House of Representatives Judiciary Committee
Subcommittee on Crime, Terrorism, Homeland Security and Investigations
October 3, 2017 Hearing
"Online Sex Trafficking and the Communications Decency Act"

Written Remarks of Evan Engstrom, Executive Director, Engine

Chairman Sensenbrenner, Ranking Member Jackson-Lee, and members of the Committee, thank you for inviting me to testify. My name is Evan Engstrom and I am the Executive Director of Engine. Engine is a non-profit advocacy and research organization that works with government and a community of startups throughout the country to develop public policies that foster innovation, entrepreneurship, and job creation.

I am grateful for the opportunity to testify on such an important and difficult topic, and I appreciate the hard work that Congress has put into fighting the scourge of sex trafficking. I cannot claim to be an expert on sex trafficking, and I certainly cannot ever comprehend the horrors that trafficking victims have endured. I am here only to present the perspective of how some of the proposed solutions to this problem may impact the startup ecosystem in unintended ways. But in my capacity as an advocate for innovators and entrepreneurs, the most important thing I can say at the outset is that the community of startups we work with is fully committed to finding solutions to the problem of online sex trafficking, through a combination of industry initiatives and governmental action. While we have concerns about the unforeseen harms that recent legislative efforts to address this critical issue may cause, we are eager to work with this Committee to craft policies that will help identify and prosecute sex traffickers.

The particular concerns we have about the latest efforts to combat online sex trafficking relate to the unintended consequences that may arise through proposed amendments to Title 18 of the United States Code and Section 230 of the Communications Decency Act. As I am sure anyone following this issue has heard countless times, we simply would not have the Internet or the startup community we have today without Section 230. Section 230 shields websites from liability for user generated speech and gives platforms breathing room to find and remove objectionable content without fear of legal consequences. For a startup, Section 230 guarantees that a website that gives users a forum to express themselves freely will not face ruinous legal liability whenever a bad actor says something illegal on its platform. This has allowed tens of thousands of startups[1] to build online platforms where users can create, post, and share media of all kinds.

[1] While it is impossible to get a full accounting of all the platforms that depend on Section 230, there are more than 115,000 companies in the Copyright Office's database of registered Digital Millennium Copyright Act agents. Each of these companies also depends on the protections of Section 230.

Section 230's protections are critical because, despite the best efforts of honest, law abiding startups, it is impossible to fully stop bad actors from doing bad things online. But that doesn't mean we should not try. This, after all, is what startups do: fix what needs fixing and find new solutions to difficult problems. But changes to existing law should be carefully tailored to address the problem of sex trafficking in the most effective manner possible while minimizing the negative impact on the broader Internet ecosystem of law abiding startups and users. We agree that bad actors like Backpage.com must be held accountable for their role in facilitating human trafficking. We hope to work together to combat trafficking and want to see justice for the victims of this terrible crime.

In my testimony, I will discuss the importance of Section 230, outline the steps startups are taking to address sex trafficking online, and attempt to identify the unintended consequences and negative impacts that may arise if changes to Section 230 are designed without appropriate precision and consideration.

Startups and Section 230

In just a few decades, the Internet has quickly become the most powerful medium for expression, communication, and commerce in history. The power of the Internet stems from its ability to facilitate near instantaneous communication between any connected points on the globe. This ubiquity and efficiency has effectively created a seamless global market. Critically, because advances in technology continue to drive down the cost of operating an Internet platform,[2] small entrepreneurs have been able to take a leading role in the Internet economy. Today, anyone with a good idea, some technical skills, and an Internet connection can start up a company that can compete with Fortune 500 firms. Indeed, research shows that startups are responsible for all new net job growth in the United States.[3] None of this would have happened without some very thoughtful decisions by policymakers at the beginning of the Internet's rise. Section 230 is perhaps the most important of these decisions.

What 230 Does

In 1996, Congress enacted Section 230 in order "to promote the continued development of the Internet" by limiting secondary liability for Internet platforms. Congress recognized that subjecting platforms to legal liability for user behavior would be unfair and inefficient in many circumstances because it is impossible for any platform to fully know, much less control, what users do on its site. To prevent this, Congress established in Section 230 that websites that do not participate in the creation or development of their users' statements cannot be held legally

[2] From 2000 to 2011, the cost of running a basic Internet application fell from $150,000 a month to $1,500 a month. Marc Andreessen, "Why Software Is Eating The World," *The Wall Street Journal*, (Aug. 20, 2011), available at http://on.wsj.com/1gt4wRH.

