TESTIMONY OF JEFF KOSSEFF

ASSISTANT PROFESSOR, CYBER SCIENCE DEPARTMENT

UNITED STATES NAVAL ACADEMY

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

"ONLINE SEX TRAFFICKING AND THE COMMUNICATIONS DECENCY ACT"

OCTOBER 3, 2017

Summary

- The U.S. legal system must provide sufficient criminal and civil penalties to deter online sex trafficking.
- Congress passed Section 230 in 1996 because the legal precedents at the time did not adequately protect online services from liability for third-party content, and the rules discouraged many companies from moderating user content.
- By passing Section 230, Congress allowed companies to create business models around user content. It is not a coincidence that many of the most successful Internet platforms in the world are based in the United States.
- In its current form, Section 230 does not provide absolute immunity to online platforms. All federal criminal laws are explicitly exempt from Section 230. And platforms are not immune from civil actions or state criminal prosecutions that arise from content that the platforms created.
- If Congress amends Section 230 to address online sex trafficking, it should do so in a manner that severely punishes bad actors while minimizing broader harms to legal online speech.
- States should not subject platforms to a patchwork of 50 different laws. Rather, if Congress creates a Section 230 exception regarding sex trafficking, it also should craft a national standard, providing clear and certain rules for compliance.
- Addressing the liability of public-facing platforms is one component of a much larger problem. Sex trafficking – like other online crimes – also occurs on the dark web, out of the reach of law enforcement. In addition to focusing on Section 230, I hope that Congress continues to examine crimes in these dark corners of the Internet.
- Amending Section 230 would not cause the Internet to shut down. But depending on the details of the amendment, it could chill some legal speech. Accordingly, changes to Section 230 must be carefully crafted and targeted.

Chairman Sensenbrenner, Vice Chairman Gohmert, Ranking Member Jackson Lee, and Members of the Subcommittee, thank you for the opportunity to testify about Section 230 of the Communications Decency Act.

My name is Jeff Kosseff, and I am an assistant professor at the United States Naval Academy's Cyber Science Department. The views that I express today are only my own, and do not represent those of the United States Naval Academy, Department of Navy, Department of Defense, or any other party.

I thank the Subcommittee for taking a close and serious look at Section 230. No other section of the United States Code has had a greater impact on the development of the Internet. Because of

Section 230, the Internet in the United States is the epitome of everything that we love and hate about unconstrained free speech.

Both the House and Senate are considering proposals to amend Section 230 to address online sex trafficking. Our legal system must have strong criminal penalties *and* civil remedies to deter not only the act of sex trafficking, but also the knowing advertisement of sex trafficking by online platforms. There are some offenses against humanity that society never should tolerate, and sex trafficking is one of them. To the extent that it determines that existing law does not sufficiently prevent such horrific crimes, I hope that Congress agrees on a solution that imposes severe penalties on bad actors – and we need to be clear, there are some very bad actors – without chilling legal speech. This is a difficult legislative balancing act, but I am confident that Congress, victims' rights groups, and the technology community can find common ground.

I am not here today to support or oppose any particular bill. Rather, I hope to provide you with information that I have gathered and conclusions that I have drawn after spending more than a year researching and writing a book about the history of Section 230 for Cornell University Press. These conclusions go beyond whether Section 230 is good or bad for society; such judgments are a matter of individual values about free speech, privacy, and other highly personal issues. Instead, I look at how Section 230 has affected the Internet, and the role that the statute might play in the future.

The recent debates over Section 230 understandably have become heated on both sides. What I hope to do today is provide insight into the history and mechanics of Section 230 that I believe have been lacking from the current discussions. A clear and objective understanding of Section 230 is essential before making any changes to a law that has so fundamentally shaped the nature of the Internet.

Below are five of my reflections about Section 230, gathered over the course of my research, that I believe might inform your analysis of this critical issue. I then suggest a few principles to guide Congress as you determine how to balance Section 230's free speech protections with the urgent need to battle online sex trafficking.

1. Section 230 Filled the Gaps in First Amendment Protections for Online Platforms

Understanding Section 230's history is key to mapping its future. Fundamentally, Section 230 is a statute that promotes free online speech. These protections exceed the requirements of the First Amendment, and were born out of a recognition that the Internet is exceptional and requires special protection.

