distributor. Consequently, Prodigy Services' control over the user-generated content on its platform opened it up to legal liability for the defamatory third-party content posted about Daniel Porush and his company. Why would an ISP make any effort to regulate third-party content if doing so meant it would be held accountable for all the third-party content on its platforms? In this way, the *CompuServe Inc.* and *Prodigy Services* rulings encouraged ISPs to take a hands-off regulatory approach. Not doing so would make them liable for all the third-party content on their platforms. Ultimately, any efforts to eliminate harmful user-generated content would forfeit their immunity as distributors, classify them as publishers/authors of all the third-party content on their platforms, and put them in legal jeopardy.

With a lack of laws to moderate the Internet and ISPs neglecting to regulate their forums, adult content, specifically child pornography, flourished online and came in contact with users of all ages, prompting the public to call on the government to intervene. Senator J. James Exon (D. Nebraska) from Nebraska was determined to limit this offensive material on the Internet. In 1995, he wrote legislation called the Exon amendment, which "criminalized the knowing transmission of obscene or indecent material to anyone less than eighteen years of age through a telecommunications device" (Spiccia, 385). According to Senator J. James Exon's legislation, ISPs and technological intermediaries could face legal repercussions for playing any role in transmitting "indecent" content on their platforms.

Senator J. James Exon hoped his legislation would reduce the immense amount of adult content on the Internet because it would effectively force ISPs to engage in extreme regulatory

practices to avoid fines or even prison time. The radical legislation garnered substantial attention from the press because of its radical approach to Internet regulation and the potential to violate a citizen's First Amendment rights. The Exon amendment would allow the government to punish ISPs for failing to monitor the third-party content on their platforms. As a result, it was more than likely that ISPs would have to intensely regulate their platforms and censor any material that could get them in trouble. Many argued that the Exon amendment would deny adults access to speech they had a constitutional right to receive and cause individuals to be unduly censored. While the Exon amendment was generating a great deal of controversy in the Senate, Congressmen Ron Wyden and Chris Cox were scrambling to produce alternative Internet legislation in the House of Representatives.

Section 230's Inception

Chris Cox, a Republican representative from California's 47th district, and Ron Wyden, a Democrat from Oregon's 3rd district, fundamentally disagreed with Senator Exon's extreme regulation approach to the Internet. They believed the Exon amendment would unequivocally prevent the development of the Internet because it would force ISPs to take down any content that could potentially violate the law. They also anticipated that ISPs would face an insurmountable number of online consumers' lawsuits alleging First Amendment rights violations because of ISP censorship. Cox and Wyden believed these suits would drain tech companies of time and money and, ultimately, prevent them from reaching their full potential.

It is important to remember that although the Internet was changing communication and revolutionizing how consumers accessed information, it was still incredibly premature. As outlined above, there were only a few big players and a complete lack of the characteristics associated with today's digital landscape, like large-scale accessibility and interactivity. Cox and

Wyden thought that the Exon amendment would ruin any chance the Internet and ISPs had to prosper. This led them to draft Section 230, a piece of legislation that would remove ISP liability for all third-party content and encourage voluntary moderation practices.

Section 230 was a far less restrictive approach to Internet regulation than the Exon amendment. Unlike the Exon amendment, Section 230 rejected government interference and the penalization of ISPs for their role in distributing any piece of third-party content. When asked about the intentions of Section 230, Representative Ron Wyden said, "We really were interested in protecting the platforms from being held liable for the content posted on their site and being sued out of existence" (Kosseff, 64). Wyden asserted that they had two primary goals in mind when they wrote Section 230. The first was to ensure the Internet's unfettered growth. The second was to do away with the *Prodigy Services* and *CompuServe Inc.* precedents that encouraged ISPs not to regulate any harmful, consumer-generated material on their platforms. Cox and Wyden thought the Internet medium had boundless commercial potential as long as it was not subject to the same liability laws as other media formats.

This led them to write subsection (c)1 of Section 230, which states, "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" (47 U.S.C. § 230). As exemplified by the hypothetical at the beginning of the chapter, subsection (c)1 of Section 230 prevents a company like *RateMyProfessors* from being held legally liable for the defamatory post about Dr. Anderson. Doing so would treat the "interactive computer service," in this case, *RateMyProfessors*, as the "publisher or speaker" of the post. In other words, Section 230 prohibits ISPs from being treated as the authors of third-party content.

Subsection (c)1 of Section 230 effectively accomplished Cox and Wyden's goal to liberate ISPs from any legal liability of the third-party content on their platform, regardless of whether they made any effort to moderate that content. It is essential to remember that under the *Prodigy Services* and *CompuServe Inc.* precedents, ISPs that regulated or edited third-party content made themselves the authors of said content and, thus, were liable for all the third-party content posted on their forums. Subsection (c)1 of Section 230 resolved this dilemma and would later become the foundation of today's digital landscape, which I will discuss in chapter 2.

Jeff Kosseff has referred to subsection (c)1 of Section 230 as the backbone of today's $550 billion online industry (539). He points out that a technology company like Facebook could not rise to media dominance without subsection (c)1 of Section 230 (539). Under the *Prodigy Services* and *CompuServe Inc.* precedents, if Facebook engaged in any regulatory action, the company could be treated as the publisher of any of the third-party content that circulated on its forum and, as a result, subject to countless lawsuits. Facebook has been subject to serious criticism because of information posted by its billions of users. If it were not for subsection (c)1 of Section 230, Facebook would have the virtually impossible job of screening all user posts and the burden of arguing that it should not be liable for each post in court if a user decided to file suit. Subsection (c)1 of Section 230 has allowed the Internet to develop into the economic powerhouse that it is today.

Cox and Wyden's other motivation behind Section 230 was to rectify the contradictory *Prodigy Services* and *CompuServe Inc.* precedents that incentivized ISPs to not make any effort to regulate the third-party content on their mediums. While the Exon amendment called for government interference through the Federal Communications Commission (FCC), Cox and Wyden wanted to leave content regulation up to ISPs. Representative Wyden said, "We were

interested in allowing platforms to take down some content that they believe shouldn't be on their site without being held liable for all the content on the site so that you could really encourage responsible behavior" (Kosseff, 64). This led them to write subsection (c)2 of Section 230, also known as "The Good Samaritan" provisions. "The Good Samaritan" provisions state,

> "No provider or users 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 provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected" (47 U.S.C. § 230).

In other words, "The Good Samaritan" provisions gave ISPs the right to make "good faith" restrictions on the material they deemed to be inappropriate without fear of being sued. The "Good Samaritan" provisions allow an ISP like *RateMyProfessors* to take down any user-generated content that it decides violates its communal guidelines without fear of being sued for violating the author's constitutional rights. Subsection (c)2 of Section 230 was a crucial part of Cox and Wyden's solution to the proliferation of adult content online. They wanted ISPs to have the freedom to take down any third-party content they deemed inappropriate without fear of being held liable for all the third-party content on their platform. They also wanted ISPs to have the final say in the third-party content on their forum, in contrast to the Exon amendment, which gave that power to the government.

The "Good Samaritan" provisions would allow ISPs to create their own community guidelines and regulate their platforms to the extent they saw fit, as long as their efforts to remove third-party content were made in "good faith." Under Cox and Wyden's legislation, ISPs would have all the regulatory power and none of the concerns about government interference or

consumer lawsuits that alleged constitutional violations. Ultimately, the passage of Subsection (c)2 of Section 230 would effectively override the *Prodigy Services* and *CompuServe Inc* precedents, which incentivized ISPs to not impose any regulations on third-party content to avoid legal liability. With the passage of Subsection (c)2, an ISP like Prodigy Services would be able to actively screen and filter user-generated content without liability for all the third-party content on its forum. If the "Good Samaritan" provisions passed, an ISP like Prodigy Services would have the freedom to foster the family-friendly digital environment it advertised.

In contrast to the Exon amendment, Section 230 gave all the regulatory power to ISPs. It cannot be overstated that one of Cox and Wyden's main goals was to support the Internet's continued development. Cox and Wyden did not want ISPs plagued by excessive lawsuits for the third-party content that circulated on their platforms because they believed it would prevent them from reaching their full economic potential. Cox and Wyden also made clear that they wanted ISPs to have the power to regulate their own platforms. In the law itself, Cox and Wyden explicitly state that Section 230 should "remove disincentives for the development and utilization of blocking and filtering technologies" (47 U.S.C. § 230). Section 230 removed ISP liability for third-party content to allow ISPs to make "good faith" regulatory actions without being held liable for all the third-party content on their forum. In my opinion, Cox and Wyden gave ISPs immunity for all the third-party content on their platforms in exchange for their institution of meaningful moderating practices.

However, neither Cox nor Wyden foresaw that ISPs would utilize the benefits of Section 230 immunity for all the third-party content on their platforms without engaging in any "good faith" moderation practices outlined by the "Good Samaritan" provisions. In other words, they did not predict ISPs would take advantage of the benefits of Subsection c(1) of Section 230

without engaging in the behaviors encouraged in Subsection (c)2. As a result, there has been a significant disconnect between Section 230's intended outcomes and reality. In my research, I have found that Subsection (c)1 of Section 230 often garners a disproportionate amount of media attention compared to Subsection (c)2, causing many misinterpret Section 230. I argue Section 230 was intended to encourage ISPs to regulate their platforms, not give them a free pass from doing so.

Despite the massive impact Section 230 would have on the digital landscape at the time and in the future, the bill moved through the legislative process with little opposition. Instead of one piece of Internet legislation being picked over the other, Section 230 was combined with the Exon amendment. In his article "The Origins and Original Intent of Section 230 of the Communications Decency Act," Chris Cox explains that by the time Section 230 passed in the House of Representatives, the Exon amendment had already passed in the Senate with 84 votes (sec. 4 par. 2). The senators that voted in favor of the Exon Amendment did not want to rescind their votes on an issue as controversial as pornography. Chris Cox explains that because they had already gone "on record with a vote one way — particularly a highly visible vote on the politically charged issue of pornography — it would be very difficult for a politician to explain walking it back" (sec 4 par. 2). Consequently, Section 230 and the Exon amendment formed one piece of legislation, which became The Communications Decency Act.

The Communication Decency Act was then added to the Telecommunications Act of 1996. The Telecommunications Act of 1996 was a larger piece of legislation that aimed to update laws that had governed phone, radio, and television services. The Internet was so underdeveloped in 1996 that it was not the focus of the larger piece of legislation, which is partly why Section 230 passed through Congress with such ease. Additionally, whatever attention was

on the Communications Decency Act was focused on the Exon amendment, not Section 230, because of the Exon amendment's harsh Internet regulation approach. Nonetheless, The Telecommunications Act of 1996, including the Communications Decency Act, was passed by Congress and signed into law by then-President Bill Clinton in 1996. The Exon amendment and Section 230 were officially the laws of the Internet landscape.

When the Communications Decency Act became law, the American Civil Liberties Union (ACLU) immediately filed a lawsuit to question the constitutionality of the Exon Amendment in *ACLU v. Reno.* The ACLU claimed the Exon amendment was unconstitutional because it "censored and criminalized expression protected by the First Amendment and because the terms' indecency' and 'patently offensive' are unconstitutionally overbroad and vague" (ACLU, sec 1; par 1). The Supreme Court ruled by a vote of 7-2 that the Exon amendment of the Communications Decency Act was in violation of the First Amendment. Supreme Court Justice John Paul Stevens delivered the majority opinion. He stated, "We agree with the three-judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment" (U.S. Supreme Court, 849). In its decision, the Supreme Court ruled preserving the freedom of expression on the Internet outweighed any potential benefit that could come from the censorship of harmful user-generated material. Thus, the courts struck down the Exon amendment as unconstitutional, and Section 230 was all that remained of the CDA.

Section 230's Interpretation

It was unclear how broadly the courts would interpret Section 230's immunity for third-party content. It was understood that Subsection (c)1 of Section 230 provided ISPs with immunity for all the third-party content on their platforms. But the courts had to decide whether the "knew or had reason to know" standard that applied *Cubby Inc. v. CompuServe Inc.* should

apply to Section 230. As a reminder, "the knew or had reason to know" standard effectively liberated CompuServe Inc. from liability for third-party content. In *Cubby Inc. v. CompuServe Inc.*, the Court ruled that CompuServe Inc. could not be held liable for the third-party content on its platform because there was no evidence to suggest that the company "knew or had reason to know" about the harmful content. Because CompuServe Inc. made no effort to screen or filter any of the content on its medium and had little ability to do so, the company liberated itself from liability for all third-party content.