[3] Ian Hathaway "Tech Starts: High-Technology Business Formation and Job Creation in the United States," *Kauffman Foundation Research Series: Firm Formation and Economic Growth*, (Aug. 2013), available at http://www.kauffman.org/~/media/kauffman_org/research reports and covers/2013/08/bdstechstartsreport.pdf.

liable for those statements. This may seem like a relatively minor rule, but its implications are massive. Without Section 230, any website that hosts user content would be at risk of ruinous legal liability any time a user posted something illegal.

Many of the startups we work with only exist thanks to the important protections they receive under Section 230, and those protections are a key reason that the United States has been home to the vast majority of top Internet companies. As the pace of innovation accelerates, Section 230 remains as important today as it did when it was passed two decades ago. While some large Internet companies may be in their teenage years, you only have to open your smartphone to see dozens of apps that were invented in the past few years. Startups less than five years old have reinvented the way we share photos, send money, date, order food, and rent our homes. All of these apps rely on user generated content, and Section 230 has facilitated their growth in multiple ways.

Section 230 establishes a uniform regulatory regime, rather than a 50 state patchwork.

One of the aims of Section 230 was to "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." By ensuring that secondary liability for most user speech is governed under a single federal standard, small platforms that lack significant legal resources can compete with well-financed incumbents that are better equipped to navigate fifty different legal codes. Because the Internet is a borderless medium, ill-advised regulations in a single state could have a disruptive impact on the global Internet ecosystem. Section 230 avoids this problem by exempting inconsistent state rules that would otherwise subject platforms to liability for user actions. For example, twenty four states have criminal defamation laws.[4] Even if a startup could navigate compliance with so many different legal standards, it would almost certainly get sued out of existence every time a user posted defamatory content on its site.

Section 230 Provides a Bar to Frivolous Litigation.

Section 230 was intended to ensure that litigation over Internet speech was directed at the speakers, not the platforms. As the Ninth Circuit has noted, without Section 230, websites would "face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties."[5] For vexatious plaintiffs, large companies represent deep pockets that are far more lucrative to sue than individual Internet users, and startups that cannot afford to fight off litigation are easy targets for nuisance value settlements.[6] Section 230's clear bar allows startups to defeat bad faith litigation

[4] Committee to Protect Journalists, "Criminal Defamation Laws in North America," available at https://cpj.org/x/6761.

[5] *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008).

[6] This Committee has examined this type of behavior in the context of patent litigation. Bad actors try to extract quick settlements from startups and small businesses because they are financially incapable of fight back.

at an early stage without having to incur exorbitant legal fees. Since studies have shown that the average high-tech startup launches with around $70,000 in outside capital, having to defend against even a single meritless lawsuit can easily bankrupt a company.[7]

Section 230 Empowers Platforms to Proactively Monitor for Objectionable Content.

Section 230 has two main operative provisions. Section 230(c)(1) says websites are not liable for third party content, and Section 230(c)(2) says websites are not liable for taking steps to moderate content they consider offensive. This latter provision is known as the "Good Samaritan" rule, and it allows platforms to remove offensive, lewd, and violent content from their sites without fear of being held liable for doing so. Because of Section 230, online services today voluntarily take many steps to suppress socially harmful content without fear of liability for the content they might miss. While the "Good Samaritan" rule has been criticized for failing to sufficiently protect platforms from bad faith litigation,[8] the principle that platforms should be free to undertake voluntary initiatives to monitor their platforms is critical for fighting bad actors online.

What Section 230 Does NOT Do

Section 230 is frequently and incorrectly described as a type of "blanket immunity" for platforms. Quite the opposite, Section 230's protections are limited in two critically important ways.

Section 230 Does NOT Prevent the Department of Justice from Prosecuting Violations of Federal Criminal Law.

Section 230 provides absolutely no immunity for violations of federal criminal law.[9] The Department of Justice has the full authority to investigate and prosecute any platform that violates a federal trafficking statute. Under 18 U.S.C. § 1591, any website that "benefits, financially or by receiving anything of value, from participation" in a trafficking venture by one of its users can—and should—face criminal liability with no limitations under Section 230. Additionally, in 2015, Congress passed the Stop Advertising Victims of Exploitation Act, which created a new federal crime for publishing online ads that promote sex trafficking victims. Section 230 does not bar the DOJ from using either of these laws to prosecute wrongdoers like

---

[7] "The Capital Structure Decisions of New Firms," *Kauffman Foundation*, (Apr. 17, 2009), available at http://www.kauffman.org/what-we-do/research/kauffman-firm-survey-series/the-capital-structure-decisions -of-new-firms.

