

TechBriefing: CDA Section 230 & Immunity for Online Intermediaries

*An explanation of recent proposals to amend Section 230,
the legal and policy issues, and TechFreedom's recommendations.*

Summary

Under current law, when an Internet user distributes unlawful content on a third-party website, that website is generally immune from liability for the user's wrongdoing. Some state Attorneys General ("AGs") have recently suggested changing the law in order to impose state criminal liability on intermediaries.

Recommendations

- Congress should reject any amendments to the Communications Decency Act that create state criminal liability for online intermediaries.
- AGs should prosecute *users* for criminal activity, not the sites and services they use.
- Policymakers should ensure that both prosecutors and civil plaintiffs can unmask anonymous defendants, while still protecting Americans' rights to privacy and free speech.
- Reputation, competition for advertising dollars, and other factors already drive intermediaries to police user content; content control should be driven by competition as Congress intended.

Background

What is user-generated content? What are online intermediaries?

Today's Internet is a vibrant tapestry of user-generated content ("UGC"),¹ a term that includes user-contributions, or "posts," to question-answer databases, blogs, forums, consumer review websites (e.g., Yelp), social networks (e.g., Facebook), video hosting services (e.g., YouTube), as well as user messages or comments on mainstream media websites or e-commerce sites (e.g., Amazon). UGC can be text, photographs, videos, survey responses, and software. UGC distinguishes the Internet from previous mass communication mediums. Online, information consumers are also information producers. A plurality of viewpoints are available on any topic, barriers to contribution are near zero, and the diverse chorus of voices can generate or mash-up information and art that is far greater in quantity and quality than anything yet seen.

Online intermediaries are the businesses and organizations that host and deliver UGC online. These intermediaries include content platforms such as Wikipedia, Youtube, or a local blog; social networks such as Facebook or Twitter; search engines such as Google; and Internet service providers ("ISPs") such as wireless or cable companies.

What is CDA Section 230? What do some state AGs want changed?

Commonly referred to as the "Safe Harbor" provision of the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230 provides immunity to intermediaries from most legal liability for UGC (so-called "secondary" or "intermediary" liability). Here's how it works:

- Prior to Section 230, courts had begun extending traditional common law doctrines of secondary liability to online publishers:
 - This meant holding site publishers liable for UGC if they policed or edited user content, *but*

¹ Every *minute*, approximately 50,000 photos are uploaded to Facebook, 3,000 images are uploaded to Flickr, and 60 hours' worth of video is posted on YouTube. By the end of 2011, there were over 180,400,000 identified blogs online, and 90,000 new blogs were created daily. See <http://tch.fm/1ags34P>.

- *not* if publishers merely hosted and displayed it without curation.
 - Congress enacted Section 230 to remove this perverse incentive against intermediary policing of UGC on their sites/services.
- Under the CDA (Section 230 (e)(1)-(4)), intermediaries may be held liable for UGC only if the content violates *federal* criminal law, intellectual property law, or electronic communications privacy law.
 - Section 230 forbids states from enlarging intermediary liability beyond these federal laws. It preempts all "inconsistent" state law.

Several state AGs recently proposed an amendment that would allow criminal prosecution of companies and their executives for state laws broken by their users.

- The proposal would amend Section 230(e)(1) as follows: "Nothing in this section shall be construed to impair the enforcement of [specific provisions of Federal law] or any other Federal **or state** criminal statute."
- While possibly intended to thwart online prostitution ads, this would impose intermediary liability on *all intermediaries* for a host of state criminal laws, including (in most states) defamation.

Discussion

What are the benefits of Section 230 as it stands?

