SESTA and the Teachings of Intermediary Liability

Draft - may be cited and circulated

Daphne Keller | November 2, 2017

The Center for
Internet and Society

SESTA and the Teachings of Intermediary Liability

Daphne Keller[1] */ Draft November 2, 2017 – may be cited and circulated*

[1] Daphne Keller is the director of Intermediary Liability at Stanford Law School's Center for Internet and Society, and previously was associate general counsel to Google. Stanford CIS funders, including Google, are listed https://cyberlaw.stanford.edu/about-us.

A. Introduction

Intermediary liability laws define Internet platforms' legal responsibilities for user generated content (UGC). They provide the legal backdrop for every story we read about Facebook and fake news or YouTube and copyright. We've had these laws only for a couple of decades, but the field is well-developed, because the Internet spawns a lot of litigation. Experience with intermediary liability to date provides important lessons about how laws affect the real-world behavior of Online Service Providers (OSPs). That behavior increasingly shapes our world – including our elections, our economy, and our private lives – today. Getting the governing law right is hugely important.

This short essay reviews basics of intermediary liability – things I teach on day one to my classes at Stanford and Berkeley. It compares existing laws to a bill currently pending in the Senate: SESTA, or the Stop Enabling Sex Traffickers Act. As the name suggests, SESTA addresses a genuine problem. Its core goal – getting sex traffickers off the Internet – is one that everyone shares. And the law is motivated by a particularly appalling website, Backpage.com, which is said to have deliberately enabled sex trafficking. SESTA changes a 1996 US Internet law, the Communications Decency Act Section 230 (CDA 230), authorizing new claims against any OSP that "should have known" about traffickers using its services.

1. SESTA's Problems

SESTA makes bad policy choices. It would give OSPs reason to remove lawful speech in some cases, and turn a blind eye to illegal and dangerous activity in others. That outcome – unnecessarily chilling lawful speech without effectively achieving Congress's valid goals – will make the law vulnerable to First Amendment challenges. SESTA is also remarkably badly drafted.[2] Lawyers who have worked on it for months can't agree on what its snarl of cross-referenced provisions actually means. Each side thinks the other is being disingenuous. But the bill is incredibly hard to parse, so the disagreements may be sincere. If those of us scrutinizing the bill's every word don't know what it means, OSPs operating under it would fare no better. Between bad choices and bad drafting,

[2] My attempt to parse its language is at http://cyberlaw.stanford.edu/blog/2017/08/what-does-new-cda-buster-legislation-actually-say.

SESTA would at best do unnecessary collateral damage – and at worst hinder rather than strengthen the fight against sex trafficking.[3]

SESTA wouldn't just affect a few bad actors like Backpage, or a few household-name megacorporations like Google or Amazon. Instead, it would create risk and uncertainty for untold numbers of American companies offering intermediary services in good faith.[4] These include anything from a news channel's online comments section to a coffee shop's wi-fi service. By changing OSPs' behavior, SESTA would also affect individuals and businesses that depend on the Internet – the new mom texting baby pictures to her family; the small-town mechanic attracting customers through online ads; the seamstress selling clothes on Etsy; the band promoting shows on Facebook; and more.

2. SESTA's Real World Consequences and Policy Challenges

The issue with SESTA is not that innocent OSPs would unwittingly violate it. The bill's proponents are right to say that normal OSP operations would remain legal. The problem is that legal uncertainty about SESTA, plus OSPs' strong incentives to avoid legal risk, will drive real-world outcomes when OSPs suspect or see allegations that a user is involved in sex trafficking. The same uncertainty will make them likelier to settle meritless lawsuits, and will make new entrepreneurs and investors less likely to build new platforms to compete against today's tech giants.[5] In short, SESTA's harms come from its highly foreseeable chilling effects.