In 1995, a domestic terrorist attack that killed 168 people occurred at the Alfred P. Murrah federal building in Oklahoma City. The tragedy garnered a significant amount of media attention, causing speculation about the attack's origins and motivations to run rampant on the Internet. Unlike the accredited media formats of the time, the still-developing Internet was a place where consumers could post harmful misinformation and unverified opinion. On American Online (AOL), an anonymous user began to post t-shirt advertisements with the bombers' names, offensive slogans, and instructions to call a phone number.

The phone number belonged to Kenneth M. Zeran, a man who had no relationship to the Oklahoma City bombing or the anonymous poster. Nevertheless, people online began to call and harass him incessantly. He immediately contacted AOL to take down the posts, which it did. However, once AOL deleted them, new ones emerged with the same kind of instructions. Fed up with AOL's inability to remove harmful third-party content it knew about, Zeran filed a negligence suit. The courts had to answer the question: Does Section 230 of the Communications Decency Act protect an ISP like AOL from being held liable for harmful third-party content that they knew about?

Zeran v. America Online was the first case to interpret Section 230 and would become the overriding precedent for years to come. At the heart of the case was the distinction between publishers/authors and distributors of third-party content. The defense claimed that the suit treated AOL as "the publisher or speaker of any information provided by another information content provider," which Section 230 explicitly prohibited. On the other hand, Zeran's legal team attempted to convince the court that its lawsuit did not treat AOL as the publisher/author of the harmful content, but instead as a distributor with knowledge of the harmful content that failed to remove it, thus nullifying Section 230 immunity.

The presiding judge, Harvie Wilkinson III, had to decide what would happen if an ISP, like AOL, "knew or had reason to know" about the harmful third-party content but did not remove it. In Zeran's case, he made AOL aware of the harmful content on its platform, and the company failed to remove it adequately. The court had to answer the question: Should knowing about the harmful content and failing to take it down result in AOL forfeiting their immunity for third-party content granted to them by Subsection c(1) of Section 230? After hearing oral arguments, Judge Wilkinson ruled that distributor liability was "a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230" (U.S. Appellate Court, 4th Circuit, 4). In other words, Judge Wilkinson decided that the distinction between publisher/author and distributor did not matter because they were both protected by Section 230 immunity. According to some scholars, Judge Wilkinson's ruling wrongly "defined the scope of Section 230 immunity" for years to come (Ziniti, 585).

According to Jeff Kosseff, Judge Wilkinson opted "to interpret Section 230's prohibition on treating online services as publishers or speakers of third party content" as meaning "these platforms have absolutely no liability for third-party content unless an exception is applied"

(Kosseff, 76). His ruling made it practically impossible to hold ISPs legally liable for the third-party content on their platform, regardless if they "knew or had reason to know" about it. In this interpretation, ISPs would not face any legal liability for any third-party content, even if they did not instate meaningful moderation practices. It is worth noting this interpretation of Section 230 adhered to Cox and Wyden's vision for the internet to be a free market, where privately owned businesses controlled the third-party content on their platforms, instead of the government or any other independent organization. However, the interpretation also allowed ISPs to get away with distributing content they know to be harmful.

If the courts had opted for the "knew or had reason to know" interpretation of Section 230, ISPs would face a new set of burdens regarding third-party content regulation. This would have drastically changed the outcome of the hypothetical discussed at the beginning of this chapter. As a reminder, *RateMyProfessors* was notified about the harmful post about Dr. Anderson but failed to take it down. Dr. Anderson's act of informing the company about the comment would sufficiently fulfill the "knew or had reason to know" standard. Under this new interpretation, she would be able to sue the company for the damage resulting from the harmful post because *RateMyProfessors* "knew or had reason to know" about the harmful third-party content and did not take it down.

As a result, ISPs would more than likely have to engage in mass censorship practices to avoid costly suits. Without Section 230, it would be in an ISPs best economic interest to delete any third-party content that could lead to a lawsuit. This would be extremely difficult for smaller ISPs that have less funding and fewer employees. They would have a more challenging time than larger ISPs because they don't have the resources to monitor all the third-party content on their forums or fend off many lawsuits. It is difficult to imagine a world where a company like

YouTube could be sued for failing to remove the third-party content posted on its forum once notified. If the courts had accepted the "knew or had reason to know" interpretation of Section 230, it would have unequivocally altered the Internet's future.

The *Zeran* ruling's significance cannot be overstated. According to Patricia Spiccia, a Section 230 scholar, the original text of Section 230 "suggests that the statute's scope is narrow—applying only to defamation claims and good faith efforts to self-regulate" (386). However, in the *Zeran* case, Judge Wilkinson chose to rule on the broader implications of Section 230. According to Justice Clarence Thomas, he established the highly controversial precedent Section 230 "confers immunity even when a company distributes content that it knows is illegal" (US Supreme Court, 4). The *Zeran* case has become the defining precedent for Section 230 and, ultimately, set the tone for how the Internet is regulated, or more accurately, not regulated.

Justice Clarence Thomas's Critique

In October 2020, Justice Clarence Thomas, one of the current Supreme Court justices, wrote the majority opinion for *Malwarebytes Inc. v. Enigma Software Group USA, LLC*. In the majority opinion, he claimed the courts wrongly interpreted Section 230 in the *Zeran* case. He argued Section 230 was not meant to protect ISPs from all liability for user-generated content. Justice Thomas conceded Section 230 should prohibit technology companies from being treated as the "publisher or speaker" of third-party content. In other words, he agreed that ISPs should not be treated as the authors of user-generated content. However, he argued that the law should not totally shield online platforms of distributor liability when they "knew or had reason to know" about the harmful third-party content like AOL did in *Zeran*. Justice Thomas claimed that if Section 230 intended to immunize ISPs from distributor liability entirely, it would have done

so in the text. He said, "Had Congress wanted to eliminate both publisher and distributor liability, it could have simply created a categorical immunity in §230(c)(1): No provider "shall be held liable" for information provided by a third party" (U.S. Supreme Court, 5).

With his written opinion, Justice Thomas condemned the *Zeran* ruling and made the claim that Judge Wilkinson wrongly expanded the powers of Section 230. He said the *Zeran* interpretation rejected the most "natural reading of the text by giving Internet companies immunity from their own content" (U.S. Supreme Court, 6). He pointed out the information content provider definition explicitly listed in Subsection (c)1 of Section 230, explicitly classifies an information content provider as anyone "responsible, in whole or in part, for the creation or development" of the content (U.S. Supreme Court, 6). In other words, Justice Thomas questioned what it means to participate in "the creation or development" of content and the legal criteria used to evaluate authorship liability for interactive computer services as outlined in the text of Section 230.

For example, when technology companies remove or edit third-party content and then distribute it to consumers, would that qualify as "the creation or development" of content? Justice Thomas deems it "dubious" to not classify it as such (U.S. Supreme Court, 7). Ultimately, Justice Thomas makes the case that the Court interpreted Section 230 too broadly in *Zeran*. His incredibly cohesive and logical argument effectively undermined the *Zeran* ruling and raised pertinent questions for the courts to consider in future interpretations of Section 230.

Internet Exceptionalism

Jeff Kosseff argues that Internet exceptionalism has led ISPs and online services to be practically immune from the law compared to other more traditional media formats like newspapers, radio, and television (96-102). According to Tim Wu, the Internet has changed how

we communicate and access information, effectively distinguishing itself from other media formats. He says, "Technologically, and in its effects on business, culture, and politics, the Internet seems, by almost any account, an exception, different from the way other systems of mass communications have operated, whether the telephone, radio or the television (8).

As I will discuss in chapter 2, a newspaper can be sued for distributing the content its reporters publish in contrast to ISPs on the Internet. A newspaper is legally liable for the news stories it publishes and the comments on its forum. However, under Section 230, ISPs and technology companies cannot be held accountable for any third-party content regardless of the content's nature. As I will explain in chapter 3, Section 230 is potentially responsible for Holocaust denial pages and QAnon conspiracy theories proliferating on digital media platforms and contaminating the information ecosystem. Because Section 230 grants ISPs immunity for all the third-party content on their platform, they have no legal obligation to take down these harmful posts.

Ultimately, I believe Internet exceptionalism is partially to blame for technology companies like Facebook, that despite actively poisoning our information ecosystem with misinformation, interfering in Americana democracy, and selling private consumer information, only pays less than 1% of its earnings in taxes (Pickard, 128). Whether Cox and Wyden were cognizant of it at the time, they were firm believers in Internet exceptionalism, as reflected by the language and purpose of Section 230. With Section 230's creation, Cox and Wyden distinguished the Internet from other media formats. As Jeff Kosseff discusses in his book, Cox and Wyden made it clear that the Internet's innovative participatory properties and dynamic features, such as immediacy and editorial control, effectively made it above the law.

One could understand why they wanted to subject the Internet to different legal and regulatory standards. However, it is undeniable that the unintended consequences of Section 230 on our information ecosystem have been costly and allow ISPs to engage in egregious conduct. One of those ISPs is *Backpage.com.*

The *Backpage.com* Scandal

In the last 24 years, there has only been one revision to Section 230. *Backpage.com* was an advertising website, where users could sell material items. The platform was designed to function as a classified version of a *News Weekly* that simultaneously ran personal ads. In other words, the website's business model depended on third-party content, meaning that *Backpage.com* needed users to actively post on the forum and interact with one another for the company to generate revenue. The website got into legal trouble in 2017 for its "Adult Entertainment" section, where users were found to be engaging in commercial sex trafficking. After several state Justice Department investigations, multiple attorney generals linked the advertisements on *Backpage.com* to several child prostitution cases. The Senate launched an investigation into the matter and demanded that *Backpage.com* remove the sex trafficking advertisements on its platform. Despite the Senate's mandate, sex trafficking persisted on the site, and it was "clear that *Backpage* knew that its users were posting sex trafficking ads, yet it failed to take all possible steps to stop them" (Kosseff 256). As a result, three child prostitution victims advertised on *Backpage.com* filed a class action against the company alleging the company had participated in sex trafficking.

Despite *Backpage.com's* failure to shut down these ads, the Court ruled that *Backpage.com* could not be held liable for third-party content because doing so would treat the company as "the publisher or speaker" of third-party content. In other words, the Court ruled that

Backpage.com could not be sued for its involvement in distributing the commercial sex advertisements that led the plaintiffs to be sold into prostitution because of Section 230. The public met the ruling with outrage and demanded the government revise Section 230 to prevent sex trafficking on these platforms and protect children.

In 2017, Congress passed legislation that prohibited the behavior of ISPs like *Backpage.com*. According to Jeff Kosseff, the legislation allowed victims to "recover damages" from an ISP if they engage in commercial sex trafficking (270). The law amended Section 230 and, for the first time, made ISPs liable for not taking "good faith" efforts to regulate the third-party content posted on their platforms. This instance showcased that there is a limit to the immunity Section 230 provides, and established Section 230 can be reformed in the future.

Conclusion

As demonstrated by this chapter, there has been a massive disconnect between what Section 230 was intended to do and how it has been implemented by ISPs today. I believe Internet exceptionalism and the overbroad *Zeran* interpretation of Section 230 are partially responsible for this disconnect. Section 230 was intended to incentivize ISPs to engage in the actions outlined in the "Good Samaritan" provisions. Instead, ISPs like *Backpage.com* have utilized the Section 230 immunity for all the third-party content on their platforms without engaging in meaningful moderation practices. By abstaining from "good faith" regulatory action, I believe ISPs have failed to fulfill their end of the bargain. As a result, Section 230 has potentially contributed to a wide variety of issues, including the rise of misinformation, disinformation, and conspiracy theories online. In chapter 2, I analyze how Section 230 has allowed this kind of content to become an integral component of ISP business models.