- ***Preserving a vibrant and diverse ecosystem of online services.*** Any website that allows for user interaction, from commenting to video uploading, is protected by Section 230. Holding such sites legally responsible for policing UGC wouldn't simply raise their costs: *the costs of monitoring the vast scale of UGC and the enormous potential legal liability involved would force many sites to close or heavily restrict interactive functionality.*
 - By protecting big and small websites alike, the CDA preserves a diverse mix of online voices, avoiding a world where the only speakers are those with pockets deep enough to lawyer-up.
- ***Enabling innovation.*** The CDA allows technology companies to generate wildly innovative and socially beneficial business models based on user contributions. For example,
 - User-edited Wikipedia has become the most comprehensive encyclopedia in the world,²
 - AirBnB has allowed individual contributors to list and rent apartments, reducing the price of lodging³ by making available surplus housing capacity that would otherwise sit unoccupied.
- ***Enabling free expression.*** The CDA immunizes ISPs from liability for the full range of online content they deliver to subscribers. Without these protections, broadband operators might feel the need to limit consumer access to a censored and sanitized world-wide web, for fear of delivering anything unlawful.

Would intermediary liability under state criminal law destroy those benefits?

Yes. Section 230 currently works because its simplicity allows compliance at relatively low costs. Intermediaries need *only* worry about liability under *federal laws*. Adding two words, "and state," may seem like a simple change, but its full implications would be disastrously complex:

1. ***Fear of criminal liability may drive intermediaries to remove UGC or limit UGC functionality.*** Civil liability leaves operators free to take reasonable risks in displaying UGC, based on the expected costs of a lawsuit. But fear of incarceration and the long-term, stigmatic consequences of an individual or corporate felony conviction may drive operators to drastically change their websites, removing or limiting components that solicit and display UGC.

² See <http://tch.fm/1agunJL>.

³ AirBnB apartment rentals cost, on average, 21.2% less than staying at a hotel: <http://tch.fm/1agv1X3>.

2. **Laws from one state may conflict with the laws of other states; compliance may become impossible.** State Legislators and AGs aren't elected (or appointed) to consider the interstate consequences of their actions. Empowering states to make laws applicable to any Internet service delivered within their borders will balkanize Internet law. Complying with the laws of New York may break compliance with the laws of California. Intermediaries will be forced to create unique versions of their service for every state or suffer the consequences of imperfect compliance, all at tremendous costs.
3. **Increasing costs will kill many sites or services, or force them to limit UGC functionality.** Many valuable online services operate with little or no profit margins. Even an incremental increase in costs from complying with various state laws could make provision of the service unfeasible. Websites may summarily remove UGC, stop hosting UGC or shut down altogether. This is especially true for smaller businesses, or nonprofits (e.g., Wikipedia). Reduced profits for larger companies may make free services (e.g., YouTube), difficult or impossible to provide.
4. **Some State AGs may unfairly target intermediaries for political gain.** In 43 states, AGs are elected politicians who have a natural incentive to grab headlines by pursuing bogus or trumped up charges against innocent but highly visible intermediaries. This is not just cynical speculation: even though Section 230 barred their state law claims legally, some AGs have already pressured intermediaries to change their UGC practices or reveal the identities of anonymous critics.⁴ Such political grandstanding would increase if Section 230 were amended.
5. **Liability under laws of all 50 states could create a race to the bottom.** Fear of criminal liability from any state may drive businesses to comply with laws from the one state with the strictest policies. Allowing a single state government to set the baseline for acceptable UGC across the entire Internet violates a basic principle of federalism: well-established "dormant commerce clause" jurisprudence bars states from regulating interstate commerce even where Congress has chosen not to do so.

What are the larger issues at stake?

