ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How Other Countries Have Dealt With Intermediary Liability

ASHLEY JOHNSON AND DANIEL CASTRO I FEBRUARY 2021

As the United States debates potential reforms to Section 230 of the Communications Decency Act, it is important to understand and evaluate the alternative approaches that other countries have taken to intermediary liability.

KEY TAKEAWAYS

- Some countries only hold online services accountable for content about which they are aware or have "actual knowledge." This gives online services some immunity, but it can incentivize services to take down too much content.
- Other countries use a notice-and-takedown approach similar to the Digital Millennium Copyright Act (DMCA). Once again, this gives online services some immunity, but can lead to removal of content may be controversial but not harmful or illegal.
- Some countries also have laws that set separate standards for certain types of content. These laws are often enacted in reaction to a specific problem, and they may place an undue burden on online services.
- Some countries without the United States' historic commitment to free speech offer fewer intermediary liability protections, while others have adopted the U.S. approach as part of trade agreements.

INTRODUCTION

Section 230 of the Communications Decency Act governs online intermediary liability in the United States. It contains two main provisions. The first, Section 230(c)(1), prevents online services from facing liability for third-party content on their platforms. The second, Section 230(c)(2), protects online services from facing liability for removing objectionable third-party content from their platforms. Section 230 also contains a few major exceptions; notably, its liability shield does not apply to federal criminal law, state or federal sex trafficking law, or intellectual property law. The United States also has a separate law, the Digital Millennium Copyright Act (DMCA), that governs online copyright law.

While many countries have laws that determine whether and under what circumstances online providers and services are liable for the third-party content they host or transmit, these laws differ from Section 230 in a few key ways.

Section 230 Series

There are three common approaches to intermediary liability in democratic countries outside the United States: the awareness or "actual knowledge" approach (Australia, India, Japan, and the Philippines), the notice and takedown approach (New Zealand and South Africa), and the "mere conduit" approach (EU, South Africa, and India). These approaches are not mutually exclusive, with a number of countries having applied a mix of multiple approaches. In addition, some countries have enacted legislation that deals with intermediary liability for certain types of content (e.g., violent or sexual content or hate speech) or for the removal of content, similar to Section 230(c)(2) in the United States. Finally, some nations have adopted the U.S. approach to intermediary liability as a condition of treaties they have signed with the United States regarding digital trade.

There are three common approaches to intermediary liability in democratic countries outside the United States: the awareness or "actual knowledge" approach, the notice and takedown approach, and the "mere conduit" approach.

Reflecting the United States' historic commitment to free speech, Section 230 offers broad intermediary liability protections in order to protect and promote free expression online, whereas most other countries without First Amendment protections offer narrower protections in order to prevent bad actors from taking advantage of the Internet. As U.S. lawmakers consider making changes to Section 230, it is important to understand other countries' approaches.

AWARENESS OR ACTUAL KNOWLEDGE

The first common approach to intermediary liability is to hold websites and online platforms accountable only for content they are aware or have "actual knowledge" of. Australia, India, Japan, and the Philippines all have provisions along these lines. The United States also uses this approach for online intermediary liability for copyrights.

For example, Schedule 5, Clause 91 of Australia's Broadcasting Services Act 1992 states that websites and Internet service providers (ISPs) are not liable for third-party content under state or

territory laws as long as they were "not aware of the nature" of the content.[1] Similarly, Chapter XII, Section 79 of India's Information Technology Act, enacted in 2000 and amended in 2008, contains a liability shield for third-party content unless "upon receiving actual knowledge …the intermediary fails to expeditiously remove or disable access to that material."[2]

Article 3 of Japan's Provider Liability Limitation Act, enacted in 2001, contains a liability shield that does not apply if a provider is aware that third-party content causes "the infringement of the rights of others," or if "there is a reasonable ground to find" that they know this.[3] And Section 30 of the Philippines' Electronic Commerce Act contains a liability shield that does not apply if a provider has "actual knowledge" or is aware that third-party content is "unlawful or infringes any rights."[4]

In the United States, the DMCA states that an online service is not liable for third-party content that violates copyright law if "upon obtaining such knowledge or awareness, [it] acts expeditiously to remove, or disable access to, the material."[5] Notably, the DMCA contains two conditions under which an intermediary would need to take action: "actual knowledge that the material or an activity using the material on the system or network is infringing" and "aware of facts or circumstances from which infringing activity is apparent" (this latter condition is often referred to as the "red flag knowledge" provision).