---

[3] There are two reasons for this. First, as discussed below, SESTA would incentivize some OSPs to turn a blind eye to trafficking. Second, and beyond the scope of this essay, some trafficking experts argue that the existence of online forums like Backpage actually aids law enforcement in apprehending dangerous traffickers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2994114. A recent study released in draft form by economists in West Virginia and Texas also concluded that the launch of online sex listings on Craiglist correlated to a remarkable 17% drop in murder rate for women overall. http://gregoryjdeangelo.com/workingpapers/Craigslist5.0.pdf.

[4] A figure in the hundreds of thousands would be conservative. That number counts companies with registered agents under the DMCA. But small or under-lawyered OSPs are unlikely to register, and some categories are not required to under the DMCA.

[5] Venture capitalists shared these reservations in this study: http://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

Like all laws that regulate expression, SESTA needs to strike a difficult balance: deterring unlawful activity on the one hand without unnecessarily suppressing lawful speech on the other. The traditional way to do this is by placing legal responsibility on the speaker or publisher. That makes sense for a number of reasons. Among other things, these are the entities with the best information (knowing whether an allegedly defamatory claim is true, for example) and the right motivations (speakers usually care about their own speech rights).

Intermediary liability laws shift this, holding OSPs accountable for other people's speech. Sometimes that's a good idea. The OSP may be the only actor with a practical ability to stop the spread of dangerous and illegal material in some cases. But OSPs are, in some very real ways, not the same as speakers. They process enormous amounts of information without knowing what it says, for one thing. If they do become aware of a particular post, video, or message, they are unlikely to have enough information to judge its legality very well.[6] And in most cases they have little motivation to undertake that assessment. Simply silencing the speaker is cheaper and easier.

These differences in motivation and capacity to assess speech mean that laws devised with speakers or publishers in mind can be a misfit when applied to OSPs. Intermediary liability laws are more successful – meaning that they get more illegal content down, and keep more legal speech up – if lawmakers recognize the ways that OSPs differ from speakers, and tailor the laws accordingly.

It's also important for intermediary liability law to correct for OSPs' natural incentives to play it safe by removing lawful speech. OSPs receive reams of mistaken and false accusations – often from people or organizations trying to silence their critics. False copyright claims have been used, for example, to get criticism of of the Ecuadorian government and videos of police brutality taken offline. False claims are also driven by monetary interest. An early study of removal requests that Google received under the Digital Millennium Copyright Act (DMCA) found that over half appeared to come from

[6] Some of today's major, sophisticated platforms use algorithms to sort users' posts or target content like ads. But as anyone annoyed with their Facebook feed or haunted by irrelevant online ads knows, this is a very crude proxy for human judgment.

competitors targeting each other's sites.[7] Research consistently shows that platforms err on the side of honoring such requests.[8] Erasing legal user speech is cheap. Defending it, or even paying lawyers to decide if it's legal, is expensive. Smaller OSPs in particular typically lack the resources to look carefully and only honor the legitimate requests. The result is that legitimate speech disappears from the Internet.

There are no perfect intermediary liability laws. OSPs will never be a substitute for courts and due process in resolving disputes over speech. Both claimants and online speakers will sometimes suffer unfair outcomes. When Congress considers a difficult balance of this sort – in which error on one side will harm speech – the First Amendment shapes its choices. OSPs are not state actors, but that doesn't make the Constitution irrelevant when OSPs act based on an actual or perceived legal obligation. The Supreme Court has repeatedly used the First Amendment to invalidate or limit laws that cause one private actor to silence another's speech.[9] A key issue in those cases, and in any First Amendment case, is whether Congress could achieve its goals by other means without as much collateral damage to speech. That will be the question in the inevitable legal challenge to SESTA, if it becomes law.