Chapter 2: Section 230 and the Development of ISP's Business Models

Introduction

The impact of Section 230 on the development of the Internet and information service providers (ISPs) cannot be overstated. ISPs like Twitter, Facebook, Google, Yelp, and Wikipedia would not exist in their current form if not for Section 230. Without Section 230, these companies could be sued for distributing any third-party content. This chapter will analyze how Section 230 contributed to the rise of the Internet and Web 2.0 and influenced ISP business models. I explain the origins of the Internet, the fundamental differences between Web 1.0 and Web 2.0, and how Section 230 effectively allowed Web 2.0 to come into fruition. I will then answer the multidimensional question: Why do social media companies have no financial incentive to take down emotionally volatile and dishonest third-party content? Later, I examine the inherent characteristics of misinformation and discuss Hunt Allcott and Matthew Gentzkow's study about the role of misinformation in the social media company business model.

I then contrast old and new media formats and the laws that govern them by examining the history of newspapers. This section will highlight the difference in how newspapers moderate the content on their platforms compared to an ISP, like Twitter, and evaluate John Berryman's argument that the Internet and newspapers should have similar rights and restrictions. The chapter concludes with an overview of Twitter as a medium and how it has democratized information and utilized algorithms to radicalize consumers, consequently relegating them to a "feedback" loop (Anderson, 220). The current digital landscape would not exist in its current form without Section 230. As I will showcase, Section 230 has allowed the Internet to become the revolutionary, informational medium it is today. It has also enabled small and large tech companies to develop and continue to break down all kinds of societal barriers. On the other

hand, Section 230 has permitted social media companies to incorporate harmful content such as misinformation and disinformation into their business model for their own economic benefit.

Section 230 and The Rise of Web 2.0

It is crucial to comprehend the context of the Internet's creation to understand how the Internet has evolved into a virtually uncensorable medium. In 1969, the U.S. Department of Defense created the Advanced Research Projects Agency Network (ARPANET), the earliest form of what is referred to today as the Internet. The primary motivations behind the ARPANET were research and military-based (Abbate, 147). Creators Robert Taylor and Robert Lawrence wanted to build a research "network that would allow and encourage contractors to share software, data, and access to sophisticated computing machines, which were still scarce and expensive" (Abbate, 150). In this way, the ARPANET was an early blueprint for the Internet. It was a non-hierarchical, decentralized network, meaning it allowed many users to share and control the same computer service from different locations.

Not only was the ARPANET a financially superior alternative to costly telephone and radio networks, but it also provided the United States' military with a robust communication network at a time of great need: The Cold War. According to Kevin Featherly, the ARPANET came with unprecedented national security benefits because it was "a computer communications system without a central core, with no headquarters or base of operations that could be attacked and destroyed by enemies" (sec 1; par 2). As ARPANET developed, it added a new dynamic layer to national security, the likes of which the United States had never seen.

However, it was not until Tim Werner invented the World Wide Web in 1990 that the Internet began to be utilized by the general public and privatized by ISPs. The United States government officially terminated its ownership of the Internet, leaving it in the hands of “a set of

commercial, academic, government, and nonprofit networks in the United States and, increasingly, abroad" (Abbate, 176). The Internet's shift to private companies in the early 1990s marked the beginning of Web 1.0. Web 1.0 is characterized by its static nature, meaning that websites associated with this period did not possess interactive features such as the ability to comment or like a post. There was only one-way communication in the sense that Internet users could only passively receive content online. In other words, Internet users could not interact with other individuals on the web pages they viewed, nor could they generate their own content on the ISP.

As mentioned in chapter 1, a few ISPs dominated the Internet landscape in the early to mid-1990s: CompuServe Inc, Prodigy Services, and American Online. They were some of the first platforms to develop the characteristics that are associated with Web 2.0. According to Crispin Thurlow, Web 2.0 is identifiable by "the putative newness of content creators (as opposed to users); of content sharing and collaboration; and, of course, of social media such as social networking (e.g., Facebook) and microblogging (e.g., Twitter)" (229). Although they came developed in the 1990s, platforms like CompuServe Inc., Prodigy Services, and AOL would contemporarily be classified as Web 2.0 because of their innovative characteristics. These platforms allowed users to create and post user-generated content and interact with content posted by others. They were some of the first Internet companies to democratize information, allowing the people to play a role in the creation of content.

It is important to note that Section 230 was passed and upheld by the courts before the characteristics exhibited by CompuServe Inc., Prodigy Services, and AOL became popularized amongst ISPs. Before most ISPs adopted digital structures that allowed users to generate their own content and collaborate with one another. CompuServe Inc., Prodigy Services, and AOL

were also some of the first ISPs to adopt business models that utilized advertising to generate revenue. In this way, their business model was a precursor to today's social media giants like Facebook and Twitter. These companies also functioned as the guinea pigs of Internet regulation in the sense that they were the first ISPs of their kind. There was no official legislation governing interactive computer services besides the paradox created by the contradictory *Prodigy Services* and *CompuServe Inc.* precedents.

The *Prodigy Services* precedent established that if an ISP took any action to regulate third-party content, then it would be held legally liable for all the third-party content on its platform. In contrast, the *CompuServe Inc.* ruling affirmed that an ISP that made no effort to regulate its platform or enforce any kind of moderation practices would not be held liable for any of the third party-content on its forum. These contradictory verdicts created a massive conflict of interest for ISPs. Why would an ISP put itself in legal jeopardy and choose to regulate third-party content if doing so meant it would be held liable for all the third-party content on its platform and, as a result, likely sued out of existence?

Cox and Wyden's solution to this regulatory paradox was Section 230. They wanted ISPs to continue developing the medium's characteristics adopted by CompuServe Inc., Prodigy, and AOL that are now associated with Web 2.0. Prodigy Services, CompuServe Inc., and AOL were ahead of their time in the sense that they had already begun to allow users to generate third-party content, interact with one another, and form digital communities. Without Section 230, these ISPs would have been held liable to some degree for the third-party content on their platforms, limiting their ability to host this content and foster a sense of community on their forums. Ultimately, the attributes associated with Web 2.0 would most likely not have been able to

develop if it were not for Section 230, nor would they become an integral component of today's Internet and social media platforms.

Section 230: The Ultimate Equalizer

In Jeff Kosseff's book, "The Twenty-Six Words That Created the Internet," he provides an in-depth analysis of how Section 230 has benefited and influenced big tech companies and their business model. To illustrate this, he explains how Section 230 has contributed to Yelp's business model. Kosseff says, "Yelp's business model could not exist without Section 230" (130). He describes Yelp as a social networking website that allows consumers to write reviews of different business services (130). Consequently, Yelp has faced countless lawsuits citing damages brought on by critical user posts that have circulated on its platform. However, Section 230 shields Yelp from these types of lawsuits. As explained in chapter 1, Section 230 prohibits ISPs, in this case Yelp, from being considered the publisher/author of any third-party content posted on its platform. Unlike a newspaper, an ISP cannot be held accountable for content published on its medium because doing so would treat it as the "speaker or publisher" of such posts. Following Section 230, the only person who could be held legally liable for the defamatory content posted on Yelp is the author of the original comment.

Kosseff points out that it is difficult to imagine a world where Yelp would be able to operate under its existing business model if it were not for Section 230 (130). Yelp does not make money from requiring consumers to pay a fee to view or rate business transactions. Instead, Yelp generates an income through hosting local and brand advertisements. Therefore, Yelp needs a large consumer base to convince advertisers to buy ads on its platform. However, if Section 230 did not exist and Yelp were held legally liable for all the third-party content on its forum like a newspaper, then the company would have to regulate user-generated content to

some degree. Whether through instituting large-scale algorithms or employing vast amounts of personnel to conduct the tedious process of reviewing every single Yelp post, the company would have to take necessary precautions to avoid lawsuits.

Section 230's absence would also severely limit the free flow of information on Yelp, which is the company's primary selling point to consumers. If individuals could sue Yelp for distributing any content on its platform, the company would most likely opt to delete all reported third-party content. Doing so would limit the platform's ability to provide consumers with insight into transactional services and, undoubtedly, would inhibit the consumer experience. Yelp would become less valuable to consumers, and as a result, to advertisers as well. Ultimately, Kosseff provides strong evidence that Yelp would be unable to generate the same amount of revenue from advertisers or even exist in its current form without Section 230.

It is a common misconception that Section 230 solely benefits big technology companies. Cox and Wyden intended Section 230 to prohibit all ISPs, regardless of size, from being sued out of business for user-generated content. I believe it's not far-fetched to say that Section 230 was designed to benefit smaller, up-and-coming technology companies. The law gives smaller ISPs a fighting chance to compete with larger ISPs in the digital market. Without Section 230, smaller ISPs would have an extremely difficult time moderating all of the third-party content on their forums. Many of them simply would not have the personnel necessary to accomplish such a task.

Also, smaller ISPs would have an even more difficult time finding the resources to fight off third-party content lawsuits. According to Brent Skorup and Jennifer Huddleston, a complete repeal of Section 230 would have a detrimental impact on smaller technology companies (36). They say, "going from a blanket to a tailored shield . . . must account for the chilling effect it will have on innovation by startups and small firms, and for the artificial barrier to entry in the market

that will grant additional protection to incumbent firms" (36). In the event of a "tailored shield," smaller ISPs would be disproportionately impacted by Section 230's removal and their businesses would undoubtedly suffer.

Section 230's Impact on ISP's Business Models

When Cox and Wyden wrote Section 230, they did not foresee ISPs like Twitter, Facebook, and YouTube utilizing the immunity for all third-party content granted by Subsection (c)1 of Section 230 without engaging in the activities outlined by the "Good Samaritan" provisions in Subsection (c)2. This raises the question of why social media companies opt to take a hands-off regulatory approach to the third-party content on their platforms, even though such action is protected by Section 230. As a reminder, the "Good Samaritan" provisions grant ISPs the authority to take any "good faith" actions to regulate their platforms regardless of whether "such material is constitutionally protected." As long as ISPs moderate the content on their forums in "good faith," they cannot be sued by consumers for their regulatory decisions. To rephrase the initial question raised above, why do ISPs take the privilege of Section 230 immunity without fulfilling their responsibility to moderate content? The answer to this question lies in their business model.

As established in chapter 1, Cox and Wyden's intent when they wrote Section 230 was to incentivize ISPs to develop their own content moderation practices and have the capacity to take down any third-party content they deemed a violation of their community guidelines. At the time, Cox and Wyden did not know that the future business models of an ISP, like Google, would predominantly rely on advertising to generate revenue. According to Feingold et al., Google generates revenue from advertising in two ways (75). The first is when "search engines provide a service to users in exchange for their user data and who consent to see ads linked to

their queries" (Feingold et al., 75). The second is when "companies pay search engines to place the companies' advertisements on relevant web pages" (Feingold et al., 75). The former illustrates why it is against Google's and many other ISPs' economic interest to take down highly evocative, harmful third-party content that generates user engagement which provides them with valuable consumer information they can sell to advertisers.

Since Section 230 prevents ISPs from being held accountable for the harmful third-party content on their platforms, they may have no financial incentive to take it down. This potentially explains why Holocaust denial pages and election fraud conspiracy theories have run rampant on today's social media platforms. These kinds of posts garner substantial user engagement, which provides ISPs with user data they can sell to advertisers. Therefore, it is against an ISPs' best interest to take such content down if operating under a profit-maximizing business ideology. Ultimately, Section 230 has allowed for harmful content, such as misinformation and disinformation, to become a critical component of the ISP business model.

This potentially explains why large social media platforms have become a haven for evocative, dishonest content that manipulates consumers, distorts their perception of reality, and corrupts democracy. According to Daniel G. Krutka, "Algorithms will ultimately push out the misinformation far further than the fact-checking article that later debunks it. Facebook and other social media companies have few incentives to prioritize democracy" (116). Social media platforms are designed to create a free-flowing forum of information where users can post or seek out whatever content they desire with little resistance. Due to a lack of meaningful gatekeeping, misinformation and disinformation can spread at a pace on these platforms where the truth cannot keep up.

Many social media companies, like Facebook, have opted to utilize large-scale flagging systems to moderate third-party content. Flagging a post on social media is how consumers notify ISPs of third-party content they think is inappropriate. After a consumer flags a piece of third-party content, Facebook's software system hierarchically ranks it. Then, a team of Facebook moderators evaluates the flagged content, and a decision is made on whether to remove it. When a user flags a post, the software asks the user to categorize the third-party content they are flagging. Some examples of categories that Facebook's software lists are "hate speech" and "harmful behavior."