[8] *See, e.g.,* Eric Goldman, *Online User Account Termination and 47 U.S.C. §230(c)(2)*, 2 U.C. IRVINE L. REV. 659 (2012), available at https://ssrn.com/abstract=1934310.

[9] 47 U.S.C. § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.").

Backpage.com and a federal grand jury has already begun an investigation into those criminal activities.[10]

Section 230 Does NOT Protect a Platform from Liability If It Develops Illegal Content.

Section 230 does not apply to an Internet platform if it has itself created or developed content "in whole or in part."[11] That is, if a platform takes actions that sufficiently shape the content of user speech, it can be held liable for both civil and criminal violations related to that speech. In one prominent case, a website structured its user profiles and searches to require users to provide information in a manner that violated the Fair Housing Act.[12] Although the website was not the direct "speaker," the court held that it developed user speech in a manner that subjected it to liability notwithstanding Section 230's protections. In light of the damning Senate report detailing Backpage.com's practice of editing trafficking posts to avoid detection by law enforcement, it is all but certain that Backpage.com cannot claim Section 230's protections for its editorial practices.[13]

How Startups Fight Human Trafficking

Neither Engine nor the startups we work with are experts in combating human trafficking. In working on this issue, we have endeavored to learn from law enforcement and victims' advocates about how trafficking activity proliferates and how to protect our platforms from such abuse. Startups are finding ways that they can proactively fight online trafficking, and while there is a long way to go in developing industry strategies to combat trafficking, startups are already working on policies and tools to mitigate criminal activity on their platforms.

Efforts to Combat Trafficking

As a baseline, all of the startups we work with that host user generated content have zero-tolerance enforcement policies for trafficking content and direct personnel to promptly investigate and disable access to such content as soon as it is identified. This type of human review is costly and imperfect, but for startups, it is usually the most efficient and effective way to identify and remove the small subset of content that is trafficking-related. These companies

---

[10] Sarah Jarvis, et al., "As Allegations Increase Against Backpage, Founders Have Become Big Political Donors in Arizona," *AZCentral.com*, (Apr. 14, 2017), available at http://www.azcentral.com/story/news/local/phoenix/2017/04/14/allegations-increase-against-backpage-founders-have-become-big-political-donors-arizona/100421528/http://www.azcentral.com/story/news/local/phoenix/2017/04/14/allegations-increase-against-backpage-founders-have-become-big-political-donors-arizona/100421528/.

[11] 47 U.S.C. § 230(f)(3).

[12] *Roommates.com, LLC*, 521 F.3d 1157.

[13] Permanent Subcomm. on Investigations, U.S. Senate Comm. on Homeland Sec. & Gov't Affairs, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (2017), available at https://www.portman.senate.gov/public/index.cfm/files/serve?File_id=5D0C71AE-A090-4F30-A5F5-7CFFC08AFD48.

promptly alert law enforcement of potential trafficking, and law enforcement groups have frequently relied on this information to track down and arrest those responsible.

Tech companies have frequently partnered with outside groups including the National Center for Missing and Exploited Children to develop and deploy a range of technologies and business practices that help combat trafficking. Here are just a few of the many examples:

- Many startups implement Microsoft's PhotoDNA fingerprinting software. PhotoDNA is a content detection program that compares scanned photographs with an industry-wide shared database of images, to help identify and eradicate child exploitation content.[14]
- The Technology Coalition hosts multiple events each year for companies, including startups, to share best practices with NGOS. The Coalition focuses on sharing best practices, both technical and operational, on stopping child exploitation online. The Coalition also partners larger companies with startups to help mentor new companies.
- Large and small companies have teamed up with Facebook at three cross-industry child safety hackathon to develop tools and products that enhance child online safety. The conference included over 75 engineers as well as child safety NGOs.[15]
- A number of smaller companies, from Pinterest to Imgur to Tumblr, participate in the Thorn Technology Task Force, a group of companies that works with Thorn to develop and deploy technology, including facial recognition and big data analysis, to help combat online child exploitation.[16]
- Uber teamed up with UPS, Walmart, and Marriott to partner with the Ending Child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purposes campaign to adopt business principles that will help prevent human trafficking.[17]
- Twilio and Salesforce Foundation partnered with Polaris and the National Human Trafficking Resource Center to develop a quick and discreet way for victims to contact the NHTRC's help hotline.[18]