Decades before Congress passed Section 230 in 1996, courts grappled with the issue of whether intermediaries could be liable for third-party content. Of course, these debates did not involve the Internet; they primarily focused on whether bookstores or newsstands could face criminal prosecutions or civil lawsuits for the books and magazines that they sold.

In 1959, Eleazar Smith, a Los Angeles bookstore owner, faced a 30-day jail sentence because his store sold an erotic book that the Los Angeles Police Department believed was obscene.[1] A local ordinance prevented stores from merely possessing obscene materials. The Supreme Court struck down his conviction on First Amendment grounds because the ordinance lacked any requirement that the bookstore was aware of the obscene material. Although the Court did not define precisely what state of mind would satisfy the First Amendment, the Los Angeles ordinance was unconstitutional, the Court wrote, because it lacked absolutely any mental element. In later cases, lower courts clarified the state of mind necessary to impose liability on distributors of third-party content: the distributors are liable only if they knew or should have known of the illegal content.[2]

This standard was well-accepted until the early 1990s, as companies began to offer services that connected personal computers to online bulletin boards and other services. These companies allowed third parties to publicly post content available to other users.

The two dominant online services of the time – CompuServe and Prodigy – took very different approaches to third-party content. CompuServe adopted a hands-off policy, and did not edit or even review any of the bulletin boards or newsletters that it distributed online. Prodigy, on the other hand, sought to frame itself as a family-friendly service, setting user content policies and engaging moderators to remove objectionable content.

In the early 1990s, both services faced defamation lawsuits – CompuServe by a former broadcaster who claimed he was defamed in an online newsletter that the company distributed,[3] and Prodigy by a financial executive and his company, who claimed that an anonymous bulletin board user had posted false claims about their business practices.[4]

CompuServe convinced a judge to dismiss its case because the judge concluded that the company was a mere conduit that had no knowledge or reason to know of the alleged defamation. But a different judge refused to dismiss the case against Prodigy because he concluded that Prodigy was not just a conduit. Prodigy hired moderators and set standards for user content. That made it a publisher, the judge concluded, and therefore Prodigy could not dodge the lawsuit by merely claiming that it was unaware of the user post.

---

[1] Smith v. California, 361 U.S. 147 (1959).

[2] *See, e.g.*, Spence v. Flynt, 647 F. Supp. 1266, 1273 (D. Wyo. 1986) ("[T]hough the defendant may not have known the exact content of the allegedly libelous statement, it knew enough about the statement so that it should have investigated the statement's truth before distributing, or continuing to distribute the publication"); Osmond v. EWAP, 153 Cal.App.3d 842, 852 (Cal. Ct. App. 1984) ("In short, innocence is generally considered a defense where such defendants merely circulate another's libel unless 'they knew or should have known' of the defamatory nature of the material.").

[3] Cubby, Inc. v. CompuServe, Inc., 776 F.Supp. 135 (S.D.N.Y.1991).

[4] Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Media L. Rep. 1794, 1995 WL 323710 (N.Y.Sup.Ct. 1995).

Taken together, the cases created a bizarre rule: online services might *increase* their liability by moderating third-party content. By taking an entirely hands-off approach like CompuServe, platforms might significantly reduce their liability.

Some members of Congress took notice of this troubling incentive. Then-Representatives Chris Cox and Ron Wyden proposed a bill that would later become Section 230. The most important part of the bill are the twenty-six words that state: "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."[5] The bill also included a few explicit exceptions: for federal criminal law,[6] intellectual property law,[7] and electronic communications privacy laws.[8]

Section 230 received virtually no media attention at the time, as it was buried in an online decency bill that itself was buried in the massive Telecommunications Act of 1996. All eyes were on other parts of the Telecom Act. Just think about it: although Section 230 would be at the heart of some of the most difficult Internet law disputes over the next two decades, the public at the time focused on the rules of competition between landline local and long-distance phone companies.