Experience with existing intermediary liability laws tells us that better options do exist. I study these laws at Stanford, and regularly talk to small platform operators, public interest advocates, and policymakers about what is and is not working. I also worked in-house at Google for years, and saw the nuts and bolts of content notice-and-takedown under different legal regimes around the world. Comparison suggests that there are better and worse rules for regulating online content. We should expect better outcomes if OSPs can claim immunity by following clear operational steps under bright-line rules, with ample public transparency. We should expect worse ones if OSPs are charged with adjudicating difficult and nuanced questions about users' speech through unaccountable

[7] Urban and Quilter (2006).
[8] http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.
[9] The Court has invalidated over-broad criminal law that led private bookstores to suppress legal books in Bantam Books and civil law that would unduly chill speech in Times v. Sullivan. A lower court ruled against an over-reaching content removal obligation for ISPs in CDT v. Pappert.

private processes. Congress should know this, and consider the lessons of other intermediary liability laws in drafting SESTA.

Section I of this essay lists some key provisions that could make SESTA better. Section II goes through a taxonomy of known IL laws that undergird these recommendations. My suggestions here are nothing very novel – they track longstanding proposals from public interest groups around the world, including those in the Manila Principles, a widely endorsed "gold standard" intermediary liability model.[10]

As our lives move more and more online, the laws governing internet intermediaries will matter more. That makes getting intermediary liability law right very important. And it makes legislation like SESTA dangerous.

B. Building a Better SESTA

A more functional version of SESTA would look something like the following. This takes as a given Congress's decision to rely on a privately operated notice-and-takedown system, as opposed to public mechanisms such as court or administrative adjudication, to tackle online sex trafficking. As will be discussed below, private notice-and-takedown is most justifiable for content that is dangerous and easy for non-experts to identify.[11] But for any content, bad faith accusations will be common – and risk-averse OSPs will be motivated to comply with them. That makes substantive and procedural rules like these critical if intermediary liability law is to serve its core purposes: getting illegal material offline, and leaving lawful material intact.

- Platforms that are too engaged with user content should not be eligible for immunity. CDA 230 already contains a version of this rule, withholding immunity if an OSP is "responsible, in whole or in part, for the creation or development of information." Many people believe this standard is, if properly interpreted, adequate to hold both Backpage and potential future bad actors to account.

[10] https://www.manilaprinciples.org.
[11] Section C.4.b.

- If an OSP knows content is illegal, it should have to take the content down in order to benefit from immunity. "Knowledge" of illegality should be defined in terms that track existing intermediary liability laws – for example, saying that an OSP has knowledge if the content would appear "obviously illegal to a reasonable person." Provisions of this sort can be found in 17 USC 512 and interpreting case law.

- Notice-and-takedown processes for platforms wishing to claim immunity should be very clearly defined, and provide at a minimum the same standards that exist in 17 USC 512. This includes things like clear definitions of what information claimants must include in notices, penalties for bad faith accusers, and requirements for OSPs to terminate repeat infringers.

- The law should spell out that OSPs do not have to proactively monitor UGC. Both 17 USC 512 and 18 USC 2258A contain language of this sort.

- The law should clearly preserve the CDA's "good Samaritan" clause (47 USC 230(c)(2)), so that OSPs do not face legal disincentives to weed out bad content.

- SESTA should clearly exclude technical infrastructure providers like ISPs from its requirements, permitting them to operate as de facto common carriers. Both the 17 USC 512 and 18 USC 2258A contain relevant language.

- The law should encourage, and possibly require, public transparency about its consequences for online information. Either OSPs or government agencies involved in the notice-and-takedown process should disclose this information. Existing company transparency reports provide possible models for doing so.

An imperfect shorthand way to do this would be to heavily rely on existing language and standards from the DMCA. People who deal with the DMCA – on both sides – would probably hate that idea, but it provides a much better starting point than SESTA.

C. Taxonomy of Intermediary Liability Laws

At a high level, real-world intermediary liability laws generally have a lot in common. As a core principle, they offer immunity only to platforms with a sufficiently hands-off relationship to user content. Extensive US precedent probes the boundary between immunized and non-immunized behavior under one standard in the CDA, and an

alternative one in the DMCA.[12] Second, platforms that know (or, in some cases, should know) about illegal content have to take it down.