Limitations of Filtering Technology

While automated tools like these can be incredibly useful for addressing certain types of illegal content, it is important to recognize the inherent limitations of algorithmic content detection programs. Even as artificial intelligence and advanced analysis technologies like facial

---

[14] See Microsoft PhotoDNA, available at https://www.microsoft.com/en-us/PhotoDNA.
[15] Catherine Cheney, "How Technology Is Taking Down Human Trafficking," *Devex*, (Feb. 7, 2016), available at https://www.devex.com/news/how-technology-is-taking-down-human-trafficking-87658.
[16] See Thorn Technology Task Force, available at https://www.wearethorn.org/about-our-fight-against-sexual-exploitation-of-children/.
[17] Cassie Ann Hodges, "How Uber, UPS, Walmart, and Marriott Are Combating Human Trafficking," available at https://www.freeenterprise.com/uber-ups-walmart-marriott-combatting-human-trafficking/.
[18] Rebecca Sadwick, "7 Ways Technology is Fighting Trafficking," Forbes.com (Jan. 2016) available at https://www.forbes.com/sites/rebeccasadwick/2016/01/11/tech-fighting-human-trafficking/#5509f2c96cac

recognition[19] proliferate, automated tools can only identify content by examining the physical characteristics of particular media (e.g. image, sound, text, etc.) or its associated metadata (e.g. file name, size, posting time, etc.). They cannot perform the often nuanced analysis that is required to determine whether content actually violates the law. Some content, like child exploitation imagery, is usually facially illegal—there is simply no context that would make distributing pornographic images of children legal. In these circumstances, automated programs like PhotoDNA can go a long way to towards combatting illegal content, but even then, these programs have non-negligible error rates and only match files with a database of previously identified content. As trafficking advertisements are written in ever-changing code to evade detection, automated tools can identify terms and symbols that are commonly associated with trafficking posts, but cannot alone accurately separate legal content from illegal activity.

While startups have robust policies and tools to detect and remove trafficking content from their sites, it is impossible for a platform that hosts a significant amount of user generated content to ever fully remediate all illegal content on its site or know with certainty whether it is being used for trafficking activity. Proposals to address online trafficking should consider these realities and not impose impossible burdens on well-intentioned startups or discourage platforms from voluntarily taking on the task of monitoring their sites for trafficking content.

Startup Concerns with Proposed Legislation

While this is not a legislative hearing, I do want to briefly address our concerns with H.R. 1865, the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 and S. 1693, the Stop Enabling Sex Trafficking Act of 2017. Both bills have the laudable goal of holding Backpage.com accountable for their role in sex trafficking. In pursuing that goal, we believe that any amendments to Section 230 and Title 18 should be approached cautiously and with thorough deliberation. We are eager to participate in the process of finding appropriately tailored legislative solutions to fight the scourge of sex trafficking online. Indeed, we have been working with Senate sponsors on suggested amendments to S. 1693 that we believe would mitigate the concerns the startup community have had with these bills while still enhancing law enforcement's capacity to bring rogue actors like Backpage.com to justice. The problems we have identified with H.R. 1865 and S. 1693 are significant but not impossible to fix.

Risk of Inconsistent and Inappropriate State Criminal Laws

H.R. 1865 and S. 1693 seek to increase the pathways to prosecute Backpage.com and similar sites by exempting state criminal laws addressing sex trafficking from Section 230's protections. Under these proposals, not only could federal law enforcement agencies bring criminal claims against platforms, state Attorneys General and local district attorneys could prosecute websites for a wide range of new and potentially disruptive state law violations. This would create

[19] "Police can use this facial recognition technology to fight sex-trafficking," *Mashable*, (2017), available at http://mashable.com/2017/06/28/facial-recognition-child-sex-trafficking/#o8_T3aMVCSq8.

uncertainty for startups in the form of 51 different and likely inconsistent legal regimes they would have to navigate. Even more problematically, the legislation is worded broadly enough to allow states to pass and enforce laws that would massively disrupt the functioning of the Internet without any meaningful decrease in trafficking activity.