These types of provisions ensure platforms are not liable for illegal third-party content unless they have "actual knowledge" of the illegal content. The goal of these provisions is to motivate platforms to allow third parties, including affected parties, to notify them of illegal content, and then take swift action to remove it. At the same time, the awareness and actual knowledge standards protect platforms from having to proactively moderate every piece of content before it is posted, and correctly determine its legality, or face liability.

The drawback of these provisions is they incentivize platforms to take down more content than may be necessary. Once they become aware of potentially harmful or illegal content, it is often easier for platforms to remove it immediately in order to avoid liability rather than go through the effort of determining whether the content actually breaks any laws.[6] This incentive structure allows others to effectively weaponize reporting capabilities, such as to retaliate against content they oppose by falsely reporting it, or imposing significant moderation costs on platforms by forcing them to review content. Still, awareness and "actual knowledge" provisions are a compromise between offering no intermediary liability protection—which would incentivize even more overcautious behavior—and a strict liability regime wherein platforms are liable for all third-party content even without any knowledge.

NOTICE AND TAKEDOWN

The second common approach to intermediary liability—and another example of the overlap between intermediary liability and copyright law—is the "notice and takedown" approach. New Zealand, South Africa, and the United Kingdom all have notice and takedown provisions in their intermediary liability laws. In each of these countries, online services must follow notice and takedown provisions for content the state deems unlawful.

In New Zealand, Section 24 of the Harmful Digital Communications Act 2015 outlines the requirements for a "notice of complaint," which is the notification an individual sends to a website requesting the removal of harmful third-party content. Types of content the law covers

include any that is unlawful or that violates one or more of the law's "communication principles," which include any content that is threatening, "grossly offensive," obscene, harassing, discriminatory, or a breach of confidence or that discloses sensitive personal information, makes a false allegation, incites individuals to send harmful messages, or incites an individual to commit suicide.[7] It also outlines the process websites must follow after they receive a valid notice of complaint, including removing the content within 48 hours. As long as websites comply with this process, "no civil or criminal proceedings may be brought against [them]. "[8]

In South Africa, Chapter XI, Section 77 of the Electronic Communications and Transactions Act, enacted in 2002, similarly outlines the requirements for a "notification of unlawful activity."[9] So does the UK's Defamation Act 2013, although, as the law's name suggests, it applies only to defamatory content. Under the Defamation Act, website operators are only liable for defamatory third-party content if the claimant can show that "it was not possible for the claimant to identify the person who posted the statement," "the claimant gave the operator a notice of complaint," and "the operator failed to respond to the notice of complaint."[10]

As noted earlier, in the United States, the DMCA contains both an actual knowledge provision and a "red flag" provision for copyright law, the former of which activates when an online service becomes aware of infringing material on its platform, and the latter of which activates when a service becomes aware of activity that indicates copyright infringement. The DMCA also creates a notice and takedown process. The purpose of a DMCA takedown notice is for copyright owners to alert online services of infringing third-party content so the service can remove the content. In response to a valid notice, a service must remove the infringing content "expeditiously" in order to avoid facing liability. The individual who posted the content can then file a counter-notice that the content is not infringing. If the individual who filed the original notice does not take any further action within 10 days, the service must then restore access to the content.[11]

The distinction between the DMCA's actual knowledge and red flag provisions and its notice and takedown process is the former require an online service to act when a provider independently becomes aware of infringing activity or material, whereas the latter requires the service to act when a copyright owner alerts it to the presence of infringing material. Online services must adhere by all three of these processes in order to qualify for the DMCA's Safe Harbor provisions, which protect online services from liability for passively hosting third-party content.