- **Reduced Innovation.** If intermediaries can be held criminally liable under state laws for the actions of users, companies must either invest heavily in services that filter, monitor or block any potentially unlawful contributions, or they may simply refuse to develop novel platforms for UGC. Simply put, liability will dramatically increase the costs of innovation.
- **Higher Costs and Reduced Competition.** In addition to the costs associated with implementing a filtering or monitoring system, Internet businesses must follow the nuances of criminal law in all 50 states as well as each AG's idiosyncratic enforcement policies and public pressure. Companies may be pressured to settle disputes repeatedly, with multiple state AGs. These crushing legal compliance costs may decrease the number of market competitors, and increase consumer prices.
- **Reduced Freedom of Expression.** Requiring intermediaries, especially ISPs, to thus monitor UGC may also result in a "chilling effect." Fearing criminal liability, intermediaries might remove legally and constitutionally protected speech. This will frustrate users' attempts to exercise their freedom of expression online even when it may not actually violate the laws of the user's jurisdiction.
- **Reduced Diversity Online.** Some large Internet businesses may be able to comply with state criminal laws (albeit at great cost), but small businesses, nonprofits, and individual blogs might be prosecuted — or simply intimidated — out of existence. The resulting Internet would look very different than the diverse tapestry of small and large websites that we see today.

⁴ Mike Masnick at TechDirt has assembled a catalog of grandstanding by AGs: <http://tch.fm/1agw20X>.

How can the AGs potential concerns be addressed without amending Section 230?

Anonymous users can already be unmasked and prosecuted or sued. Users often post criminal, abusive or defamatory material anonymously, but Courts will unmask such defendants if a sufficient claim can be established. These actions are already unencumbered by CDA 230:

- **Criminal Prosecution.** Section 230 does not affect the Electronic Communications Privacy Act, which allows law enforcement to obtain identifying information about a criminal defendant.
- **Civil Actions.** Private plaintiffs can bring tort and other common law actions against a *John Doe*. While courts differ on the exact standard they will apply, if a plaintiff can make an adequate showing, a court will issue subpoenas compelling the intermediary to provide whatever identifying information they might have about the anonymous defendant. At a minimum, that should include an IP address, which can allow a second subpoena to the ISP to identify the defendant.

Moreover, existing jurisprudence already allows a state AG to enforce the state's criminal laws against individual defendants even without having to meet the "minimum contacts" requirement that exists in civil cases, provided the act in question causes — and is intended to cause — detrimental effects in the state.⁵

Our Position

Section 230 in its current form is essential to innovation, diversity, and freedom on the Internet.

Section 230 is the very cornerstone of Internet Freedom. Intermediaries provide an infinite variety of online communities that flourish from the diverse range of online voices contributing content. But these diverse communities only exist because those who build, host, or enable access to them don't have to fear crushing liability for UGC. The costs that intermediaries will inevitably incur from amending Section 230 will stifle innovation, competition, and the development of free and diverse online communities.

Users rather than intermediaries are the appropriate targets of efforts to reduce harmful UGC online.

State AGs should focus their efforts on enforcing Section 230 against users who have broken state criminal laws. Rather than hold intermediaries liable, policymakers should ensure that both prosecutors and civil plaintiffs can effectively identify anonymous users responsible for illegal, abusive or defamatory speech — while still preserving Americans' privacy and free speech rights. For example, that might include clarifying the legal standard for *John Doe* subpoenas, lessening the costs associated with bringing these suits, awarding attorneys fees to successful plaintiffs, or simply raising awareness about the option.

Further Reading

To browse all the links in this document, please visit: <http://tch.fm/17iozeE>

- *Section 230 of the Communications Decency Act*, Electronic Frontier Foundation (last visited July 1, 2013), <http://tch.fm/1auTwjq>
- *Shielding the Messengers: Protecting Platforms for Expression and Innovation*, Center For Democracy & Technology (updated Dec. 2012), <http://tch.fm/1auVccM>
- Eric Goldman, *The State Attorneys General Want to Eviscerate a Key Internet Immunity*, Forbes (June 26, 2013), <http://tch.fm/124nFNi>
- Eric Goldman, *Why The State Attorneys General's Assault On Internet Immunity Is A Terrible Idea*, Forbes (June 27, 2013), <http://tch.fm/124lsAk>
- Adam Thierer, *Web 2.0, Section 230, and Nozick's "Utopia of Utopias"*, TechLiberation (January 13, 2009), <http://tch.fm/17ioJmh>

⁵ <http://tch.fm/19OV2Kv>