Tarleton Gillespie has criticized Facebook's large-scale flagging system. She argues these kinds of mass moderation systems that rely on user flagging are not an adequate methodology for regulating user-generated content (326). She says,

> "Discerning the fake from the genuine is not the same as identifying pornography or discouraging harassment, but because Facebook has responded with its existing moderation apparatus rather than developing new strategies for addressing fake news, future expectations, claims, tactics and disputes will be shaped by it" (Gillespie, 326).

Gillespie argues that the spread of misinformation and disinformation online presents a dilemma that social media companies' current regulatory practices are ill-equipped to address. The one-size-fits-all approach to content moderation will not sufficiently address the rise of misinformation on social media platforms. It is challenging enough for humans to distinguish between the real and the fake online, let alone large-scale digital software. By failing to take action and revise its current approach to third-party content moderation, Facebook has prioritized its current business model over the deterioration of the information ecosystem.

As Daniel G. Krutka pointed out, ISPs like Facebook have little incentive to change their approach to third-party content moderation because doing so would be against their financial interest. The role fake news plays in their business model is another reason why it is so difficult to stop its spread on social media platforms. According to Hunt Allcott and Matthew Gentzkow's study, fake "news articles that go viral on social media can draw significant advertising revenue when users click to the original site" (217). In other words, fake news garners exactly what the ISP business model desires: user engagement. User engagement translates to personal information that social media companies can sell to advertisers. Ultimately, the engagement that fake news stimulates is directly correlated with the desired outcome of the ISP business model.

Further complicating the spread of fake news on social media is human nature. According to Kyle Anderson, "the human mind is not only ill-equipped to discern truth, it is also, in some ways, designed to avoid truth," which "presents unique technological advantages in the spreading of misinformation" (212). Utilizing algorithms, social media companies can personalize content to fit into consumers' pre-existing ideologies and beliefs. These algorithms are designed to maximize clicks and likes and simultaneously reinforce user beliefs. Anderson notes algorithms can create a "feedback loop" because they only expose consumers to information consistent with their pre-existing views (220). As a result, they are more likely to fall victim to false information (Anderson, 220). Content catered to a user's understanding of the world makes it extremely difficult to be skeptical of online information. Ultimately, social media algorithms exploit human nature and have the propensity to create a never-ending cycle. They can exacerbate and eventually radicalize user beliefs, even relegating them to an alternative reality where they cannot discern fact from fiction.

Section 230 is partially to blame because it has enabled these platforms to become a breeding ground for misinformation, with algorithms actively spreading false content to users. It does not help that human nature makes it extremely difficult for consumers to differentiate dishonest from truthful content. If Section 230 did not provide ISPs with immunity for all user-generated content, including the content they know to be harmful, false, or even illegal, they would have to crack down on the spread of misinformation, disinformation, and conspiracy theories.

In sharp contrast to the Internet and ISPs, newspapers are legally liable for all content published on their forums. As a result, they have to rigorously fact-check and moderate the information they distribute to the public. The upcoming section will explore the history of newspapers, the laws that govern them, and John Berryman's argument that the Internet and ISPs should have similar rights and restrictions on the content they distribute.

The History of Newspapers

When evaluating the degree to which the Internet should be regulated, it is vital to consider how the Internet medium compares to other existing media formats and how they have been and continue to be regulated. When newspapers rose to prominence in Britain, they were considered an enemy of the state because they provided a forum for "revolutionary politics . . . that left even the highest officials soiled and sullied" (Foerstel, 1). As a result, they were heavily censored by the British government. In accordance with the English common law of the time, newspaper publishers actively ran the risk of being charged with "seditious libel," a crime for publishing criticism of a public official that the Crown utilized to suppress speech (Foerstel, 2). Upon the inception of the British colonies in America, the newly established judiciary had to determine whether the "seditious libel" common law would apply to the colonies.

In *Crown v. Zenger,* the courts made this determination. A journalist named John Peter Zenger published critical information about William Cosby, then colonial governor of New York, in the *New York Weekly Journal.* Consequently, he was indicted for libel. However, instead of following the British law of the time and convicting Zenger for libel, the jurors famously ruled that "the truth cannot be libelous," "setting an informal legal precedent and influencing the form of press freedom eventually embodied in the new nation's constitution" (Foerstel, 3). The *Zenger* case set the precedent that newspapers cannot be sued for truthful content, regardless of whether the printed material was critical of the government. The ruling has allowed newspapers and other journalistic sources to speak truth to power without fear of retaliation. They could no longer face potential libel charges for factually accurate content. *Crown* v. *Zenger* opened the floodgates for what could be published in newspapers and provided the foundation for today's free press.

Jerry Berman, the founder and president of the Internet Education Foundation, argued in 1997 that the closest medium to the Internet is newspapers, and that they should have comparable rights and restrictions (Foerstel, 195). He said,

> "The Internet's First Amendment can also be best compared with that of newspapers. The Supreme Court saw it that way. We argued in court that the Internet is not a scarce medium like radio or television, and it's not a one to one communication system like the telephone. It is a one-to-many and many-to-many medium" (Foerstel, 195).

Foerstel asserted that because the Internet and newspaper mediums are intrinsically alike and communicate information to the public in a similar one-to-many and many-to-many manner, they should have the same rights and restrictions and be held accountable for the content

distributed on their mediums. Although Berman's analysis may be slightly outdated, I believe there is still some merit to his argument, but for slightly different reasons.

It is undeniable that newspapers and the Internet have the propensity to shape public opinion because of their shared roles in distributing information to the public. According to a Pew Research Center poll conducted on January 12, 2021, "About half of Americans get news on social media at least sometimes" (sec 1; par 1). Despite the growing number of individuals that get their news from social media websites, there is a stark contrast in the number of restrictions and the level of responsibility newspapers and social media websites face regarding the content published on their forums. In contrast to ISPs and technology companies, newspapers and digitized newspapers can be sued for the content published on their forums, even in their comments' sections. In other words, they are always treated as "the publisher or speaker of third-party content" on their forum and, consequently, can be sued for libel. As a result, they employ rigorous fact-checking and screening processes for the content they publish because, as the *Crown v. Zenger case e*stablished, the truth is their only defense.

Although newspapers cannot be sued for truthful content, their ability to fully exercise their First Amendment rights is still limited by government regulation under a few distinct scenarios. Over time, the Supreme Court has developed tests for prior restraint that outline when the government can legally suspend the press's First Amendment rights, such as the Miller obscenity test and the imminent lawless action test. The fact that there are prior restraint tests to allow the government to legally abridge newspapers' First Amendment rights reveals that their First Amendment rights are not absolute. So, why is there an absence of these kinds of prior restraint tests for the Internet?

As discussed in chapter 1, Internet exceptionalism is a widely shared belief that the Internet's benefits and unique qualities exempt it from outside regulation. Internet exceptionalism explains why the government and current laws do not have the same restrictive effect on the Internet and ISPs as they do for newspapers, despite their shared role in distributing information to the public and shaping public opinion. Internet exceptionalism is at the core of not only Section 230, but also the difference between how the Internet and more traditional formats like newspapers are regulated. To demonstrate this disparity, I examine the difference in how the government approaches First Amendment rights on the Internet versus other media formats when there is a threat to national security. According to Ojan Aryanfard, "Periodically, the Supreme Court has examined whether the government can restrict speech to further the compelling interests of national security. In doing so, the Court has recognized that national security as a governmental interest does justify restrictions on First Amendment rights" (sec 4; par 1).

In *Near v. Minnesota*, the Supreme Court recognized newspapers could be subject to prior restraint by the government if they are going to publish information that jeopardizes national security (U.S. Supreme Court, 716). This begs the question, should the government develop a specific policy that outlines a scenario or a test where it or an independent organization can restrict the content published on the Internet or on an ISP if it jeopardizes national security? For example, it has been widely documented that Russian bots spread misinformation on social media during the 2016 presidential election in an attempt to influence the outcome and “strengthen their authority” (Yerlíkaya, 182). Is this kind of activity a significant enough threat to national security that the U.S. government or an independent actor should be able to influence the information available on a platform like Facebook? Should there be a new kind of test to evaluate the third-party content on online platforms to prevent individuals from becoming

radicalized? Has Internet exceptionalism gone too far? It is crucial to ask these questions because, despite their similar roles in distributing information to the public and shaping public opinion, the Internet and ISPs are held to a much less rigorous regulatory standard than newspapers.

After reflecting on the similarities between the Internet and newspaper mediums, I believe there is some merit to John Berryman's argument. While the First Amendment certainly guarantees the right to free speech, it does not guarantee the right to be a publisher on a private platform. Nowhere in the Constitution or Bill of Rights does it state that citizens have the right to be published in the *New York Times* or the right to publish a "tweet" on Twitter. I believe ISPs have to take more accountability for the content published on their platforms, given their ability to shape public opinion. Although granting ISPs the exact same rights and restrictions as newspapers is far from a perfect solution, it could provide an outline for the degree to which ISPs should be held accountable for the content they distribute and how they could regulate their platforms.

One ISP that recently adopted a more decisive approach to slowing the spread of dishonest content on its platform is Twitter. The upcoming section will give an overview of Twitter, describe how the company has contributed to the spread of misinformation, and outline its recent efforts to combat dishonest content online.

An Overview of Twitter and Its Business Model

Twitter has revolutionized the way in which members of society communicate with one another. The platform allows everyone from the president of the United States to an average person to share their thoughts and feelings about virtually anything immediately. Twitter is an interactive social media platform in which users create a personal profile, microblog their

thoughts, and instantaneously belong to a virtual community. Twitter enables users to follow other user-profiles and see when they like, “tweet,” or “retweet” a “tweet.” “Tweets” are messages that can be up to 280 characters long that contain information, thoughts, and ideas of the poster. Once a user publishes a “tweet,” it shows up on their profile and the Twitter feed of any users that follow the account from which the tweet originated.

A Twitter feed is a stream of content that shows the activity of the accounts a user follows. A “retweet” is when someone republishes the original “tweet” of another user, thus causing it to show up on their profile and also the Twitter feed of users that follow the person who “retweeted.” All of the content that shows up on user feeds retains the same formatting, regardless of any differences in content. The extremely minimalistic design of a tweet makes them seem universally legitimate.

All “tweets,” regardless of who they are from or what they are about, must be 280 characters or less. They also all retain the same format, with the author’s Twitter handle located at the top tweet. A Twitter handle is a personalized username that begins with the @ icon. It helps other users identify the author of the tweet. Below the Twitter handle is the substantive message from the author. Under each “tweet’s” message, users can view the date and time of the post, along with any comments, as well as the number of likes and retweets from other Twitter users. When scrolling through one’s Twitter feed, there is no visual distinction between a “tweet” about what someone ate for breakfast versus a radical QAnon conspiracy theory. Both “tweets,” despite their extreme contrast in subject matter, retain the same structure and format.

The uniformity of every "tweet" suggests that they all have the same value regarding their credibility and truthfulness. There is little to differentiate between a "tweet" from a credible news outlet, such as the *Wall Street Journal,* to one from *Newsmax,* an alt right, conservative news

network that recently faced criticism for amplifying widespread voter fraud conspiracy theories in the aftermath of the 2020 presidential election. As a result, *Newsmax* has been rated a "questionable" source by numerous independent fact-checking organizations such *Media Bias Fact Check LLC* because of its "promotion of conspiracy theories and pseudoscience as well as numerous failed fact checks" (sec 1; par 1). Until recently, there was little on Twitter to visually distinguish an everyday post about someone's life, from a post from an accredited journalist institution, or radical conspiracy theory with no basis in reality.

Twitter's business model, like many other ISPs, depends on user-generated content and advertising. As discussed earlier, social media companies utilize algorithms that expose users to content that fits their preexisting political ideology. The content on Twitter is "specifically targeted to users based on their political proclivities (i.e., what items they "like," which sites they visit, and whom they're "friends" with)" (Ott 65). In other words, the content that shows up on a user's Twitter feed has been tailored to their preferences, which can, as Anderson described, relegate them to a "feedback loop" that can cause radicalization (220).