The notice and takedown process is similar in countries that take that approach to intermediary liability. Using New Zealand as an example, within 48 hours of an individual submitting a notice of complaint that identifies specific harmful or illegal content, the website hosting the content must contact the author of the content or, if the author's identity is unknown, remove the content. The author can then file a counter-notice either consenting or refusing to the content's removal. If the author consents to the content's removal or fails to file a counter-notice, the website must remove the content within 48 hours.[12]

The benefit of the notice and takedown approach is it does not penalize online services if they fail to remove all potentially harmful or illegal content on their platforms as long as they follow the notice and takedown process. Expecting online services to find every potential instance of harmful or illegal content would be an unreasonable expectation for most online services, especially large ones. A large platform such as YouTube, with over 1 billion users, has over 500

hours of user-generated content uploaded every minute.[13] It would be unreasonable to expect YouTube to accurately find and remove every instance of potentially harmful or illegal content, even with its team of over 10,000 human moderators and machine learning algorithms.[14] The notice and takedown approach only holds online services liable for failing to remove harmful or illegal content within a certain timeframe upon receiving a notice.

The drawback of this approach, however, is that it incentivizes online services to remove content upon receiving notice that it may be harmful or illegal, even if the notice is mistaken or unfounded and the content is in fact permissible, to avoid potential liability. This could lead to censorship of content that is controversial but not harmful or illegal, such as unpopular political opinions, accusations of misconduct such as those posted on social media during the #MeToo movement, or even bad reviews of products and businesses. The risk of online services removing content that is not harmful or illegal is especially high when the law requires them to act within a very short timeframe to remove content after receiving a notice.

Although the notice and takedown approach succeeds in holding online services accountable for harmful and illegal content on their platforms without overburdening them by forcing them to proactively screen for all potentially harmful or illegal content, it can also jeopardize the Internet's role as a forum for free and open discourse when platforms remove legitimate content.

MERE CONDUIT, CACHING, AND HOSTING

The EU's approach to intermediary liability, which some countries such as South Africa and India have borrowed from, was established in the Directive 2000/31/EC (the "E-Commerce Directive"). The E-Commerce Directive only extends liability protections to online services when their activity "is of a mere technical, automatic and passive nature."[15] Thus, the liability protections extend only to "passive" online services offering "mere conduit" (Article 12), "caching" (Article 13), or "hosting" (Article 14). Online services that play a more active role in organizing content, such as a traditional social media site, do not qualify—a significant difference from Section 230, which applies broadly to all online services.

As outlined in Article 12 of the E-Commerce Directive, an online service is not liable for third-party content on its platform when it serves as a "mere conduit" to transmitting or temporarily storing third-party content. This condition applies if it "does not initiate the transmission" of information, "does not select the receiver of the transmission," and "does not select or modify the information contained in the transmission."[16]

The E-Commerce Directive also provides liability protections for caching and hosting services, distinguishing it from other countries' approaches that treat all types of online services or providers the same. Article 13 defines "caching" as "the automatic, intermediate, and temporary storage of … information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request."[17] In other words, caching services temporarily store content so users can access it more quickly, rather than requesting it again from the original source.

Article 14 of the Directive defines "hosting" as "the storage of information provided by the recipient of a service." Hosting services allow individuals and organizations to publish a website on the Internet.[18] Articles 13 and 14 each contain an "actual knowledge" provision that applies

only to caching and hosting services: Once the service becomes aware of illegal content, it must act "expeditiously" to remove that content, or it may face liability.