In my interviews with the lawyers, staffers, and members of Congress who were instrumental in creating Section 230, it became clear that they had two goals in enacting the statute. First, they hoped the statute would allow online services to moderate and set community standards; indeed, Section 230 also included a provision that prevents platforms from being held liable for taking good-faith actions to restrict access to objectionable content.[9] And over the past 20 years, many online platforms have, in fact, adopted a wide range of policies and procedures to moderate user content.[10]

But the drafters had a second goal: to promote the goal of free speech in the nascent online industry. In fact, Section 230 explicitly states that it is the policy of the United States "to promote the continued development of the Internet and other interactive computer services and other interactive media;"[11] and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation[.]"[12]

---

[5] 47 U.S.C. § 230(c)(1).
[6] 47 U.S.C. § 230(e)(1).
[7] 47 U.S.C. § 230(e)(2).
[8] 47 U.S.C. § 230(e)(4).
[9] 47 U.S.C. § 230(c)(2).
[10] *See* Jeff Kosseff, *Twenty Years of Intermediary Immunity: The U.S. Experience*, 14:1 SCRIPTed 5, 30 (2017) ("In addition to the limits imposed on Section 230 by courts, intermediaries have developed policies, procedures, and technology to moderate user content.").
[11] 47 U.S.C. § 230(b)(1).
[12] 47 U.S.C. § 230(b)(2).

It was not until more than a year after Congress passed Section 230 that courts began to affirm broad scope of this immunity. In *Zeran v. America Online*,[13] Ken Zeran sued America Online because an anonymous AOL user had posted advertisements purporting to sell merchandise that contained crude jokes about the recent Oklahoma City bombing. The fake ads included Zeran's home telephone number, and they soon caused him to receive frequent angry and threatening calls. Zeran sued America Online for negligently distributing defamatory material.[14] A district court judge dismissed the case, reasoning that the new Section 230 shielded America Online.[15] His lawyers asked the United States Court of Appeals for the Fourth Circuit to reverse the ruling, arguing that Section 230 merely clarified that online services such as America Online are liable only if they know that they host illegal user content. Because Zeran had complained to America Online and the company failed to promptly remove the posts, his lawyers argued, Section 230 did not immunize America Online.

The Fourth Circuit rejected Zeran's argument. Section 230, the Court ruled in a Nov. 12, 1997 opinion, immunizes online services for claims arising from user content regardless of whether the company knew about the allegedly illegal content. Zeran's interpretation of Section 230, the Court reasoned, would have a chilling effect on online speech. "Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information," the Fourth Circuit wrote. "Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context."[16]

In the two decades since the Fourth Circuit decided against Zeran, courts have cited the ruling in hundreds of opinions interpreting Section 230. As I discuss below, some courts have begun to erode this immunity; however, the broad holding of *Zeran* remains the law of the land: Section 230 provides online platforms with protections that often go beyond those of the First Amendment.

Congress is free to amend – or even eliminate – Section 230; it is a policy choice of Congress, not a constitutional right. But Congress should be aware that any such amendments would impact free speech online and could fundamentally change the Internet that is part of the fabric of American life.

2. Section 230 is Responsible for the Internet that Americans Know Today

Initially, my Section 230 book was titled *The Twenty-Six Words that Changed the Internet*. After spending months immersed in Section 230's history, I decided that did not capture the full impact of Section 230. The book is now titled *The Twenty-Six Words that Created the Internet*.

---

[13] Zeran v. America Online, Inc., 129 F. 3d 327 (4th Cir. 1997).
[14] *Id.* at 329.
[15] *Id.* at 330.
[16] *Id.* at 333.

Of course, the Internet was created before Congress passed Section 230 in 1996. But the Internet that we all know today -- in which every person owns a virtual printing press, and every social media post can be a sharp sword or a strong shield – traces back to the twenty-six words in Section 230.

For better and worse, Section 230 allowed online platforms to thrive by providing them with a simple and far-reaching immunity from claims arising from user-generated content. Yelp, Google, Facebook, Wikipedia, and Twitter are among the platforms that have convinced courts to dismiss user content-related claims because of Section 230.

Imagine a world in which Congress never had passed Section 230. Online platforms would be left only with the protections that CompuServe and Prodigy received in the pre-Section 230 days. In the best-case scenario for online platforms, the companies would receive protection from lawsuits only if they were unaware of harmful content; this would allow anyone who is upset with a user post to demand takedown and exercise a heckler's veto. At worst, online platforms could lose even the prospect of immunity merely because they moderate user content or set online community standards. We would be back to the same problem that led Congress to pass Section 230 in the first place: online platforms might avoid editing any user content out of fear of becoming liable for all of it. Alternatively, the platforms might simply decide that user content is too risky, and only provide access to materials that the companies created.