There are only a few basic models for doing this. They all have strengths and weaknesses. It's important to know what those are before legislating.

1. The Current Law: CDA 230

CDA 230 immunizes platforms for most legal claims, except under federal criminal law, intellectual property law, and ECPA. Congress passed CDA 230 in 1996 with stated goals that included promoting Internet development and encouraging OSPs to do what they could to weed out harmful or offensive content.[13] They were responding to problems that arose when courts tried to assess OSPs under existing law – more on that below.

CDA 230 covers OSPs broadly, from cable and wi-fi services to websites, apps, and social media platforms. It provides immunity as long as the OSP is not wholly or partly responsible for the creation or development of content.[14] The exact meaning of this standard is – of course – disputed in the case law. For Backpage, courts initially granted immunity under CDA 230, but as more facts have come to light the legal and opinions of many experts have turned against them. A few weeks ago, for example, plaintiffs reached an undisclosed settlement figure after the Washington State Supreme Court held that CDA 230 did not immunize them. And there are some signs that DOJ may soon finally use the expanded prosecutorial powers Congress created in different anti-Backpage legislation two years ago.

The other key provision in CDA 230, the "Good Samaritan" rule, says that platforms can't be sued for removing content in an effort to weed out inappropriate material. When

[12] In DMCA cases, the question is framed as whether the OSP falls within one of the four defined safe harbors at 512(a)-(d), and whether it has the right and ability to control activity from which it derives a direct financial benefit.
[13] 47 USC 230(b).
[14] 47 USC 230(f)(3).

Twitter or YouTube enforce policies against things like racist speech, this is a key law they are relying on.

2. The Worst Law: Strict Liability

The most extreme intermediary liability regime would be one of strict liability – holding platforms liable for any illegal content posted by users, whether or not the platform knew about it. Academics toy with this idea sometimes, but I've never seen a real-world legislature deliberately enact it for OSPs.[15] That's partly because it could make any intermediary business – from telcos to app developers– economically non-viable from day one. A fledgling business could be wiped out if just a handful of its users shared pirated songs,[16] or posted the wrong video of Hulk Hogan.[17] No country with any sort of tech economy wants that. China, for example, enforces notice-and-takedown standards – not strict liability – for tort, intellectual property, and terrorism laws.

Strict liability regimes would also drive platforms to seriously curtail online expression and information access. The best ways to avoid liability would be by aggressively policing users' speech or retreating to 1990s style "walled gardens," in which users see only selected, curated content. That would hurt Internet users' rights to speak and access information online – as several courts around the world have held in rejecting strict liability for OSPs. Courts including the European Court of Human Rights and the Supreme Courts of India and Argentina have rejected legal interpretations that would have effectively required platforms to monitor all user communications, saying they violated constitutional free expression guarantees.[18] US courts have mostly not had to wrangle with questions about users' speech rights and OSP takedowns, because statutory rules under the DMCA and CDA largely occupy the field. When given the

[15] Lichtman & Posner; see also Lemley.
[16] Copyright damages under 17 USC 504 can be as high as $150,000 per work.
[17] Bollea v. Gawker.
[18] Shreya Singhal (India), Belen-Rodriguez (Argentina), MTE (ECtHR); see generally http://cyberlaw.stanford.edu/blog/2016/04/new-intermediary-liability-cases-european-court-human-rights-what-will-they-mean-real.

chance, however, they have strongly warned against the over-removal problem that would arise from broad liability provisions.[19]