The Digital Services Act (DSA), the EU's proposal to update the E-Commerce Directive, contains provisions almost identical to the original E-Commerce Directive's mere conduit, caching, and hosting provisions, but also adds a number of other obligations for online services. For example, it would require an online service to comply with Member States' orders to act against illegal content on its platform and provide information the online service has collected on its users.[19] The DSA would also establish a set of "due diligence obligations" that would require online services to establish points of contact for Member States, designate a legal representative within the EU, publish annual content moderation reports, and create an internal complaint-handling system. It would require online platforms to suspend users that frequently post illegal content (as defined by Member States), notify Member States of potentially illegal activity, ensure anyone using the platform to promote products or services is traceable, and ensure advertisements are displayed transparently. Finally, the DSA includes an additional set of requirements for "very large online platforms," which are those that have at least 45 million average monthly users in the EU.[20] The DSA would also impose penalties of up to 6 percent of an online service's annual income or turnover for failing to comply with the obligations listed in the DSA, and up to 1 percent for supplying "incorrect, incomplete, or misleading [information]."[21]

In addition to its notice and takedown provision, South Africa's Electronic Communications and Transactions Act, enacted two years after the EU's E-Commerce Directive, contains sections on mere conduit, caching, and hosting with similar language. South Africa's law does not include awareness or "actual knowledge" provisions, but does state that online services that meet the requirements for mere conduit, caching, or hosting must still comply with any court order to remove unlawful content.[22]

When India amended its Information Technology Act in 2008, it added similar language to the E-Commerce Directive on mere conduits, caching, and hosting. In addition to the law's requirement that online services remove illegal content upon receiving "actual knowledge" that the content exists, online intermediaries may only qualify for the law's liability shield if they provide "temporary storage" (caching) or hosting services, or if they are not "initiating the transmission" of information, not "selecting the receiver of the transmission," and not "selecting or modifying the information contained in the transmission" (what the E-Commerce Directive defines as a "mere conduit").[23]

The benefit of the EU's approach with the E-Commerce Directive is that it does not overly burden online services with obligations they must fulfill in order to avoid penalties or liability. It also forbids Member States from imposing an obligation on online services to monitor their users' activity, which would undermine consumer privacy.[24] However, the E-Commerce Directive has resulted in an uneven playing field between competing online services both because the law makes an outdated distinction between active and passive online services and Member States have been free to exclude certain types of online services from their implementation of the law.[25] As EU policymakers grapple with growing concerns about disinformation, hate speech, and other forms of harmful content, they have turned to reform proposals such as the DSA as a means to reduce online harm.

With regards to intermediary liability, the DSA provides a useful update to the E-Commerce Directive by focusing on increasing transparency in content moderation decisions, providing clarity where the E-Commerce Directive remains vague, holding online services responsible for removing illegal content, and maintaining the E-Commerce Directive's prohibition on general monitoring obligations.[26] However, since Member States still have autonomy to decide what content is considered illegal, the DSA will not create a fully harmonized approach across the EU's Digital Single Market.

Although many countries have adopted "mere conduit" provisions similar to the EU's, some British policymakers take issue with theirs, arguing that it should not apply to social media companies, which not only host third-party content but amplify it with their news feed algorithms that decide what content users see. They see the United Kingdom's departure from the EU as an opportunity to change the way their country tackles intermediary liability. The country's former secretary of state for Digital, Culture, Media, and Sport suggested one possibility: a new set of laws that would regulate social media companies differently from other online platforms, placing them somewhere between "mere conduits," with no liability for third-party content, and publishers, which are liable for the content they publish.[27] However, to date, the United Kingdom has yet to move forward with a more detailed proposal.

REMOVAL OF CONTENT

Section 230 does not just protect websites and online platforms from liability for failing to remove harmful or illegal content, it also protects them from liability for engaging removing potentially harmful or illegal content.[28] This protection was intended to incentivize "good faith" content moderation. A few other countries, including Japan and South Africa, also have provisions that protect websites from liability for removing content.