For the reasons outlined above, Twitter has become one of the leading proponents of the misinformation crisis and the extremely polarized political climate. The company has created an environment where Americans are radicalized through isolated exposure. In his article, "The age of Twitter: Donald J. Trump and the politics of debasement," Brian Ott investigates how President Trump's Twitter account has created a post-truth, digital environment, as well as fostered mass "incivility" online (62). Ott describes "incivility" as "speech that is impolite, insulting, or otherwise offensive" (62). He points to the informal nature of Twitter and how there is a de-emphasis on syntax and grammar, as well as a disconnect between the words of a user and their impact on someone else (62). Regarding the former, Twitter devalues well-written

speech due to the forum's informal nature, which results in harsh wording that would otherwise not occur in a more formal setting. The latter refers to how Twitter creates an environment where users don't have to face the individual they attack and, consequently, do not appreciate the emotional toll of their words.

Upon reflecting on his case study, Brian Ott said, “I can think of no better word than ‘contagion’ to describe the toxic effect that Twitter, as a mode of communication, and Trump, as a model of that mode, have had on public discourse” (64). In response to President Trump using his Twitter to promote conspiracy theories about the coronavirus and early voting in 2020, Twitter flagged some of his tweets as “disputed” and “misleading.” President Trump was outraged by Twitter’s moderating practices but could not sue the company because of the “Good Samaritan” provisions of Section 230. In this case, Twitter was acting in “good faith” when the company flagged Trump’s content and described it as “disputed” and “misleading.” As outlined by the “Good Samaritan” provisions, such actions are protected, meaning a user cannot sue an ISP for editing, restricting, or even outright censoring any third-party content that it deems to be “objectionable.” Therefore, President Trump could not sue Twitter for flagging his tweets and later deleting his account.

In response to more labeling of his tweets, President Trump tweeted on Oct. 6, 2020, “REPEAL SECTION 230!!!” While President Trump did not explain which part of Section 230 he wanted repealed, it is fair to assume he was not referring to the Subsection (c1) of Section 230 that protects ISPs from all legal liability of the third-party content on their forum. Instead, he was most likely referencing the “Good Samaritan” provisions that allow ISPs to take any “good faith” action to regulate their platform.

Conclusion

Ultimately, Section 230 is at the core of the structure and business models of today's ISPs. Without Section 230, ISPs could have the same First Amendment rights and restrictions as newspapers, meaning they would face greater accountability for all the third-party content distributed on their mediums. More than likely, Web 2.0 would not have developed in the same way, and most of today's ISPs, like Yelp, Facebook, and Twitter, would not exist in their current forms. These companies would not be able to rely on their current business model that depends on user-generated content and advertisers to generate revenue.

On the flip side, Section 230 has allowed for dishonest content to become an inherent part of ISP's platforms. Utilizing algorithms, ISPs like Twitter and Facebook have indoctrinated consumers with falsehoods and distorted their perception of reality. Until recently, most ISPs were able to do this with little public scrutiny. However, due to public outrage, Twitter was one of the first platforms to institute fact-checking on the third-party content posted by President Trump's account. Twitter was able to take such action because of Subsection (c)2 of Section 230, also known as the "Good Samaritan" provisions. Chapter 3 will further discuss the "Good Samaritan" provisions of Section 230 and how Section 230 potentially led to the misinformation crisis and the proliferation of conspiracy theories online.

Chapter 3: The Proliferation of Misinformation, Disinformation, and Conspiracy Theories Online

Introduction

Since Section 230 eliminates all liability for third-party content, it has enabled ISPs to ignore and encourage the spread of misinformation on their platforms. As mentioned in chapters 1 and 2, Subsection (c)2 of Section 230, also known as the "Good Samaritan" provisions, rectified the troubling *CompuServe Inc.* and *Prodigy Services* precedents. These rulings encouraged ISPs not to regulate any third-party content on their forums to avoid liability. According to Cecilia Ziniti, "Even the staunchest § 230 critics accept that in passing § 230, Congress sought to reverse this result and aimed to encourage interactive service providers to implement voluntary self-policing" (597).

The "Good Samaritan" provisions put Internet regulation responsibility solely on the ISPs instead of the government or another independent organization. Therefore, Cox and Wyden gave ISPs a privilege that allowed them not to be held accountable for any of the third-party content on their platforms. Doing so encouraged economic growth and granted ISPs the freedom to take "good faith" regulatory actions. This chapter will demonstrate how many ISPs have failed to fulfill their end of the bargain and, in doing so, created a misinformation crisis.

They have taken the privilege of Section 230 immunity for all the third-party content on their platforms without engaging in any of the actions outlined in Section 230's "Good Samaritan" provisions. ISPs like Facebook, YouTube, and Reddit have not only permitted but encouraged the proliferation of harmful third-party content for their economic benefit. The world is in the midst of a misinformation crisis, where consumers daily struggle to differentiate between fact and fiction online has had potentially devastating effects on the public and political

spheres. There is strong circumstantial evidence that misinformation regarding widespread election fraud may have radicalized members of the extreme right and incited violence during the insurrection on the Capitol on Jan. 6.

In this chapter, I give a broad overview of the current misinformation crisis and how Section 230 has contributed to it. I also provide insight into the different types of false information, why dishonest content is hardest to combat online, and how digital platforms can create a hyperreality. I conduct an in-depth analysis of two conspiracy theories to demonstrate their pervasive impact: the 'birther' conspiracy theory and 2020 election fraud misinformation campaigns. Additionally, I examine how the removal of former President Donald Trump's social media accounts potentially affected the amount of misinformation and disinformation on social media platforms and the public's acceptance of this content. It is worth noting that ISPs were able to take such regulatory action without being sued by President Trump because of the "Good Samaritan" provisions of Section 230. I make the case that Cox and Wyden intended for Section 230 to allow social media companies to engage in these kinds of regulatory practices routinely. Ultimately, the impact of Section 230 on today's digital media platforms has come with incredible communal and informational benefits and a new set of problems that run the risk of evolving into dire consequences.

The Misinformation Crisis: Differentiating False Information

The need to differentiate the different kinds of malignant content polluting the body of information online is essential to understand the unique challenges false information poses to consumers. According to Claire Wardle and Hossein Derakhshan, there are three types of false information: misinformation, disinformation, and malinformation (Wardle and Derakhshan, 71). They define misinformation as “false information shared by someone who believes it to be true”

(Wardle and Derakhshan, 71). Misinformation broadly encompasses unintentional mistakes made by an author or distributor. These mistakes can range from inaccurate dates to a misinterpretation of data to reposting a fraudulent article. When misinformation spreads, the author or distributor has no intention to deceive and does not want to cause harm. Some examples of misinformation are when journalists accidentally publish an article with illegitimate testimony from eye-witnesses or when consumers share news articles they genuinely believe to be factual.

In contrast, disinformation is "false information shared with knowledge of its falsity and thus intention to deceive or otherwise do harm" (Wardle and Derakhshan, 71). Unlike misinformation, disinformation is a conscious lie intended to mislead. Disinformation can take many forms, such as deep fakes or deliberately created conspiracy theories. For example, Russia utilized Facebook's "tools for microtargeting and advertisement distribution" to spread disinformation during the 2016 presidential election (Guilbeault, 36). Despite the malintent behind it, disinformation can be challenging for consumers to distinguish because it is often strategically made to resemble accredited information.

Lastly, malinformation refers to "instances where private information is made public or genuine imagery is reshared in the wrong context" (Wardle and Derakhshan, 71). Unlike disinformation, malinformation is based on reality and is not entirely false. However, like disinformation, it is generally used to inflict harm on another entity, whether it be a person, organization, or country. An example of malinformation is revenge porn. Revenge porn is when another party distributes sexually explicit content from another person without their consent. Revenge porn meets the criteria of malinformation because it is authentic, "private" content that is released to damage the reputation of an individual and has been taken out of its original

context. Another example of malinformation was when Wikileaks released 30,000 emails from Hillary Clinton's "private" email server. This meets the criteria of malinformation because the content was authentic, but also "private" and released without the full context to harm Hillary Clinton's reputation.

Many of the people who create, share, and repost false content on social media do so not with the intent to harm but because they cannot differentiate between dishonest information and the truth. While some actors purposely publish and distribute false information, many consumers who disseminate disinformation do so believing the content is credible, which is why I refer to the current poisoning of the information ecosystem as the misinformation crisis. People who repost a fraudulent story often do so unknowingly and without malice, which under Wardle and Derakhshan's methodology, would classify as misinformation instead of disinformation or malinformation. An example that illustrates this occurred during the 2016 presidential election, where one of the top misinformation stories shared on Facebook falsely claimed that Pope Francis had endorsed then Republican presidential nominee, Donald Trump (Lee, sec 1; par 2). Many of the users that reposted the story did so without knowing it was false, thus classifying the action as the spread of misinformation.

Further complicating the spread of false content online is that "on social media, anybody can become a 'journalist' and, anything can become 'news'" (Bialy, 74). To the detriment of the information ecosystem, everyday consumers have taken on the role of citizen journalists through either publishing or distributing content without abiding by the standard ethical and verification protocol. The evolution of the digital terrain has opened up a new realm of possibilities for anyone to become a citizen journalist and take on the all-important "watchdog" role previously occupied solely by the mainstream press (Gordon-Murnane, 120). The problem with citizen

journalism taking on a “watchdog” role is that the content posted by citizen journalists frequently doesn’t go through the same rigorous fact-checking process as content from more traditional media outlets. This has made it possible for non-objective citizen journalists to publish content filled with exaggerations and falsehoods.

The speed with which dishonest content can spread online is unprecedented to any other medium. Beata Bialy finds "[o]ne of the most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency and availability 24/7" (82). These elements make it incredibly difficult for the mainstream media to fact-check the content that spreads on these platforms in real-time to combat their spread. Also, fact-checking by the mainstream media has proven to be highly unsuccessful at debunking misinformation online for two primary reasons. The first is that many Americans do not trust the "mainstream media," as demonstrated by a recent Gallup poll, highlighting that "Six in 10 Americans have "not very much" trust (27%) or "none at all" (33%)." (Brenan, par 1; sec 1). In other words, a fact-check by an established news outlet like *The New York Times* or *The Wall Street Journal* does not carry any weight if the audience believes that the media outlet is not credible.

The second main problem with fact-checking is that it often amplifies the original lie. Mark Andrejevic notes debunking a false claim actually “reproduces its own conditions of possibility,…” allowing the claim to reach more people and intensifying the toll of the original misinformation (Andrejevic, 21). The dilemma might explain why it is so challenging for credible, journalistic entities to combat the spread of viral misinformation online and highlights how ISPs and social media platforms can corrupt the public’s perception of the real world and create a hyperreality.

A hyperreality is a realm “where the divide between media and reality implodes, and what goes for “reality” becomes a media product or a simulation of reality, which is impossible to discern from the real thing” (Hendrick and Vestergaard, 36). When credible media resources cannot fulfill their duty as “the watchdog,” misinformation, disinformation, and malinformation can relegate consumers to a hyperreality. Under this condition, media users may no longer be able to discern fact from fiction and, consequently, cannot make rational decisions because they have been overwhelmed with lies.

One notable example of this kind of behavior is Kellyanne Conway's defense of President Trump's false claim that his inauguration crowd was exponentially larger than President Obama's. Conway suggested that Trump was referring to "alternative facts" (NBC Universal, 02:01-04). As Vincent F. Hendricks and Mads Vestergaard point out, there is no such thing as "alternative facts" (52). They say, "Statements regarding factual matters are either true or false. An alternative claim denying a true statement is simply a false one. You may, of course, disagree that these *are* the facts*;* but disagreeing *with* facts is to disagree with reality" (52). The intentional spread of disinformation, or as Conway referred to it, "alternative facts," jeopardizes journalistic truth, intentionally manipulates the public, and can distort one's view of the world.

Conspiracy Theories

Social media platforms have become home to divisive conspiracy theories that are often politically motivated and designed to undermine public trust in the government and its officials. According to the News Literacy Project, “a conspiracy theory is an unfounded explanation of an event or situation that blames the secretive work of sinister, powerful people or organizations such as the government, a company, or even one influential personality” (News Literacy Project; Video 2; 00.28-38).

Conspiracy theories appeal to people for several reasons. For starters, they are straightforward, comprehensible narratives that make sense of complex phenomena that are difficult to understand. For example, the widely circulated conspiracy theory that COVID-19 was manufactured in a Chinese laboratory is easier for some to comprehend than its true origin. Conspiracy theories also reinforce the "us versus them" mentality. The News Literacy Project reports, "Believers identify as 'us' and 'we'. While non-believers are referred to as 'they' and 'them'" (News Literacy Project; Video 4; 00:50-56). This kind of thinking further isolates conspiracy theory believers and causes them to fall further away from reality. As Robin Thompson describes, "Users may one day find themselves down the proverbial radical rabbit hole, unsure of how they ended up there; or they may very well have chosen the radical path, knowing full well where it led" (168).