3. The Second-Worst Law: Treating Platforms Like Publishers (aka No One Knows What the Law Is)

Many countries around the world apply traditional tort and criminal law to OSPs, usually because legislatures haven't yet passed Internet-specific laws. Applying the laws designed for individual speakers, publishers, or traditional media distributors to companies that automatically process massive quantities of third party speech is usually hard. It is far from clear how centuries-old doctrines should apply to OSPs.[20] Courts and academics struggle with this question – and, tellingly, reach widely divergent conclusions.[21] Platforms don't know the answers either, and can't find out until one of them gambles on litigation. Legal uncertainty encourages over-removal, along with its other obvious downsides for investment and innovation.[22]

Experience also suggests that for OSPs, traditional laws often don't motivate the behavior lawmakers want. Instead, statutory and common law doctrines in areas such as defamation and privacy push platforms toward one of two extremes: taking down too much online content, or taking down too little. The reasons for risk-averse platforms to take down too much are obvious. The reasons to take down too little are pretty simple as well. Platforms rightly fear that assuming *some* responsibility for online content will leave them liable for all of it. A platform that tries to eliminate illegal or offensive content will inevitably fail in some cases. But their very effort will support arguments that the platform "acted like an editor" or "should have known" about the bad content that it missed. Even

[19] Cubby v. Compuserve, Zeran v. AOL, CDT v. Pappert.
[20] See discussion Cubby at 139.
https://law.justia.com/cases/federal/district-courts/FSupp/776/135/2340509/
[21] Lessig, Easterbrook, Crooks v. Wikimedia (hyperlinks do not constitute "publication" and thus are not defamatory in Canada), Duffy v. Google (hyperlinks can be defamatory in Australia).
[22] http://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

where a platform acted reasonably, defending its actions is risky and expensive – and protracted litigation, or numerous suits, can derail or bankrupt the company.[23]

The perverse result is that platforms may *want* to take down bad content, but conclude that the law gives them reasons to bury their heads in the sand instead. This is the bind that many European platforms find themselves in now: taking down offensive content makes good business sense, but European lawyers warn that it's legally risky.[24] It's also what used to happen in the US. When Congress passed CDA 230, it was specifically trying to remove these perverse incentives. They were inspired by two real life cases against 1990s platforms. One, Prodigy, enforced content guidelines by removing user posts from its bulletin boards. The other, CompuServe, didn't. Both were sued for defamation. CompuServe successfully defended its case, but Prodigy lost – because its efforts to police speech made it look, to the court, like a publisher. Congress reformed US law on this point with CDA 230's "Good Samaritan" provision, ensuring that platforms can *try* to enforce speech policies without risking liability.

SESTA undoes this, putting platforms back in the murky world of unclear laws and perverse incentives.[25] That in itself is bad policy – as discussed below, if Congress wants content taken down, there are better ways to do it. If SESTA passes as currently drafted, real-world businesses will be back in the Internet of 1995: unsure of their obligations, and legally incentivized to avoid dealing with unlawful content at all.

4. OSP-Specific Notice-and-Takedown Laws

CDA-style immunity and traditional laws are not the only – or even the most common – model for intermediary liability. Longstanding laws, including the US's Digital Millennium Copyright Act (DMCA) and the EU's eCommerce Directive, offer an alternate approach. These laws immunize platforms unless they knowingly transmit illegal content.

---

[23] Veoh, for example, ultimately prevailed in DMCA litigation but went bankrupt in the process. UMG v. Veoh.

[24] See September 2017 EU Commission Communication, urging that this common interpretation be rejected. https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.

[25] SESTA will have this effect whether or not it revises the literal language of 230(c)(2), because new language about information the OSP "should have known" will change the way (c)(2) is interpreted by cautious OSPs and, perhaps, courts.

Platforms typically comply with these laws by operating some form of notice-and-takedown system for online content. Such systems are notoriously flawed. On one hand, as discussed above, they are vulnerable to abuse by people trying to game the system and silence lawful speech – and abuse of this sort is both rampant and successful. Legitimate claimants who use these systems to enforce their rights don't like them either. US copyright holders complain that content they take down quickly pops up again, for example.