In addition to its awareness provision, Article 3 of Japan's Provider Liability Limitation Act also states that when providers block content, they are not liable for "any loss incurred by" the user who posted the content, as long as providers meet one of two requirements. First, if they had "reasonable ground … to believe that the rights of others were infringed without due cause" by the content in question, they are not liable. Second, if they receive a takedown notice, they must ask the user who posted the content for consent to remove it—and if the user does not respond within seven days, they are also not liable.[29]

Similarly, under Chapter XI, Section 77 of South Africa's Electronic Communications and Transactions Act, websites are not liable for wrongful takedown if they remove content in response to a takedown notice. Rather, the individual who submitted the notice is liable for damages if they knowingly misrepresented the facts.[30]

Once again, these provisions are similar to U.S. copyright law. Under the DMCA, online services are not liable for their "good faith disabling of access to, or removal of, material or activity claimed to be infringing, … regardless of whether the material or activity is ultimately determined to be infringing."[31] Instead, any individual who files a takedown notice or counter-notice is liable if they "knowingly materially misrepresents" that either the content in question was infringing, or that it was not infringing and was mistakenly removed. [32]

TRADE AGREEMENTS

Two of the United States' recently negotiated trade agreements contain provisions similar to Section 230, which has caused controversy. First, on October 7, 2019, the United States and Japan signed both the U.S.-Japan Trade Agreement and the U.S.-Japan Digital Trade Agreement. While the first dealt with tariffs on agricultural products, the second included provisions on data localization, cross-border data flows, and online intermediary liability.

The reason for including language on online intermediary liability in trade agreements comes down to the international nature of the Internet. Many online services have users from multiple countries; and online businesses may offer their products and services to foreign customers. It is beneficial for these online services and businesses, and for their users and customers, to have a similar set of rules that apply across borders.

The language of Article 18 of the U.S.-Japan Digital Trade Agreement is very similar to Section 230. Paragraph 2 mimics Section 230(c)(1), which protects websites and online platforms from liability for failing to remove content. It states that neither the United States nor Japan will treat a website, online platform, or other online provider or service as the publisher or creator of third-party content "stored, processed, transmitted, distributed, or made available by the service," unless they had any part in creating or developing the content.

Article 18, Paragraph 3 mimics Section 230(c)(2), which protects websites and online platforms from liability for removing content. It states that neither the United States nor Japan will "impose liability on a supplier or user of an interactive computer service" for "any action voluntarily taken in good faith … to restrict access to or availability of" harmful or objectionable content, language taken directly from Section 230. Like Section 230, Article 18 contains exceptions for intellectual property law and criminal law.[33]

Just months after the United States and Japan signed their Digital Trade Agreement, the United States, Mexico, and Canada signed and ratified the United States-Mexico-Canada Agreement (USMCA), which replaces the North American Free Trade Agreement (NAFTA). Article 19.17 of the USMCA is almost identical to Article 18 of the U.S.-Japan Digital Trade Agreement, obligating the United States, Mexico, and Canada to adopt Section 230-like liability protections for online intermediaries.[34]

Section 230's critics oppose including similar language in trade agreements. Members of Congress on both sides of the aisle—including House Speaker Nancy Pelosi (D-CA), Representative Frank Pallone (D-NJ), and Representative Greg Walden (R-OR)—have expressed concerns "about enshrining the increasingly controversial Section 230 liability shield in our trade agreements, particularly at a time when Congress is considering whether changes need to be made in U.S. law."[35] They and other critics worry that including language from Section 230 in various trade agreements would make it more difficult for Congress to change the law in the future.

SEXUAL CONTENT

Some countries have, in addition to broader laws governing intermediary liability, laws that create exceptions for certain types of content. This is similar to the approach the United States took to sex trafficking when Congress passed the Allow States and Victims to Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act (FOSTA-SESTA). The law amended

Section 230 so that its liability shield no longer protects websites and online platforms from liability for "knowingly assisting, supporting, or facilitating [sex trafficking]."[36]

The Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*, or "Marco Civil"), enacted in 2014, includes a similar exception for nonconsensual pornography, colloquially known as "revenge porn." Article 21 of the law applies to third-party content depicting nudity or sexual activities and posted online without the participants' permission. "Internet application providers"—websites and online platforms—are responsible for removing this content "diligently" and "within the technical limits of their service" upon receiving notice from one of the participants. If they fail to do so, the participant can hold them liable for a breach of privacy.[37]