Under this regime, it is unlikely that companies like Yelp and Twitter ever could have been created in the United States, at least in their current form.[17] Whether that would have been a net benefit or harm to society is a policy discussion that Congress should have.

Other countries – including many western democracies – do not protect online platforms to the same extent as the United States. Many of them generally provide the same protections as the pre-Section 230 United States: platforms become liable for user content once they have notice of the allegedly illegal material.

Consider the European Union. In 2015, the Grand Chamber of the Court of Justice for the European Union ruled against Delfi, an Estonian news website on which an anonymous user posted allegedly defamatory comments.[18] Although Delfi removed the comments about six weeks after receiving a complaint, the Grand Chamber ruled that the site did not move quickly enough, nor did it adopt sufficient safeguards to prevent defamatory comments in the first place.

---

[17] *See, e.g.*, DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 171 (2014) ("Supporters of Section 230 argue that without immunity, search engines like Google, Yahoo!, and Bing and social media providers like Facebook, YouTube, and Twitter might not exist. The point is well taken. The fear of publisher liability surely would have inhibited their growth.").

[18] Judgment, Case of Delfi v. Estonia, Application no. 64569/09 (Grand Chamber, European Court of Human Rights June 16, 2015).

Likewise, the European Union recognizes a Right to Be Forgotten, which allows individuals to ask search engines to de-index content that infringes on their privacy rights (such as an old newspaper article about personal financial difficulties).[19]

Many in Europe believe that these restrictions on online platforms are reasonable; they argue that such protections are necessary to protect reputations and privacy. However, such restrictions come at a price: by increasing the risk for platforms, these laws reduce the likelihood that the companies will allow their users to communicate freely, and they also likely reduce entrepreneurship in interactive online technologies by imposing significant risks on companies.

3. Section 230 Cases Never Have Been Easy

In recent years, Section 230 has received increased scrutiny for courts' denial of civil relief to victims with heartbreaking stories: families of people killed terrorist groups that organized and recruited via social media;[20] people who were the subject of scurrilous and vicious lies on websites;[21] and, most notably, people who were trafficked on sites such as Backpage.com.[22]

These cases reveal a truth about Section 230: the statute's free speech protections often prevent sympathetic victims from recovering damages from online platforms. To be clear, Section 230 does not block them from suing the people who created the harmful content. Nor does Section 230 prevent federal criminal prosecutions. Nonetheless, there is an understandable unfairness in any statutory preemption of a civil claim, particularly when the plaintiff has faced devastating harms.

But this inequity is not a new development in the world of Section 230. Ever since Congress enacted the statute, it has led to some harsh results for victims.

Zeran was the first complaint filed to result in a court opinion interpreting Section 230; the second such case was *Doe v. America Online*,[23] filed in Florida state court. As I researched my book, I found the outcome of *Doe* to be far more troubling than that of *Zeran*.

In *Doe*, the mother of a boy who was 11 years old in 1994 claimed that a man recorded and photographed her son and two other minors engaged in sexual activity, and that he marketed the images and videos via AOL chat rooms. The mother sued America Online in January 1997, and the case advanced to the Florida Supreme Court.

Four of the seven Florida Supreme Court justices ruled that Section 230 barred the claims. But three justices issued a stinging dissent, writing that Section 230 has "been transformed from an

---

[19] *See*, Google Spain, SL v. Costeja Gonzalez, Case C-131/12 (Grand Chamber May 13, 2014); Article 17, European Union General Data Protection Regulation.
[20] *See, e.g.*, Fields v. Twitter, Inc., 200 F. Supp. 3d 964 (N.D. Cal. 2016).
[21] *See, e.g.*, Jones v. Dirty World Entertainment Recordings LLC, 755 F. 3d 398 (6th Cir. 2014).
[22] *See, e.g.*, Doe No. 1 v. Backpage. com, LLC, 817 F. 3d 12 (1st Cir. 2016).
[23] Doe v. America Online, Inc., 783 So.2d 1010 (Fla. 2001).

appropriate shield into a sword of harm and extreme danger which places technology buzz words and economic considerations above the safety and general welfare of our people."[24]

And *Doe* is not the only difficult Section 230 case that has emerged over the past two decades. Section 230 has stifled claims by an actress who suffered threats after an online dating service published a false profile of her, forcing her to temporarily move from her home;[25] a lawyer whose business struggled after she was falsely accused of saying that she was Heinrich Himmler's granddaughter and owning stolen Nazi artwork;[26] and a political aide who was falsely accused of spousal abuse.[27]

Courts ruled on these tough cases more than a decade ago. Although Section 230 suddenly is receiving public attention because of online sex trafficking, terrorists' use of social media, and other new threats, Section 230 always has presented tough fact patterns.