This is not just hyperbole. Under H.R. 1865 for example, a state could likely pass and enforce a law nominally intended to prevent sex trafficking that would require users to provide personal information to any user-generated content startups they visit and prosecute those startups if this user-supplied information is inaccurate. Since it is technologically impossible to accurately track or verify such user information, no startup could feasibly comply with such a law. While this example may seem far-fetched, it would not be much of a departure from state legislative practices. Right now, dozens of state legislatures are considering a law that would require device manufacturers to install non-existent "pornography filters" on all cell phones and computers.[20] Since this type of legislation is nominally meant to combat sex trafficking, it would conceivably fall within the exemptions created under recent legislative proposals and would be effectively impossible for startups to comply with.

We support the goal of enabling more law enforcement agencies to lock up criminal actors like Backpage.com. To accomplish this without subjecting startups to inconsistent state laws, Congress could amend Section 230 to only exempt state laws that mirror the federal sex trafficking statute, 18 U.S.C. § 1591. This proposal would increase law enforcement's capacity to prosecute Backpage.com without functionally changing Section 230's substantive provisions, since federal criminal laws have always been carved out of its protections.

Exposure to Bad Faith Litigation

H.R. 1865 and S. 1693 are particularly troubling to startups because they would remove Section 230's civil liability shield. Civil claims have never been exempted from Section 230's protections, as Congress was originally worried that many plaintiffs would try to bring lawsuits against platforms rather than the actual speakers, because platforms are usually easier to find and more lucrative to sue. Expanding liability and opening up the possibility of civil lawsuits against startups will encourage a barrage of frivolous litigation targeting platforms, as well as fishing expeditions searching for any evidence that might be used against them. For two decades, we have seen time and time again how perfectly legitimate online platforms have been targeted by meritless lawsuits. Section 230 has been an important wall of protection against such mistargeted legal action.

It is important that victims of sex trafficking are able to seek justice against the platforms who perpetrated these horrendous crimes. We are working to craft a more narrowly tailored approach than H.R. 1865 and S. 1693, including allowing civil cases to proceed against

[20] Dave Maas, "States Introduce Dubious Anti-Pornography Legislation to Ransom the Internet," *EFF Deeplinks Blog*, (Apr. 12, 2017), available at https://www.eff.org/deeplinks/2017/04/states-introduce-dubious-legislation-ransom-internet.

platforms that have been found criminally liable of a trafficking offenses and crafting pleading standards to make it harder for vexatious litigants to extort startups with meritless claims.

Impossible Burdens and Dangerous Disincentives from Changed Knowledge Standard

Both H.R. 1865 and S.1693 would change the definition of "participation in a venture" in 18 U.S.C. § 1591 in a manner that could unintentionally subject well-intentioned platforms to criminal liability. These provisions could end up disincentivizing platforms from engaging in proactive monitoring efforts. As currently drafted, this legislation could potentially subject platforms to liability for facilitating trafficking activity on their sites even if they do not have any actual knowledge that any trafficking is occurring. And, under H.R. 1865 and S. 1693, platforms could be held to have effective knowledge of trafficking activity merely because they engaged in proactive monitoring efforts to remove illicit content but failed to thoroughly identify and disable all such material. This approach would be counterproductive, disincentivizing platforms from undertaking good faith efforts to address illegal user behavior and directly undermining the sound logic of Section 230's "Good Samaritan" provision.

Congress could more accurately target bad actors by establishing that a platform can be liable for participating in a trafficking venture if it had actual knowledge that it was assisting, supporting, or facilitating a specific trafficking violation and clarifying that platforms are neither legally obligated to employ content moderation practices nor potentially liable for those content moderation practices. Congress should also consider creating a safe harbor regime that gives honest platforms some certainty about how to safely address trafficking activity that it may not be able to clearly identify. This would ensure that an honest platform cannot be held liable for trafficking content it had no knowledge of, and would encourage platforms to take good faith steps to address trafficking on their sites without subjecting them to impossible burdens.

Conclusion

We want to thank the Committee for holding a hearing on this important issue. Sex trafficking is a heinous crime, and platforms like Backpage.com must be held liable for facilitating criminals. Policymakers, prosecutors, and industry—including startups—must continue to work towards a solution to this multifaceted problem. As with all policy changes, there is a need to consider unintended consequences and mitigate potential harms. We hope that we have outlined the potential harms from the perspective of startups. On behalf of the startup community, we are eager to work with this Committee to craft balanced policies that will help identify and prosecute sex traffickers while also fostering the growth of startups nationwide.