For all other forms of third-party content, the Marco Civil only holds websites and platforms civilly liable if they fail to remove content following a specific court order, within the time frame the court order provides.[38] The lower liability standard the law sets for nonconsensual pornography—that websites must remove it upon receipt of a notice, not a court order—is a reflection of the irreparable damage revenge porn can inflict on victims' lives, according to Luiz Fernando Moncau, former head of the Center for Technology and Society (*Centro de Tecnologia e Sociedade*) at the FGV Direito Rio law school in Rio de Janeiro.[39]

The Marco Civil also makes it easier for the police to identify the culprits behind revenge porn and other harmful or illegal content. Article 15 of the law requires websites to keep users' connection logs for six months and to provide these logs when presented with a court order.[40] With a court order, law enforcement can obtain important information about who first posted the harmful or illegal content in question, as well as who spread it. They can then more easily investigate and prosecute those responsible.[41] However, this provision has stirred up controversy, with digital-rights advocates arguing that mandatory data retention violates users' right to privacy.[42]

Section 230's critics frequently cite revenge porn as an area where the U.S. law fails. Currently, there is no federal law criminalizing nonconsensual pornography, although there are state laws.[43] But Section 230 only includes an exception for federal criminal law, while preempting state laws. Revenge porn websites can claim Section 230 liability protection when law enforcement or victims try to hold them accountable for amplifying and profiting off of harmful, illegal content.[44] Provisions such as Article 21 of the Marco Civil represent a different approach to the problem of revenge porn and intermediary liability.

VIOLENT CONTENT

Australia was one of the first countries to pass online intermediary liability legislation in 1992. Decades later, in 2019, it passed an additional law. While the United States takes a special approach to intermediary liability for sex trafficking, and Brazil takes a special approach to nonconsensual pornography, Australia takes a special approach to violent content with the Sharing of Abhorrent Violent Material Act.

The Sharing of Abhorrent Violent Material Act was Australia's reaction to the Christchurch mosque shooting in New Zealand in March 2019, in which a lone Australian gunman killed 51 worshippers and injured an additional 49.[45] The shooter livestreamed the attack on Facebook,

and the video quickly spread across the Internet, continuing to circulate on social media even after Facebook removed it. Before the attack, the shooter had also uploaded an 87-page anti-immigrant and anti-Muslim manifesto to 8chan, an anonymous online forum popular among white supremacists and other extremists.[46]

The Internet helps like-minded people find each other, including people with radical views. White supremacists use the Internet to connect with one another and normalize and spread their views. And terrorists of all sorts publicize their actions online, especially on social media, where they can find a large audience. Legislation such as Australia's Sharing of Abhorrent Violent Material Act aims to prevent terrorists and other hate groups from finding this audience.

The Act creates two new criminal offenses: failing to remove violent content and failing to report it to the Australian Federal Police. Its definition of "abhorrent violent material" includes acts of terrorism, murder, attempted murder, torture, rape, and kidnapping.[47] Failure to remove such content carries penalties of up to three years imprisonment or AU$2.1 million for an individual, or up to AU$10.5 million or 10 percent of annual turnover for corporations. Failure to notify law enforcement carries penalties of up to AU$168,000 for an individual or up to AU$840,000 for corporations.[48]

The Act had an extremely short legislative timeframe: The Senate introduced and passed the bill on April 3, the House of Representatives passed it on April 4, and it became law on April 5.[49] Stakeholders, experts, and the general public did not have time to offer their comments, and as a result, the final Act is controversial. Critics cite its ambiguous language, which exacerbates legal uncertainty; in particular, it fails to define "expeditious" removal, raising questions of how quickly websites and online platforms must identify, remove, and report violent content in order to avoid liability. The Act also incentivizes websites and platforms to remove more content than necessary to avoid the high penalties of failing to remove violent content.[50]

HATE SPEECH

In 2017, Germany passed a law designed to target hate speech. Germany has strong laws criminalizing hate speech, including the use of racial slurs or Nazi imagery, Holocaust denial, and incitement to hatred against minorities.[51] Germany's Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*, or "NetzDG") was the country's attempt to combat hate speech online, which has presented a unique challenge for all countries trying to combat hatred and extremism. Just as users can share harmless or uplifting content, they can also easily and anonymously spread hate speech to potentially billions of other users; and just as users can join online communities that share advice or support, they can also join online hate groups where they can become radicalized.