In other words, like the other systems discussed, OSP-specific notice-and-takedown laws *also* fail, in predictable ways, at intermediary liability's core goals. Too much legal speech disappears, and too much illegal material stays up. But there is reason to believe that well-structured notice-and-takedown laws fail a little less – and certainly less than SESTA would. Key aspects of these laws include the definition of OSP "knowledge," the designation of a legal decision-maker, and the selection of OSPs covered by the law. Each is discussed below.

a. Defining "Knowledge"

For any intermediary liability law, a major drafting challenge lies in defining when a platform knows enough that it must take action. In most intermediary liability laws, including the DMCA and eCommerce Directive, this is defined as a question of "knowledge." Courts have had twenty years of experience in applying this standard to real-world facts of OSP operation. For example, they have wrangled with the relevance of various communications or items of UGC seen by executives, employees, and volunteer platform moderators; and considered the level of legal expertise that should be expected of such individuals.[26] They have arrived at useful formulations to define "knowledge" in ways that avoid the extremes: requiring such a high degree of certainty that OSPs effectively never have "knowledge," or requiring so little certainty that they will take down anything. For example, one court in a copyright case recently said that

[26] Capitol Records v. Vimeo (2nd Cir. June 2016); UMG v. Veoh (9th Cir. 2013); Viacom v. YouTube (2nd Cir. 2012).

platforms "know" they must take content down when its illegality is "immediately apparent to a non-expert."[27]

SESTA also uses the word "knowledge" – repeatedly – but embeds it in such a thicket of other terms that its meaning becomes unclear. The law would be better – more effective in taking down the bad and leaving up the good – if it tracked definitions and precedent developed in existing law.

b. Decision-Making Process

Another key issue for intermediary liability laws is who decides whether speech is unlawful, and how they decide it. Different rules lead to very different likely outcomes. For laws that, like SESTA, put decision-making entirely in the hands of private platforms, clear procedural rules and transparency can greatly improve the odds that an OSP will correctly differentiate between lawful and unlawful content.

1. The "Court Order Standard"

The most speech-protective standard is that courts, and not private technology companies, should be the ones to adjudicate whether an individual's speech violates the law. This rule is widely endorsed in human rights literature as a means of protecting Internet users' rights against the improper exercise of private power. Laws establishing this standard, and clarifying that a mere allegation cannot make an OSP liable for a user's speech, exist in some form in a handful of countries.[28]

2. Other Procedural Rules

When the law does put OSPs in the shoes of judges "adjudicating" speech, logistical and operational rules are important. Procedural protections for the parties involved in

[27] Mavrix v. LiveJournal (9th Cir. April 2017). US law on point almost invariably involves copyright, because the DMCA is our major notice-and-takedown regime. Other countries that apply notice-and-takedown to other claims have also reached useful conclusions.
[28] Argentina, Brazil, Chile, Spain.

platforms' privately operated notice-and-takedown systems can, like civil and criminal procedure rules in courts, lead to more just outcomes. The DMCA has provisions like this, as do some other national laws outside the US. A broad menu of possible rules, too long to replicate here, can be found in the Manila Principles. As examples:

- Rules can protect speakers who are the victims of false or mistaken allegations. For example, when an Internet user's speech is removed under a notice-and-takedown law, he or she should have an opportunity to refute the allegation – and recover damages if the accuser acted in bad faith. Public transparency can also protect speakers by allowing researchers to identify removal problems. A transparency model for specific cases exists in Harvard Law School's Lumen database; aggregate reporting models can be found in company transparency reports.

- Rules can protect the claimant. For example, they can require OSPs to provide easily accessible forms to submit notices or require OSPs to terminate accounts of users who repeatedly violate laws.

- Rules can protect the OSP by streamlining procedures and reducing uncertainty about what to do, when. For example, claimants alleging that online content violates the law should have to provide some basic level of information to the service provider – most importantly, the URL or other precise location of the content.