A large reason conspiracy theories have gained traction in the 21st century is because the Internet and social media platforms amplify and spread them. Social media platforms like YouTube, Reddit, and Facebook have actively turned a blind eye to conspiracy theories circulating on their platforms because they generate clicks and likes due to their highly evocative nature (Allcott and Gentzkow, 217). For example, the conspiracy theory that alleged the Chinese government concocted the coronavirus in a laboratory in Wuhan gained massive attention online. So much so that *The New York Times* reported that more than 33% of Americans "believe that the Chinese government engineered the coronavirus as a weapon" (Carey, sec 1; par 1).

Recognition that conspiracy theories can result in more than just the corruption of public opinion is crucial. As demonstrated by the 2020 presidential election fraud conspiracy theory, which I will discuss later in this chapter, conspiracy theories can result in serious violence and even fatalities. Ultimately, the proliferation of conspiracy theories and misinformation on digital

media poses a potentially devastating threat to modern democracy. There is no better place to start than the ‘birther’ conspiracy theory about President Barack Obama and the role Twitter played in its spread.

The ‘Birtherism’ Conspiracy Theory

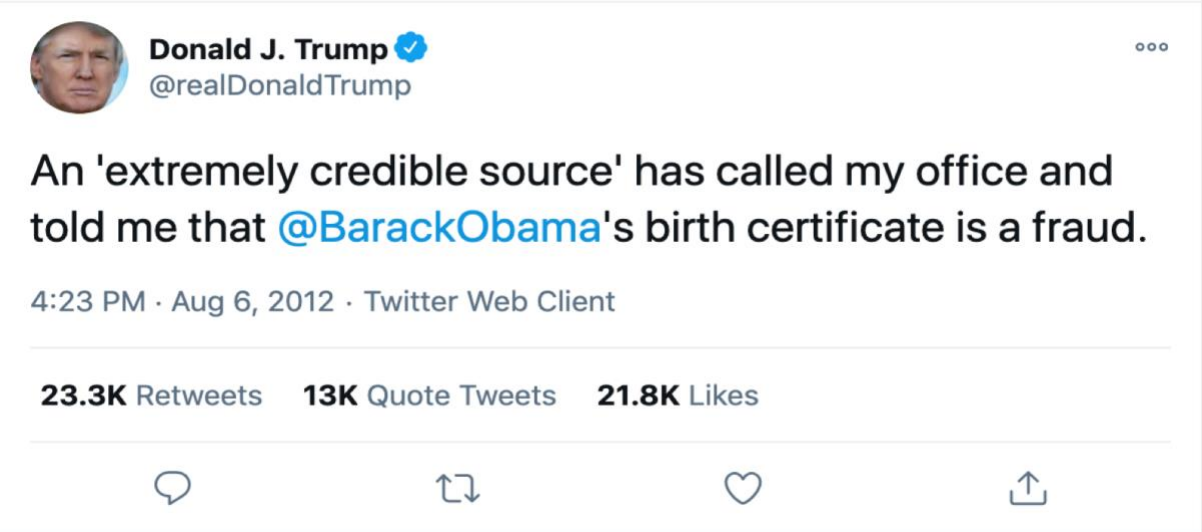
The 'birtherism' conspiracy theory refers to the widely debunked claim that the first African American President, Barack Obama, was a Muslim and not born in the United States. According to the criteria set out by the News Literacy Project, this would classify as a conspiracy theory because it was an "unfounded explanation" to an event that made sense of a complex phenomenon that was difficult for many individuals to understand. In this case, the complex phenomenon was the election of the first African American president, President Obama. Many individuals could not come to terms with the fact that the American people had elected a Black man as the next president of the United States. Conspiracy theorists developed the "unfounded explanation" that President Obama was not born in the United States and that there was a mass cover-up by the Democratic Party and other organizations to get him elected.

The origins of the ‘birther’ conspiracy theory continue to be debated in political and public spheres. Investigative journalists have reported that the beginnings of ‘birtherism’ can be traced back to August 2004, when Andy Martin, a Republican politician from Illinois, claimed, “Obama is a Muslim who has concealed his religion” (Rutenberg, sec 1; par 1). Some politicians, such as President Trump and Senator Ted Cruz, have falsely asserted that Hillary Clinton and her campaign were the creators of the ‘birther’ conspiracy theory. This incorrect assertion traces back to a leaked strategy memo from Mark Penn, an advisor to Hillary Clinton’s campaign. “Numerous fact checks, reports, and interviews . . . revealed although some Clinton supporters

circulated rumors about Obama's citizenship, the campaign and Clinton herself never trafficked in it" (Cheney, sec 1; par 2).

Despite a complete lack of evidence, the 'birtherism' conspiracy theory corrupted the public's opinion of President Obama. In response to the conspiracy theory's growing popularity, President Obama released a photocopy of his short-form birth certificate that verified his birth in Honolulu, Hawaii, on August 4th, 1961. In spite of this, a great deal of skepticism surrounding President Obama's citizenship persisted in the public sphere. The 'birther' conspiracy theory soon evolved into the 'birther' movement because such a large segment of the American population believed that President Obama was not born in the United States. A huge reason behind the 'birtherism' conspiracy theory gaining so much traction was due to Trump's Twitter activity.

Trump became one of the faces of the 'birther' movement when he used his Twitter to amplify the conspiracy theory 67 times (Struyk, sec 1; par 1). He reportedly did so to "appeal to the large segment of Republican voters who were upset about the presence of a Black man in the White House" (Abramowitz, 123). Trump's Twitter activity caused the 'birther' movement to become a legitimate news story, reach new heights of popularity, and manipulate the public's perception of President Obama. Despite President Trump admitting that President Obama was born in the United States in a press conference on September 16th, 2016, a poll conducted by *Morning Consult* a week later found that *only* 62 percent of Americans believed Obama was born in the U.S (2). The digital screenshot below is one of Trump's 67 tweets that potentially influenced the remaining 38% of Americans to believe the 'birther' conspiracy theory and mistakenly question President Obama's religion, citizenship, and ultimately the legitimacy of his presidency.



On August 6th, 2012, at 4:23 pm, Trump tweeted, "An 'extremely credible source' has called my office and told me that @BarackObama's birth certificate is a fraud." In his tweet, Trump utilized several rhetorical strategies to assert his credibility, captivate his Twitter audience, and evoke an emotional response. According to Kathryn L. Carew and Stephanie Kelley-Romano, Trump has a history of being a "conspiracy theory advocate" and "paranoid spokesperson" (38). In the tweet, Trump took on the role of a "conspiracy theory advocate" because of how he claimed to have access to insider information that no one else was privy to (Carew and Kelley-Romano, 38). Trump alleged he obtained knowledge from a "credible source," despite not naming the "credible source" or offering any information as to why they were reliable. Per the "conspiracy theory advocate" criteria outlined by Carew and Kelley-Romano, Trump also made it seem like he was working on behalf of the American people to expose the truth about President Obama's origins for the public good (38-39).

Carew and Kelley-Romano also discuss how Trump took on the role of the “paranoid spokesperson” in the ‘birtherism’ movement (39). They say, “Trump constructed himself as essential to exposing the conspiracy, as the hero within a larger struggle for justice and truth” (40). In the tweet, Trump claims that “experts” have reached out to him, recognizing his status

as a critical voice of the ‘birther’ movement. In this way, the tweet affirmed Trump’s authority and gave him credibility in the eyes of the Twitter audience because it made him out to be “the hero within a larger struggle.” Given the characteristics of Twitter as a free-flowing forum of information with little gatekeeping, Trump could control the ‘birtherism’ narrative. He could post whatever content he desired without being undermined by Twitter’s moderators or the mainstream media. The tweet is a prime example of how Trump utilized rhetorical strategies to captivate his Twitter audience and made Americans believe the fundamentally racist ‘birther’ conspiracy theory.

But how does Section 230 fit into all of this? Twitter failed to remove, edit, or flag a single one of Trump’s 67 tweets that promoted the ‘birther’ conspiracy theory. The platform was able to turn a blind eye to Trump’s activity because of Subsection (c)1 of Section 230 that grants ISPs immunity for all third-party content and allows Twitter to disseminate harmful material it knows to be false. As discussed in chapter 2, it did so because the ‘birtherism’ conspiracy theory benefited the company’s business model because it generated user activity, which translated to higher revenue from advertising. Trump’s use of Twitter to promote the ‘birtherism’ conspiracy theory is a classic example of Section 230 failing to do what Cox and Wyden intended. Instead of motivating Twitter to engage in the activities outlined in the “Good Samaritan” provisions, Section 230 permitted Twitter to ignore Trump’s efforts to mislead the American public. The following section will focus on how President Trump similarly used Twitter to promote the voter fraud conspiracy theory during the 2020 presidential election and contrast how Twitter utilized Section 230 to handle this situation.

President Trump's Call to Remove Section 230

On May 26th, 2020, Twitter, for the first time, added disclaimers to one of President Trump's tweets that claimed mail-in voting would lead to mass voter fraud and a "Rigged Election." The disclaimers read "Potentially misleading information about voting processes" and "Get the facts about mail-in ballots" and linked to several articles from accredited journalistic outlets that thoroughly debunked President Trump's claims (Silverstein, sec 1; par 4). Undoubtedly, President Trump was outraged, but because of the "Good Samaritan" provisions of Section 230, he could not sue Twitter for their regulatory efforts. As a reminder, the "Good Samaritan" provisions of Section 230 state,

> "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 provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

In this case, Twitter's addition of disclaimers to President Trump's tweet was the "action voluntarily taken in good faith." President Trump could not claim that Twitter violated his right to free speech because the "Good Samaritan" provisions explicitly state that it does not matter whether the restricted material is "constitutionally protected." Per the "Good Samaritan" provisions, as long as the ISP completed their moderation practices in "good faith," it could not be held liable for said practices. Therefore, Section 230 prohibited President Trump from suing Twitter for adding disclaimers to his tweet.

On May 29th, 2020, at 11:15 am, President Trump tweeted, "Revoke Section 230." This would be the first of many tweets from President Trump to call for Section 230's removal. As

discussed at the end of chapter 2, it is fair to infer that President Trump was not referring to Subsection (c)1 of Section 230 that gives ISPs immunity for all the third-party content on their platforms. Instead, he was referring to the "Good Samaritan" provisions that basically grant ISPs the authority to regulate their forums however they see fit. Due to President Trump's tweets about Section 230, the law garnered extreme amounts of media attention. Section 230, the law that was initially a late addition to the Telecommunications Act of 1996, took center stage and became what everyone was talking about. In the upcoming section, I examine the 2020 election fraud conspiracy theory and how it gained traction on social media platforms.

The 2020 Election Fraud Conspiracy Theory

The election fraud conspiracy theory fulfills the News Literacy Project's definition of a conspiracy theory because it was an "unfounded explanation" to an event that many did not understand. When most Americans went to bed on November 2nd, President Trump had a lead in many battleground states like Michigan, Wisconsin, Pennsylvania, and Georgia. Over the next week, states continued to count mail-in ballots, resulting in Joe Biden's vote tally surpassing President Trump's in these states. Consequently, Joe Biden was the winner of the Electoral College, and projected to be the next president of the United States. The election fraud conspiracy theory further meets the News Literacy Project's definition of a conspiracy theory because it claimed the unexpected event's result was a cover-up made possible by "powerful people or organizations" like Hugo Chávez and the Democratic Party.

In response to Joe Biden's election as the 46th president of the United States, the election fraud conspiracy theory proliferated on social media. Many users falsely contended the election was stolen and that President Trump had actually been re-elected. As previously demonstrated, President Trump was also able to spread these falsehoods on his social media accounts, even

though many ISPs like Twitter and Facebook continued to actively flag his posts with disclaimers. Despite their efforts, social media platforms like Instagram, Facebook, and Reddit became home to radicalized individuals who genuinely believed President Trump won the election. These individuals organized on these platforms and spread the #StoptheSteal movement, an effort to overturn the results of the presidential election that resulted in the storming of the United States Capitol on January 6, 2021.