The NetzDG requires social networks with at least two million German users to remove "manifestly unlawful" content within 24 hours of receiving a complaint, with fines of up to €50 million for noncompliance.[52] The law applies not only to hate speech but also to other forms of unlawful content such as defamation, incitement to crime, nonconsensual pornography, and depictions of violence.[53] In response to the law, Facebook and Twitter not only added more ways for users to flag potentially unlawful content as well as any posts that violate the networks' community standards, but hired more German-language moderators to review flagged content.[54] In Facebook's first report on its handling of complaints in Germany after the NetzDG's passage,

the social network said it had received 1,704 complaints and removed 362 posts between January and June 2018.[55]

The NetzDG received criticism from across the German political spectrum. The far-right Alternative für Deutschland (AfD) party objected to the law, calling it a form of censorship, especially after some of the first posts social networks removed under the new law were from AfD politicians. Meanwhile, the center-left Green Party argued that, by requiring tech companies to delineate between lawful and unlawful content, the law placed an undue burden on these companies and gave them a legal responsibility best left to the judiciary.[56] Two other German political parties, The Left and the Free Democratic Party, also opposed the NetzDG. The law also drew criticism from outside Germany, with the international non-governmental organization Human Rights Watch calling it vague, overbroad, and censorial, and accusing Germany of setting a precedent for other governments, including authoritarian governments, to restrict free speech in their countries.[57]

In 2020, the Bundestag passed a reform to the NetzDG that, instead of relaxing the obligations on tech companies, added even more obligations. The amendment requires social networks to report certain types of unlawful content to Germany's Federal Criminal Police Office.[58]

Though Germany has taken a stricter approach than many other democratic countries, the debate surrounding the NetzDG is representative of the struggle many countries face when deciding how to regulate content moderation. On the one hand, extremists around the world have used the Internet and social media to spread their message of hatred and violence against minorities, and governments understandably want to minimize this activity. On the other hand, laws such as the NetzDG can easily go too far by creating pressure for tech companies to censor potentially lawful speech because of high fines and short takedown periods.

CONCLUSION

Outside the United States, approaches to online intermediary liability in democratic countries generally fall in between a broadly permissive approach that shields online services from any and all liability for third-party content and a restrictive approach that holds online services fully responsible for the content on their platforms. When finding a compromise between the two extremes, democracies need to balance many different factors, including free speech, innovation, competition, transparency, accountability, and reducing online harms.

There are many options beyond the binary of preserving Section 230 as it is and repealing it altogether. As U.S. policymakers consider a variety of proposals to reform Section 230, they should use other countries' approaches as a guideline, evaluating what has and has not worked and predicting some of the side effects different reforms would have for businesses, consumers, and the economy.

About the Authors

Ashley Johnson (@ashleyjnsn) is a policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