Without these kinds of procedural protections, SESTA tilts the playing field against online speakers, incentivizing OSPs to take speech down just to be safe. At the same time, it creates unnecessary complexity and barriers to good outcomes for both OSPs and trafficking victims themselves.

3. Rapid Removal for "Worst of the Worst" Content

As a warning, this section discusses some of the worst material on the Internet. Thinking carefully and analytically about it isn't pleasant. It's upsetting enough that most platforms provide, and all of them should provide, counseling and support for the employees who must review and apply legal standards to material such as Child Sex Abuse Images (CSAI).

Every legal system I am aware of requires platforms to remove CSAI first, and ask questions later if at all. In the US, the federal criminal code includes OSP-specific provisions such as reporting requirements, and immunizes OSPs from claims arising from that reporting.[29] It also specifies that the law does not require OSPs to monitor user speech.[30] CDA 230 does not affect these existing obligations, because they arise from federal criminal law.

To my knowledge, little case law or literature discusses what makes particular content bad enough to warrant instant erasure with no procedural protections for speakers.[31] As a practical matter though, two key characteristics stand out. First, this is content that poses a very serious threat. Second, it is very easy to identify. Anyone, including platforms, can "know it when they see it."

SESTA effectively says that sex trafficking content belongs in this "worst of the worst" category, alongside child pornography. As a result OSPs would remove it with no hesitation or procedural constraints. Putting sex trafficking content in this category clearly meets the first, "danger" criterion. There are few graver or more imminent dangers than the ongoing sexual exploitation of vulnerable and underage people.

The second, "know it when they see it" criterion is harder. For child pornography images, nearly everything a legal decision-maker needs to know is on the screen in front of them.[32] Content promoting sex trafficking is different. It requires the reviewer to draw

---

[29] 18 USC 2258B (immunity for claims based on reporting by "electronic communication service provider, remote computing service provider, or domain name registrar under this section").

[30] 18 USC 2258A(f):

> Protection of Privacy.—Nothing in this section shall be construed to require an electronic communication service provider or a remote computing service provider to—
> (1) monitor any user, subscriber, or customer of that provider;
> (2) monitor the content of any communication of any person described in paragraph (1); or
> (3) affirmatively seek facts or circumstances described in sections (a) and (b).

[31] First Amendment case law on unprotected content, such as obscenity, would be highly relevant.

[32] As someone who has done this work, the main judgment calls I am aware of are (1) guessing the age of an individual depicted, and (2) determining whether a nude image is "sexually explicit conduct" under 18 USC 2256. An error on this second consideration presumably led to Facebook's widely-reported removal of the iconic Vietnam War photo of a young girl after a napalm attack.

conclusions about real-world, off-screen behavior based on online speech. Sometimes that will be easy; other times it will be very hard – for example, because of ambiguous language.[33] The other important distinction is that discussions of sex trafficking, unlike child pornography, can be legal or illegal depending on the context. Identical words or images can have entirely different significance in different places. For example, the codewords used in online sex advertisements to describe underage or trafficked victims are also used in news reporting and educational materials to *prevent* trafficking.[34] Phrases like "Lolita" or "new," and even exact replication of real world ads, can be both legal and important in this context. The distinction between always-illegal child pornography content and other sometimes-illegal content is especially important when OSPs are asked to apply filters or other automated analysis to online speech.

The greater difficulty in identifying sex trafficking content means that removal errors are more likely. Protections such as procedural limitations for the specific situation of OSPs seem logically *more* important than they are for CSAI, which is uniquely recognizable and illegal in every situation. Yet SESTA reverses this – providing even fewer protections against false allegations and wrongful removals.

c. Distinguishing Between Kinds of Intermediaries

[33] See, e.g., Pizzagate – in which Internet users became convinced that a discussion of pizza was code for child trafficking. If they asked an Internet host to take down the leaked email on that basis, what would be the normatively right result? This example is complex in part because of honest disagreement about the meaning of words used – if claimants told an OSP that "cheese pizza" was a code word, what research efforts would the OSP undertake before deciding whether that was correct? It is also a hard case because many online copies of the allegedly trafficking-related message appeared in the context of honest, if mistaken, efforts to disclose and prevent trafficking. Moreover, had the allegations about the email been correct, the email itself would have been important to news reporting about a public figure.

