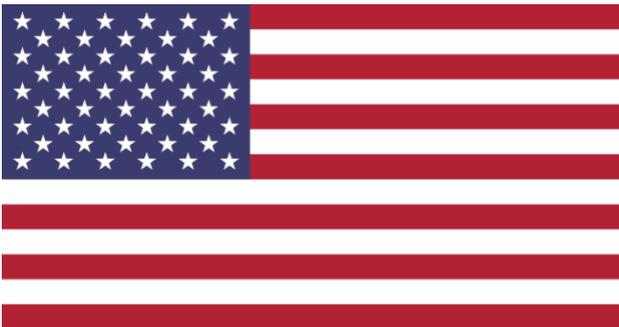


INTERMEDIARIES' LIABILITY: THE US EXPERIENCE

The U.S. experience is widely praised for protecting intermediary immunity for user-generated content. It is useful to compare it to other regimes as jurisdictions across the world assess their Internet liability systems.

The United States, like other countries, balances the right to free expression and the right to privacy. However, courts often decide in favor of free expression. Hence, it is unlikely that the United States would adopt a Right to be Forgotten similar to that of the European Union. Similarly, immunizing intermediaries for user content is consistent with the broad free speech values embedded in the First Amendment of the U.S. Constitution.

In his article "Twenty Years of Intermediary Immunity: the U.S. Experience" Jeff Kosseff reviews the U.S. legal framework and case law, examining in particular Section 230 and its implementation.



It is not exaggeration to state the fact the United States provides some of the strongest legal protection for online intermediaries. In 1996, the U.S. Congress enacted Section 230 of the Communications Decency Act under which online service providers are immune from liability for user-generated content. There are three explicit exemptions: Section 230 does not apply to enforcement of federal criminal laws, intellectual property laws, or electronic communications privacy laws. (Communications Decency Act, Section 230(e) 1996). The statute also provides websites with flexibility to edit, delete, or retain user-generated content. Its broad definition of "interactive computer service" includes Internet service providers, websites, mobile apps, and any other platforms that transmit user content. The two provisions of Sections 230(c)(1) and 230(c)(2) reflect Congress's twin goals of encouraging online platforms to voluntarily moderate user content and support innovation and development of the nascent commercial Internet.

The *Cubby* and *Stratton Oakmont* cases promoted the

approach that online intermediaries are legally responsible for user-generated content only if they take steps to control the content. On the other hand, if intermediaries take an entirely hands-off approach to third-party content, they would not be held liable for it.

Policymakers and advocacy groups worried that such rulings would turn the Internet into a lawless no-man's land ridden with highly offensive content. However, policymakers then believed that the free market would effectively force the imposition of responsible content rules that consumers demand. The people who posted the allegedly defamatory content may have used an anonymity service such as Tor, allowing them to mask their true identities, therefore making it difficult for the subject to name them in a lawsuit. Section 230 generally has prevented such lawsuits, allowing sites such as Yelp and other consumer review services to act as neutral intermediaries without facing the burden of pre-screening every user comment for accuracy.

As new forms of harmful online behavior emerged, U.S. courts began to more carefully scrutinize online platforms' claims. This trend became clear in 2008, when the ruling in *Fair Housing Council of San Fernando Valley v. Roommates.com* allowed liability to be imposed if the very act of soliciting user-generated content violates an existing law. If users incidentally violate the law by voluntarily providing information, the intermediaries retain their immunity. Later *Diamond Ranch Academy* and many other similar cases demonstrated a gradual willingness of courts to seek to hold intermediaries accountable for third-party content.

The US experience provides interesting examples of self-regulation. To assess the extent to which U.S. websites have voluntarily restricted user content, Kosseff reviewed the 25 most popular U.S. websites, as ranked by Alexa.com. Eighteen of them have implemented terms of use that include extensive restrictions on user content for illegal activities, hate speech, harassment, bullying, distribution of personal information, nudity or pornography and violent content.

Google recognizes that although its products "are platforms for free expression," it does not "support content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability,

gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these core characteristics.” According to Google, assessing such content “can be a delicate balancing act, but if the primary purpose is to attack a protected group, the content crosses a line.” (Google 2016).

Some U.S. news websites use a technology, known as Civil Comments to enable community moderation of online comments. When users comment on a story on a participating news website, they also are asked to rate the civility and quality of two randomly chosen comments. The news website’s staff then manually reviews comments that many users have deemed uncivil.

In August 2016, the National Public Radio (NPR) announced that its news website would no longer allow user comments. In its announcement of this change, NPR concluded that user comments “are not providing a useful experience for the vast majority of our users.”

Online platforms also have gone far beyond their legal duties to prohibit illegal and obscene content on their services. For instance, federal criminal law requires U.S. online service providers to notify the National Center for Missing and Exploited Children (NCMEC) if the providers have actual knowledge that their customers apparently have used their services to distribute child pornography. (18 U.S.C. 2258A). NCMEC then analyzes the content and, if it determines it is child pornography, contacts the proper law enforcement agency. Though under the law U.S. service providers are not required to proactively search for the illegal content, the exact opposite approach has emerged. Many of the largest U.S. online intermediaries

have developed and implemented technology that scans the content of their users’ cloud data, email, and other content for hash values that match a NCMEC database of hash values of known child pornography. The service providers’ arguments for this were that they responded adequately to consumers’ demands for a family-friendly online environment free of illegal content. In other words, the market has driven the decision for online intermediaries to go far beyond their legal duties. This is precisely the rationale behind Section 230.

By and large user-generated content has transformed commerce in the United States, as consumer review sites have proliferated. In a 2014 survey conducted by BrightLocal, 88 % of respondents stated that they read online user reviews to determine whether or not to purchase products or services from local businesses, and nearly 40 % read these reviews on a regular basis. (BrightLocal Consumer Review Survey 2015.)

Consistent implementation of Section 230 also has enabled the proliferation of social media, which relies on content generated by users. Although people use social media for a wide range of reasons, it has become a cornerstone of public dialogue in the United States.

Compiled by Media 21 Foundation (2019) from

<https://script-ed.org/article/twenty-years-of-intermediary-immunity-the-us-experience/>