In the wake of the riot that forced members of Congress to take emergency shelter during the reporting of the Electoral College votes, the United States House of Representatives voted to impeach President Trump for inciting the insurrection where five people died and 140 police officers were injured (Jackman, sec 1; par 1). During the Senate's impeachment trial, impeachment manager, Stacey Plaskett, emphasized surveillance footage that revealed "rioters were within 100 feet of where the vice president was sheltering with his family" (Sprunt and Lucas, sec 1; par 8). This goes to show that the outcome of the Capitol insurrection could have been much worse.

Ultimately, conspiracy theories have had a devastating impact on the information ecosystem, democracy, and the public good. In contrast to the 'birtherism' movement, the election fraud conspiracy theory resulted in real violence and even deaths. This is not to belittle the impact of the 'birtherism' movement. Instead, it is to showcase that conspiracy theories can have a wide array of consequences. They have the propensity not only to distort one's perception of reality, but also to radicalize people and incite violence. Social media companies and other ISPs must engage in the activities outlined by the "Good Samaritan" provisions of Section 230 regarding this content. As demonstrated by the election fraud conspiracy theory, neglecting to do so has proven to be a matter of life and death.

But how should ISPs go about regulating their platforms? Does the removal of social media accounts that actively spread misinformation and disinformation impact the degree to which this content persists on these forums? And would regulatory action affect the public's acceptance of misinformation and disinformation?

The Potential Impact of President Trump's Removal from Social Media

The upcoming section will attempt to answer these questions by examining the potential effect of removing President Trump's social media accounts on the amount of misinformation and disinformation online and the percentage of the public that perceived such content to be true before and after his removal. In other words, the independent variable is the removal of President Trump's social media accounts. The dependent variables are the amount of misinformation and disinformation on these platforms and the degree to which the public accepted misinformation and disinformation before and after the removal of President Trump's accounts.

Two days after the Capitol insurrection, many social media giants like Twitter, Facebook, and Instagram suspended President Trump's accounts indefinitely. As a reminder, President Trump could not sue these companies because such regulatory action was protected by Section 230's "Good Samaritan" provisions. According to Elizabeth Dwoskin and Craig Timberg, "Online misinformation about election fraud plunged 73 percent after several social media sites suspended President Trump and key allies" (sec 1; par 1). The study, conducted by Zignal Labs, "reported that conversations about election fraud dropped from 2.5 million mentions to 688,000 mentions across several social media sites in the week after Trump was banned from Twitter" (Dwoskin and Timberg, sec 1; par 2). These findings showcase that a few major actors can shape an entire information ecosystem.

Dwoskin and Timberg refer to President Trump and his allies as misinformation and disinformation "superspreaders" because their posts make up "a disproportionate share of the falsehoods and misleading narratives" (sec 1; par 17). As the Zignal Labs study illustrates, the removal of President Trump and his allies' accounts contributed to a massive decrease in the amount of misinformation about election fraud that circulated on social media. These findings provide significant implications for how ISPs can reduce the amount of dishonest content that circulates on their platforms. Should misinformation and disinformation "superspreaders" like President Trump and his allies be removed from social media platforms given their disproportionate impact on the amount of dishonest content online and potential to undermine democracy and incite violence?

Another question is whether the removal of President Trump and his allies' social media accounts impacted the degree to which the public accepted dishonest election content as true. The Monmouth University Polling Institute recently surveyed "a national random sample of 809 adults age 18 and older" on November 20th, 2020 and January 21, 2021 (5). As a reminder, most social media platforms removed President Trump and his allies' social media accounts by mid-January. One of the questions the Monmouth survey asked was, "Overall, how confident are you that the 2020 election was conducted fairly and accurately– very confident, somewhat confident, not too confident, or not at all confident?" (4). In November, 44% of respondents said that they were confident in the results of the election compared to 54% in January. (5) Another question asked was, "Do you believe Joe Biden won this election fair and square, or do you believe that he only won it due to voter fraud?" (4). Participant's responses showed that 60% believed that Joe Biden won the election fair and square in November compared to 65% in January (4).

These findings suggest a possible correlation between President Trump and his allies' removal from social media websites and the amount of election fraud misinformation and disinformation accepted by the public. It is worth noting that there could be other factors that influenced these results. However, I interpret both studies' findings to show that removing misinformation and disinformation "superspreaders" could be a potential solution, or at least starting point, to the misinformation crisis. And because of the "Good Samaritan" provisions of Section 230, these kinds of actions are wholly protected.

Bialy describes social media platforms as "a battlefield where we can observe different military strategies and tactics, such as deception, disinformation, propaganda, threatening opponents, mobilization of supporters, and coordination of actions" (86). I find her description of social media to be incredibly accurate. The significant decrease in election fraud misinformation after the deletion of President Trump and his allies' accounts potentially implies that a few actors can employ a series of strategies, work together, and manipulate the American public. Therefore, ISPs must be required to engage in the activities outlined by the "Good Samaritan" provisions of Section 230 because failing to do so could result in grave consequences.

Conclusion

I believe Section 230 has undoubtedly contributed to the rise of misinformation, disinformation, malinformation, and conspiracy theories on digital media. This kind of content undermines our information ecosystem by providing social media users with an alternate set of facts and even an alternate reality, where they can no longer distinguish the real from the not real. ISPs must utilize the “Good Samaritan” provisions of Section 230 to engage in meaningful third-party content moderation. If they refuse, I believe they should face consequences. There is a clear need for such action, given the pervasive impact conspiracy theories have had on present

society. Removing the accounts of so-called “superspreaders” of misinformation and disinformation could be a viable place to start. I believe taking such action would meet the criteria set forth in the “Good Samaritan” provisions and allow ISPs to carry out the original intent of Section 230.

Conclusion: The Future of Section 230

The future of Section 230 is uncertain. Politicians on both sides of the aisle have expressed a desire to reform the "Twenty-Six Words That Created The Internet," but for different reasons. Many Republicans, such as President Trump and Senator Ted Cruz, want to revise Subsection (c)2 of Section 230, also known as the "Good Samaritan" provisions that grant ISPs the authority to censor the conservative speech on their platforms. In other words, members of the Republican Party do not want ISPs to have the capacity to engage in mass moderation practices of user-generated content, such as adding disclaimers or editing, without being held legally liable for such actions. It is worth noting that Justice Clarence Thomas echoed this sentiment in his recently released opinion discussed in chapter 1.

In contrast, many Democrats like President Joe Biden and House Majority Leader Nancy Pelosi want to reform the law to prevent ISPs from knowingly spreading illegal and dishonest third-party content. To elaborate, Democrats want to limit the immunity granted by Subsection (c)1 of Section 230 that has permitted ISPs to consciously turn a blind eye to the spread of misinformation and conspiracy theories online. Despite their ideological differences, it seems that politicians across the political spectrum can agree that Section 230 is in desperate need of reform.

As demonstrated by chapter 1's investigation of the history of Section 230, the intentions of the law's writers, Cox and Wyden, were undoubtedly good. They wanted Section 230 to resolve the *CompuServe Inc.* and *Prodigy Services* precedents that encouraged ISPs to adopt a hands-off regulatory approach to the third-party content on their forums. Cox and Wyden also wanted to support the growth and development of the Internet. They feared that ISPs and technology companies would be unnecessarily burdened with lawsuits and regulatory actions

without Section 230. As Kosseff noted, Cox and Wyden were proponents of Internet exceptionalism, the belief that the Internet, because of its unique communal and informational benefits, disqualified it from regulation similar to that of other media formats (96-102). I argued that Section 230 granted ISPs immunity for all the third-party content on their platforms in exchange for them engaging in the "good faith" regulatory actions outlined by the "Good Samaritan" provisions. Unfortunately, ISPs have failed to fulfill their moderation obligations.

Chapter 2 examined how Section 230 contributed to the evolution of the digital sphere. As evidenced by this chapter, the Internet and ISP business models would not exist in their current forms without Section 230. The law enabled the characteristics associated with Web 2.0, like user-interactivity and content sharing, to become inherent components of the online space. It also allowed ISPs to develop a business model dependent on user-generated content. Without Section 230, ISPs like Facebook, Twitter, and Yelp would not operate in the manner that they do today because entities could sue them for distributing any piece of third-party content. In this way, Section 230 has had profound economic, informational, and communal benefits. However, it has also allowed ISPs to ignore harmful third-party content, prompting the deterioration of our information ecosystem. Lastly, chapter 3 explored the different kinds of fraudulent content, the 'birther' and election fraud conspiracy theories, and Section 230's impact on the present misinformation crisis. I also investigated how removing President Trump and his allies from social media potentially impacted the amount of election fraud misinformation and disinformation and the public's opinion on the outcome of the election.

While writing this thesis, my view on how to resolve Section 230 has changed numerous times. I finalized my opinion after listening to an episode of *The New York Times* production "The Argument" titled "I Love Section 230. Got a Problem with That?" In the episode, Jane

Coaston, Klon Kitchen, and Danielle Citron debate the merits of Section 230. Citron, a law professor at the University of Virginia, eloquently makes the case that Section 230 was designed to "incentivize monitoring . . . to have 'Good Samaritans' block and filter offensive speech" (Coaston, 03.02-11). She claims the problem with Section 230 is the actors who do not engage in these monitoring practices, and that Section 230 immunity should only extend to "Good Samaritan" actors who do engage (Coaston, 21:07-59). Citron's suggested reform addresses the core of Section 230's issues, and I think it could resolve them.

In contrast to Citron, Klon Kitchen, the former director of tech policy at the conservative think tank, The Heritage Foundation, argues the problem with Section 230 is the over-filtering of speech online. He says, "We need to clarify the line between acceptable editing and labeling and becoming a publisher who no longer enjoys the protections of Section 230" (Coaston, 15:25-33). Kitchen claims that certain editorial actions should force ISPs to forfeit their distributor liability, make them a publisher/author, and allow them to be sued for their attempts to moderate third-party content.

I disagree with Kitchen's opinion because I think it completely contradicts the original intent of Section 230, which was to incentivize ISPs to moderate user-generated content. Also, as Citron notes, "These are private actors. So the First Amendment doesn't apply to them naturally, right? They're not state actors. They're not state agents" (Coaston, 3:39-46). In other words, she is saying that it is within the discretion of ISPs to regulate, edit, or filter any of the third-party content on their platforms. Legally, an ISP like Twitter has the right to exercise control over the speech on its forum just as consumers have the right to go to another speech platform. Ultimately, I do not think the problem with Section 230 is the over-filtering of speech. The issue

with Section 230 is that it has permitted ISPs to blatantly disregard their responsibility as distributors of information to the public.

In my opinion, it is ridiculous that there has been no such reform to Section 230, or any reform for that matter, since the law's passage in 1996. I cannot think of another policy area in which there has been this level of political stagnation. It is especially alarming when you consider how the internet medium has evolved over time and the pervasive impact it has on public opinion and society writ large. We need to move past complacent, status quo thinking and revise Section 230 in a way that addresses the current misinformation crisis. Therefore, I believe the government must amend Section 230 to incentivize ISPs to actually engage in the activities outlined by the "Good Samaritan" provisions.

I also think we have a responsibility as consumers to think more critically about the media we consume. Failing to do so would cause us to fall victim to dishonest content and, consequently, prohibit us from making rational decisions when we vote. Ultimately, I consider Section 230 to be a major threat to present-day democracy because it has allowed ISPs to turn a blind eye to misinformation, disinformation, and conspiracy theories that distort the American people's perception of reality and, potentially, prevents them from voting in their best interest.

Today, anyone from foreign actors to average citizens to the president of the United States can post falsehoods and lies that pollute the media ecosystem to deceive and manipulate the American people online. The evolution of the digital landscape has made it possible for bad actors to corrupt public opinion with malicious content that can radicalize people and threaten our institutions and even democracy. Regardless of whether Section 230 continues to exist in its current form or is revised, these actors are not going anywhere. It is not hyperbole to say we are in the fight of our lives to save our democracy. We must arm ourselves with the media literacy

skills to differentiate fact from fiction and call on ISPs to enforce Section 230's "Good Samaritan" provisions, as failing to do so could mean the end of truth as we know it.