4. Section 230 Immunity is Not Absolute

Section 230 contains very few explicit exceptions to immunity. However, courts are increasingly reluctant to immunize platforms that appear to have played a role in creating the harmful content.

Section 230 prevents an interactive computer service provider from being treated as the publisher or speaker of information provided by *another information content provider*. The statute defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

If a court determines that the online platform – and not another information content provider – provided the illegal information, then Section 230's immunity will not apply. Likewise, Section 230 only applies to claims that treat the defendant as the "publisher or speaker" of the information.

The trend toward a narrower reading of Section 230 began in 2008, when the United States Court of Appeals for the Ninth Circuit, sitting en banc, ruled that a roommate-matching website could be sued for asking questions that required users to violate federal and state housing discrimination laws.[28]

"If such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online," Judge Alex Kozinski wrote for the majority.[29]

---

[24] *Id.* at 1019 (Lewis, J., dissenting).
[25] Carafano v. Metrosplash. com. Inc., 339 F. 3d 1119 (9th Cir. 2003).
[26] Batzel v. Smith, 333 F. 3d 1018 (9th Cir. 2003).
[27] Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).
[28] Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008) (en banc).
[29] *Id.* at 1164.

Since the Ninth Circuit's opinion, courts have become more likely to deny Section 230 immunity, often on the basis that the online platform somehow created or contributed to the offending third-party content, or that the lawsuit does not seek to hold the defendant liable as the publisher or speaker of information. In an article that I published in Columbia Science & Technology Law Review earlier this year, I found that between July 1, 2015 and June 30, 2016, courts refused to provide full Section 230 immunity in fourteen of twenty-seven cases. In comparison, in 2000 and 2001, courts provided full Section 230 immunity in eight of the ten Section 230 cases.[30]

One of the most controversial Section 230 rulings was the United States Court of Appeals for the First Circuit's 2016 decision to affirm the dismissal of a complaint against Backpage filed by plaintiffs who claim that they were victims of sex-trafficking, and that their traffickers advertised on the site.[31] The plaintiffs argued that Section 230 did not apply because they did not seek to hold Backpage responsible as the publisher of the content; rather, their claims arose from the design of Backpage's site, such as the lack of phone number verification methods and the procedures for uploading photos. The First Circuit rejected this argument, concluding that such features, "which reflect choices about what content can appear on the website and in what form, are editorial choices that fall within the purview of traditional publisher functions."[32]

The First Circuit judges clearly were torn about the decision; in the first sentence of the opinion, they wrote that this is a "hard case" because the law requires the court to "deny relief to plaintiffs whose circumstances evoke outrage."[33] And just few months before the First Circuit issued its opinion, the Washington state Supreme Court allowed a strikingly similar case to proceed against Backpage, concluding that Section 230 did not shield the site from liability.[34]

It is tough to square the First Circuit's opinion with the Ninth Circuit's *Roommates.com* decision, particularly in light of the Senate Homeland Security and Government Affairs Committee's Permanent Subcommittee on Investigations report about Backpage's operations earlier this year. The Subcommittee report described in detail how Backpage "knowingly concealed evidence of criminality by systematically editing its 'adult' ads."[35] The Senate's findings were followed months later by a Washington Post report that a Backpage contractor "has been aggressively soliciting and creating sex-related ads, despite Backpage's repeated insistence that it had no role in the content of ads posted on its site[.]"[36] Both the Senate report and the Washington Post