[34] http://mnhttf.org/site/wp-content/uploads/2013/10/Sex-Trafficking-Terminology-RCAO.pdf (County attorney discussing term "special" in online advertising); https://readwrite.com/2010/08/11/craigslist_says_no_increase_in_reported_violations/ (article discussing "good time" generally and "fresh" or "new" for underage trafficking); http://inpublicsafety.com/2014/07/know-the-language-of-human-trafficking-a-glossary-of-sex-trafficking-terms/ (glossary of trafficking terminology); https://www.nytimes.com/2017/03/11/us/backpage-ads-sex-trafficking.html (discussing terms "new in town" and "100% young"); http://www.sandiegouniontribune.com/business/technology/sd-fi-emojis-trafficking-20170526-story.html (discussing emoji).

Distinct kinds of intermediaries work very differently. There are huge variations between the daily operations of an ISP, for example, versus a user-facing content platform like Facebook or YouTube. Part of the appeal of a platform like Facebook is that it makes judgments about user content – by directing employees to identify and take down bullying or racist speech, for example, or by algorithmically suggesting posts users might like. The function and value proposition of technical infrastructure providers – from mobile carriers to domain name registrars – is very different. Few people want Verizon to pick what inbound texts they receive, or to block particular webpages from loading on smartphones. These OSPs are most valuable when they stay out of the content regulation business. But SESTA doesn't carve them out. It is hard to even predict what SESTA would require these entities to do when they receive allegations of online trafficking.

More carefully drafted laws, like the DMCA and the EU eCommerce Directive, distinguish between different kinds of intermediaries.[35] Obligations like notice-and-takedown generally don't apply to ISPs, for example. And other laws, like those relating to network neutrality, *do* apply to ISPs and limit their ability to intervene in content and speech. I've seen no indication that changing law in this area is the sponsors' intent. So, if the Senate proceeds with SESTA, it should revise it to recognize technical differences between OSPs, and define their legal obligations accordingly.

D. Conclusion

It is possible to draft a version of SESTA that comes far closer to achieving Congress's goals, and that poses less of a burden to lawful speech. To do that, Congress should consider legal precedent and real-world experience under intermediary liability laws, and model SESTA on the approaches that have worked best in getting unlawful content off the Internet, and keeping lawful speech protected.

[35] 17 USC 512; eCommerce Directive Arts. 12-14. US CSAI law uses terminology drawn in part from ECPA for this purpose. 18 USC 2258B.

About the Author

Daphne Keller studies the ways that Internet content platforms – and the laws governing them -- shape information access and other rights of ordinary Internet users. As the Director of Intermediary Liability at the Stanford Center for Internet and Society, she has written and spoken widely about the Right to Be Forgotten, copyright notice-and-takedown systems, cross-border content removal orders, platforms' own discretionary content-removal decisions, and more. She has testified on these topics before legislatures, courts, and regulatory bodies around the world. In her previous role as Associate General Counsel at Google, Daphne worked on cases including Viacom, Perfect 10, Equustek, Mosley, and Metropolitan Schools; and was the primary counsel for products ranging from Web Search to the Chrome browser. Daphne has taught Internet law at Stanford, Berkeley, and Duke law schools. She is a graduate of Yale Law School and Brown University, and mother to some awesome kids in San Francisco

About the Center for Internet and Society

The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. CIS also sponsors a range of public events including a speakers series, conferences and workshops. CIS was founded by Lawrence Lessig in 2000.