Bibliography

1. Abbate, Janet. “Government, Business, and the Making of the Internet.” *The Business History Review*, vol. 75, no. 1, 2001, pp. 147–176. *JSTOR*, www.jstor.org/stable/3116559. Accessed 12 Mar. 2021.
2. Abramowitz, Alan I. *The Great Alignment: Race, Party Transformation, and the Rise of Donald Trump*. Yale University Press, 2018. *JSTOR*, www.jstor.org/stable/j.ctvhrczh3. Accessed 12 Mar. 2021.
3. Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives*, 31 (2): 211-36. DOI: 10.1257/jep.31.2.211
4. American Civil Liberties Union. “Reno v. ACLU — Challenge to Censorship Provisions in The.” *American Civil Liberties Union*, 20 June 2017, www.aclu.org/cases/reno-v-aclu-challenge-censorship-provisions-communications-decency-act.
5. Anderson, Kyle. "Truth, Lies, and Likes: Why Human Nature Makes Online Misinformation a Serious Threat (and What We Can Do about It)." *Law & Psychology Review*, 44, 2019-2020, p. 209-244. *HeinOnline*, https://heinonline-org.proxy.library.emory.edu/HOL/P?h=hein.journals/lpsyr44&i=221.
6. Andrejevic, Mark. *Fake News: Understanding Media and Misinformation in the Digital Age (Information Policy)*. Edited by Melissa Zimdars and Kembrew McLeod. The MIT Press, 2020, pp. 19-44.
7. Aryanfard, Ojan. “National Security.” *The First Amendment Encyclopedia*, www.mtsu.edu/first-amendment/article/1134/national-security. Accessed 12 Dec. 2020.
8. Biały, Beata. “Social Media—From Social Exchange to Battlefield.” *The Cyber Defense Review*, vol. 2, no. 2, 2017, pp. 69–90. *JSTOR*, www.jstor.org/stable/26267344. Accessed 12 Mar. 2021.

9. Brenan, Megan. “Americans Remain Distrustful of Mass Media.” *Gallup.Com,* 14 Jan. 2021, news.gallup.com/poll/321116/americans-remain-distrustful-mass-media.aspx.
10. Carew, Kathryn L., and Kelley-Romano, Stephanie. “Make America Hate Again: Donald Trump and the Birther Conspiracy.” *Journal of Hate Studies*, vol. 14, no. 1, 2019, p. 33. *Crossref*, doi:10.33972/jhs.123.
11. Carey, Benedict. “A Theory About Conspiracy Theories.” *The New York Times*, 28 Sept. 2020, www.nytimes.com/2020/09/28/health/psychology-conspiracy-theories.html.
12. Cheney, Kyle. “No, Clinton Didn’t Start the Birther Thing. This Guy Did.” Politico, 16 Sept. 2016, www.politico.com/story/2016/09/birther-movement-founder-trump-clinton-228304.
13. Coaston, Jane “I Love Section 230. Got a Problem With That?” from *The New York Times, Danielle Keats Citron, Klon Kitchen,* 14 Jan. 2021 https://www.nytimes.com/2021/01/14/opinion/the-argument-trump-twitter-ban.html
14. “Conspiracy Theories Video 2 Render G.” *YouTube*, uploaded by News Literacy Project, 15 Dec. 2020, www.youtube.com/watch?v=JpNhO_Job2E.
15. “Conspiracy Theories Video 4 Render G.” *YouTube*, uploaded by News Literacy Project, 15 Dec. 2020, www.youtube.com/watch?v=IabjIYX7zeE&t=35s.
16. “Conway: Press Secretary Gave ‘Alternative Facts.’” *NBC News*, uploaded by NBC Universal, 22 Jan. 2017, www.nbcnews.com/meet-the-press/video/conway-press-secretary-gave-alternative-facts-860142147643.
17. Cornell University. “Summary Judgment.” *LII / Legal Information Institute,* 2021, www.law.cornell.edu/wex/summary_judgment.

18. Cox, Christopher. “The Origins and Original Intent of Section 230 of the Communications Decency Act.” *Richmond Journal of Law and Technology*, Jolt, 28 Aug. 2020, jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act.
19. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991)
20. Dropp, Kyle, and Brendan Nyhan. “It Lives. Birtherism Is Diminished but Far From Dead.” *The New York Times*, 23 Sept. 2016, www.nytimes.com/2016/09/24/upshot/it-lives-birtherism-is-diminished-but-far-from-dead.html.
21. Dwoskin, Elizabeth, and Craig Timberg. “Misinformation Dropped Dramatically the Week after Twitter Banned Trump and Some Allies.” *Washington Post*, 16 Jan. 2021, www.washingtonpost.com/technology/2021/01/16/misinformation-trump-twitter.
22. Featherly, Kevin. “ARPANET | Definition & History.” *Encyclopedia Britannica*, 11 May 2016, www.britannica.com/topic/arpanet.
23. Foerstel, Herbert. *Banned in the Media: A Reference Guide to Censorship in the Press, Motion Pictures, Broadcasting, and the Internet (New Directions in Information Management)*. 1st ed., Greenwood, 1998.
24. Gordon-Murnane, Laura. *Web of Deceit: Misinformation and Manipulation in the Age of Social Media*. Edited by Mintz, Anne, et al. CyberAge Books, 2012, pp. 107-133.
25. Guilbeault, Douglas. “Digital Marketing in the Disinformation Age.” *Journal of International Affairs*, vol. 71, no. 1.5, 2018, pp. 33–42. *JSTOR*, www.jstor.org/stable/26508116. Accessed 12 Mar. 2021.

26. Hwang, Tim. “Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment.” *SSRN Electronic Journal*, 2017, pp. 2–40. *Crossref*, doi:10.2139/ssrn.3089442.
27. Jackman, Tom. “Police Union Says 140 Officers Injured in Capitol Riot.” *Washington Post*, 28 Jan. 2021, www.washingtonpost.com/local/public-safety/police-union-says-140-officers-injured-in-capitol-riot/2021/01/27/60743642-60e2-11eb-9430-e7c77b5b0297_story.html.
28. Kosseff, Jeff. *The Twenty-Six Words That Created the Internet*. 1st ed., Cornell University Press, 2019.
29. Krutka, Daniel. “Move Slower and Protect People: Toward Social Media Inquiry and Activism in Social Studies.” *National Council for the Social Studies*, vol. 84, no. 2, 2020, pp. 113–17, www.ingentaconnect.com/contentone/ncss/se/2020/00000084/00000002/art00008.
30. Lee, Timothy. “The Top 20 Fake News Stories Outperformed Real News at the End of the 2016 Campaign.” *Vox*, 17 Nov. 2016, www.vox.com/new-money/2016/11/16/13659840/facebook-fake-news-chart.
31. *Malwarebytes, Inc v. Enigma Software Group USA*, LLC, 592 U. S. ____ (2020)
32. Media Bias Fact Check. “Newsmax.” *Media Bias Fact Check*, 10 Mar. 2021, mediabiasfactcheck.com/newsmax.
33. Mintz, Anne, et al. *Web of Deceit: Misinformation and Manipulation in the Age of Social Media*. CyberAge Books, 2012.

34. Monmouth University. “Majority Support Trump Impeachment.” *Monmouth University Polling Institute,* 27 Jan. 2021, www.monmouth.edu/polling-institute/reports/monmouthpoll_us_012521.

35. Morning Consult. “National Tracking Poll.” *Morning Consult,* Sept. 2016, intel.morningconsult.com/public/mc/160910_topline_NYT_v2_KD.pdf.

36. *Near v. Minnesota,* 283 U.S. 697 (1931)

37. Ott, Brian L. “The Age of Twitter: Donald J. Trump and the Politics of Debasement.” *Critical Studies in Media Communication*, vol. 34, no. 1, 2016, pp. 59–68. *Crossref*, doi:10.1080/15295036.2016.1266686.

38. Patricia Spiccia, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 Val. U. L. Rev. 369 (2013).

39. Pickard, Victor. *Fake News: Understanding Media and Misinformation in the Digital Age (Information Policy)*. Edited by Melissa Zimdars and Kembrew McLeod. The MIT Press, 2020, pp. 123-144.

40. Tarleton Gillespie, *Fake News: Understanding Media and Misinformation in the Digital Age (Information Policy)*. Edited by Melissa Zimdars and Kembrew McLeod. The MIT Press, 2020, pp. 324-341.

41. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)

42. Feingold et al, *Fake News and Misinformation: The Roles of the Nation's Digital Newsstands, Facebook, Google, Twitter, and Reddit*, Fake News/Misinformation: The Challenge and the Most Effective Solutions, October 2017.

https://www-cdn.law.stanford.edu/wp-content/uploads/2017/10/Fake-News-Misinformation-FINAL-PDF.pdf

43. Rutenberg, Jim. “The Man Behind the Whispers About Obama.” *The New York Times*, 14 Oct. 2008, www.nytimes.com/2008/10/13/us/politics/13martin.html.
44. Shearer, Elisa, and Amy Mitchell. “News Use Across Social Media Platforms in 2020.” *Pew Research Center’s Journalism Project*, 12 Jan. 2021, www.journalism.org/2021/01/12/news-use-across-social-media-platforms-in-2020.
45. Silverstein, Jason. “Twitter Adds Fact-Check Label to Trump Tweets for First Time.” *CBS News*, 14 Sept. 2020, www.cbsnews.com/news/twitter-adds-fact-check-warning-trump-tweets.
46. Skorup, Brent, and Jennifer Huddleston. “The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation.” *SSRN Electronic Journal*, 2019, pp. 1–44. *Crossref*, doi:10.2139/ssrn.3420304.
47. Sprunt, Barbara, and Ryan Lucas. “NPR Cookie Consent and Choices.” *National Public Radio*, 10 Feb. 2021, choice.npr.org/index.html?origin=https://www.npr.org/sections/trump-impeachment-trial-live-updates/2021/02/10/966508091/using-new-video-footage-managers-show-how-close-rioters-got-to-pence-lawmakers.
48. *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995)
49. Struyk, Ryan. “67 Times Donald Trump Tweeted About the ‘Birther’ Movement.” *ABC News*, 17 Sept. 2016, abcnews.go.com/Politics/67-times-donald-trump-tweeted-birther-movement/story?id=42145590.

50. Thompson, Robin. “Radicalization and the Use of Social Media.” *Journal of Strategic Security*, vol. 4, no. 4, 2011, pp. 167–190. *JSTOR*, www.jstor.org/stable/26463917. Accessed 12 Mar. 2021.

51. THURLOW, CRISPIN. “Fakebook: Synthetic Media, Pseudo-Sociality, and the Rhetorics of Web 2.0.” *Discourse 2.0: Language and New Media*, edited by Deborah Tannen and Anna Marie Trester, Georgetown University Press, 2013, pp. 225–250. *JSTOR*, www.jstor.org/stable/j.ctt4cg8wd.17. Accessed 12 Mar. 2021.

52. Trump, Donald (@realDonaldTrump). “REPEAL SECTION 230!!!” 6, Oct. 2020, 12:08 pm. Tweet.

53. Trump, Donald (@realDonaldTrump). “"An 'extremely credible source' has called my office and told me that @BarackObama's birth certificate is a fraud." 6, Aug. 2020, 4:23 pm. Tweet.

54. Trump, Donald (@realDonaldTrump). “There is NO WAY (ZERO!) that Mail-In Ballots will be anything less than substantially fraudulent . . . This will be a Rigged Election” 26, May 2020, 8:17 am. Tweet.

55. Wardle, Claire and Derakhshan, Hossein. *Fake News: Understanding Media and Misinformation in the Digital Age (Information Policy)*. Edited by Melissa Zimdars and Kembrew McLeod. The MIT Press, 2020, pp. 71-86.

56. YERLİKAYA, TURGAY. “Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process.” *Insight Turkey*, vol. 22, no. 2, 2020, pp. 177–196. *JSTOR*, www.jstor.org/stable/26918129. Accessed 12 Mar. 2021.

57. *Zeran v. America Online, Inc*., 129 F.3d 327 (4th Cir. 1997)

58. Zimdars, Melissa, and Kembrew Mcleod. *Fake News: Understanding Media and Misinformation in the Digital Age (Information Policy)*. The MIT Press, 2020.

59. Ziniti, Cecilia. “The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got It Right and Web 2.0 Proves It.” *Berkeley Technology Law Journal*, vol. 23, no. 1, 2008, pp. 583–616. *JSTOR*, www.jstor.org/stable/24118328. Accessed 12 Mar. 2021.

60. 47 U.S.C. § 230