---

[30] Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet*, 18 COLUM. SCI. & TECH. L. REV. 1 (2017).
[31] Doe No. 1 v. Backpage.com, 817 F.3d 12 (1st Cir. 2016).
[32] *Id.* at 21
[33] *Id.* at 15.
[34] J.S. v. Village Voice Media Holdings, 359 P.3d 714 (Wash. 2015).
[35] UNITED STATES SENATE, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS, BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING (Jan. 9, 2017)
[36] Tom Jackman & Jonathan O'Connell, *Backpage Has Always Claimed it Doesn't Control Sex-Related Ads. New Documents Show Otherwise*, WASH. POST (July 11, 2017).

article were published after the First Circuit issued its ruling; had this information been part of record before the First Circuit, I believe that it is less likely that the First Circuit would have affirmed the dismissal of the claims against Backpage. Indeed, my views on Backpage's Section 230 immunity and the First Circuit's decision evolved after reading the Senate report and media coverage; it became clear to me that Section 230, as currently drafted and interpreted by courts around the country for two decades, does not immunize Backpage.

5. Private Sector Cooperation is Possible – and Effective in Fighting Cybercrime

My final observation provides a bit of hope for compromise and collaboration.

Online platforms, the National Center for Missing and Exploited Children (NCMEC), and law enforcement for years have battled online child pornographers.[37] This successful effort gives me hope that technology companies and federal and state officials can work together to combat sex trafficking – and other crimes that threaten Americans' safety.

As I describe above, Section 230 does not immunize online platforms from federal criminal law. A federal criminal law requires online platforms to file a report with NCMEC if the provider obtains "actual knowledge of any facts or circumstances" of an "apparent violation" of federal child pornography laws.[38] NCMEC then investigates and works with law enforcement.

The federal criminal law only requires service providers to file these reports if they have *actual knowledge*. The law does not require the providers to monitor user content for child pornography; in fact, the statute explicitly states that the platforms are not obligated to monitor user content.[39]

Nonetheless, many large technology companies have gone beyond their legal duties and sought to identify the use of their services to traffic in child pornography. Technology companies have worked with researchers to develop sophisticated, automated scanning technology that identifies known child pornography images and videos. When this scanning technology identifies a match, the provider then has actual knowledge and must file a report with NCMEC.[40]

---

[37] *See* Emil Protalinski, *Facebook Taps Microsoft to Fight Child Pornography*, ZDNET (May 19, 2011).
[38] 18 U.S.C. § 2258A.
[39] 18 U.S.C. § 2258A(f).
[40] *See* Testimony of John Shehan, National Center for Missing and Exploited Children, for the United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Committee on the Judiciary, *Preventing Crimes Against Children: Assessing the Legal Landscape* (Mar. 16, 2017) ("Many Internet companies take proactive steps to limit the presence of child pornography on their platforms, including the use of innovative technology, such as PhotoDNA, a private hash matching technology tool developed by Microsoft in partnership with Dartmouth College, and sharing best practices to eradicate the dissemination of child sexual exploitation images. The use of these hashing technologies enables companies to prevent child sexual abuse content from being transmitted across their platforms and to report users who attempt to transmit such illegal content.").

The program has been so successful that some criminal defendants in child pornography cases have argued that both the service providers and NCMEC are agents of the government that should be subject to the Fourth Amendment's restrictions on searches and seizures.[41] The companies have argued that they scan user content because it is in their business interests to keep their services free of child pornography.[42]

Likewise, I hope that online platforms would see the need to work with law enforcement and take all practical steps to rid their services of sex trafficking. And I hope that federal and state law enforcement would work with the platforms against a common enemy.

Moving Forward

I'll conclude by suggesting some guiding principles to apply to the online sex trafficking discussions. These principles also could guide other debates about intermediary liability in contexts such as terrorist recruitment and nonconsensual distribution of intimate images (also known as revenge pornography).

First, we must have an honest discussion about Section 230: perhaps Congress will decide existing law does not adequately deter online sex trafficking advertisements, and that amending Section 230 is necessary to hold some platforms accountable. For instance, Congress might conclude that the federal government alone may not have the resources to adequately investigate and prosecute platforms that knowingly advertise online sex trafficking, requiring an amendment to Section 230 that enables states to prosecute and victims to sue. That is a policy judgment for elected lawmakers. Section 230 is a statutory privilege, not a constitutional guarantee. But we must be aware that abrogation of Section 230 immunity may cause at least some platforms to reduce or eliminate user-generated content, ultimately burdening free online speech.

Second, any changes to Section 230 should be tailored and focused on preventing online sex trafficking and allowing victims to seek justice. The changes should minimize harms to legal online speech. This requires careful drafting, and extensive discussion about issues such as mens rea. The goal should be holding culpable platforms accountable without forcing other platforms to over-censor legal speech. A Section 230 exception should target the platforms that knowingly advertise sex trafficking. Recklessness or negligence standards for user-generated content could create great uncertainty. Likewise, the laws should specify a responsible and effective procedure for platforms to take after they learn of sex trafficking advertisements, such as expeditiously reporting to law enforcement and taking down content. And Congress should assess the role that restitution might play in aiding victims.[43]

Third, to the greatest extent possible, any Section 230 exception to address online sex trafficking advertising should apply a uniform national standard. In my time practicing and writing about technology law, I have come to believe that the Internet is most efficiently and effectively

[41] *See, e.g.*, United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); United States v. Keith, 980 F.Supp.2d 33 (D. Mass. 2013).
[42] *See* Keith, 980 F.Supp.2d at 40.
[43] *See* 18 U.S.C. § 1593.

regulated with national standards, rather than a patchwork of different state laws. I do not suggest that we should preclude state attorneys general from seeking justice, or state courts from hearing claims; rather, I am concerned about platforms facing 50 different laws that might contain very different substantive and procedural requirements. A single national legal standard would provide clear and certain rules, and ultimately increase the likelihood of compliance. The Stop Advertising Victims of Exploitation Act – which sets a federal criminal standard for addressing sex trafficking advertising – is a good example of a strong and effective national standard.

Fourth, any changes to Section 230 should only be one part of a larger solution to fight online sex trafficking. We must be aware that any amendments to Section 230 will not completely eliminate online sex trafficking or other cybercrimes. Criminals also operate on the dark web, where they often can entirely avoid law enforcement and operate under a cloak of anonymity. In my experience researching and teaching cybersecurity law, I have learned far too much about the use of the dark web by sex traffickers, child pornographers, terrorists, and other criminals. I have no doubt that even if sex trafficking were eliminated entirely on public-facing platforms, the crime would continue in the dark corners of the Internet.[44] This is not to suggest that we should give up on holding public platforms accountable for knowingly advertising sex trafficking; rather, changing platform liability laws is one piece of a larger puzzle. Law enforcement must have adequate resources and legal authorities to fight online crime wherever it exists.

To be clear, this debate does not a present us with a binary choice. Changing Section 230 would not cause the Internet to shut down. It is possible to amend Section 230 while preserving its core values of an open and free Internet. But the magnitude of harm to online speech will vary depending on the precise wording of any exceptions.

Section 230 is a complicated and enormously important law. As a lawyer, I advised media companies on user content liability, and long have been an enthusiastic supporter of Section 230.[45] I remain convinced that the statute is essential to preserving the open Internet that Americans know today, particularly for the start-ups that are the future Yelps and Twitters. However, after spending more than a year researching a book about Section 230, my support for the statute is tempered by the very real harms suffered by some victims who cannot get their day in court. The challenge for all of us will be to combat terrible acts such as online sex trafficking while preserving the free Internet that Section 230 made possible.

I realize that everyone who is immersed in the Section 230 debate likely will disagree with at least some of the conclusions that I have stated today. And that is a good thing. Before

---

[44] *See, e.g.*, Barbie Latza Nadeua, *Inside 'Black Death Group,' the Dark Web Gang that Kidnapped a Model*, DAILY BEAST (Aug. 7, 2017); Robert Siegel, *Investigators Use New Tool to Comb Deep Web for Human Traffickers*, NPR (July 6, 2015) ("In the deep and dark webs, there are ads for erotic services from sex workers who are victims of trafficking, of exploitation.").
[45] *See* Jeff Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 J. TECH. L. & POL'Y 123 (2010).

deciding if and how to change a law as important as Section 230, we need to have a thoughtful, spirited, and respectful dialogue.

The questions that are before you today are some of the most difficult and important technology policy issues that our nation confronts. Individual safety, free speech, privacy, and other fundamental rights and values are at stake. We must ensure that victims have meaningful remedies, bad actors face severe punishments, and the Internet remains free and open. And I believe that we can.