Daniel Castro (@CastroTech) is vice president at ITIF and director of its Center for Data Innovation. He writes and speaks on a variety of issues related to information technology and Internet policy, including privacy, security, intellectual property, Internet governance, e-government, and accessibility for people with disabilities.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. Broadcasting Services Act 1992 (Commonwealth of Australia), Schedule 5, Clause 91.
2. The Information Technology Act, 2000 (Republic of India), Chapter XII, Section 79, Subsection 3.
3. Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 1.
4. An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof, and for Other Purposes (Republic of the Philippines, 2000), Section 30.
5. 17 U.S.C. § 512(c)(1)(A) (1998).
6. Lucas Logan, "Free Expression, Privacy, and Intellectual Property Online: Contesting Intermediary Liability," Communication Law Review 16, no. 1 (2016), http://www.commlawreview.org/Archives/CLRv16i1/CLRv16i1_Free_Expression_Lucas.pdf.
7. Harmful Digital Communications Act 2015 (New Zealand), Section 6.
8. Ibid., Section 24.
9. Electronic Communications and Transactions Act, 2002 (Republic of South Africa), Chapter XI, Section 77.
10. Defamation Act 2013 (United Kingdom of Great Britain), Section 5.
11. 17 U.S.C. § 512(g)(2)(C) (1998).
12. Harmful Digital Communications Act 2015 (New Zealand), Section 24.
13. Anmar Frangoul, "With over 1 billion users, here how YouTube is keeping pace with change," CNBC, March 24, 2018, https://www.cnbc.com/2018/03/14/with-over-1-billion-users-heres-how-youtube-is-keeping-pace-with-change.html.
14. Sam Levin, "Google to hire thousands of moderators after outcry over YouTube abuse videos," The Guardian, December 5, 2017, https://www.theguardian.com/technology/2017/dec/04/google-youtube-hire-moderators-child-abuse-videos.
15. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (European Union), Preamble.
16. Ibid., Article 12.
17. Ibid., Article 13.
18. Ibid., Article 14.
19. Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (European Union), Chapter II.
20. Ibid., Chapter III.
21. Ibid., Article 42.
22. Electronic Communications and Transactions Act, Chapter XI, Section 73-75.
23. The Information Technology Act, 2000 (Republic of India), Chapter XII, Section 79, Subsection 2.
24. Directive 2000/31/EC, Article 15.
25. Daniel Castro and Eline Chivot, "What the EU Should Put in the Digital Services Act" (Information Technology and Innovation Foundation, January 2020), 2, https://www2.datainnovation.org/2020-eu-digital-services-act.pdf.

26. Ibid.
27. Alex Hern, "UK could rethink social media laws after Brexit, says minister," The Guardian, March 14, 2018, https://www.theguardian.com/media/2018/mar/14/uk-could-rethink-social-media-laws-after-brexit-says-minister.
28. 47 U.S.C. § 230(c)(2) (1996).
29. Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 2.
30. Electronic Communications and Transactions Act, 2002 (Republic of South Africa), Chapter XI, Section 77.
31. 17 U.S.C. § 512(g)(1) (1998).
32. 17 U.S.C. § 512(f) (1998).
33. U.S.-Japan Digital Trade Agreement (United States-Japan, 2019), Article 18.
34. United States-Mexico-Canada Agreement (United States-Mexico-Canada, 2019), Article 19.17.
35. Lauren Feiner, "Pelosi pushes to keep tech's legal shield out of trade agreements with Mexico and Canada," CNBC, December 5, 2019, https://www.cnbc.com/2019/12/05/pelosi-pushes-to-keep-section-230-out-of-usmca-trade-agreement.html.
36. "H.R. 1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017," Congress.gov, accessed March 25, 2020, https://www.congress.gov/bill/115th-congress/house-bill/1865/text.
37. Chamber of Deputies, "The Brazilian Civil Framework of the Internet (in English)" (Brasília: Edições Câmara, 2016), 33, http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf.
38. Ibid., 32.
39. Diego Iraheta, "Pornografia da vingança: Marco Civil da Internet facilita punição e obriga sites a tirar vídeos íntimos do ar," Huffpost Brasil, March 28, 2014, https://www.huffpostbrasil.com/2014/03/28/pornografia-da-vinganca-marco-civil-da-internet-facilita-punica_n_5052468.html.
40. Chamber of Deputies, "The Brazilian Civil Framework," 31.
41. Iraheta, "Pornografia da Vingança."
42. Katitza Rodriguez, "Privacy Is a Human Right: Data Retention Violates That Right," Americas Quarterly 9, no. 3 (Summer 2015): 109-110, https://www.americasquarterly.org/content/privacy-human-right-data-retention-violates-right.
43. "46 States + DC + One Territory Now Have Revenge Porn Laws," Cyber Civil Rights Initiative, accessed February 26, 2020, https://www.cybercivilrights.org/revenge-porn-laws/.
44. Danielle Keats Citron and Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity," Fordham Law Review 86, no. 2 (2017): 413, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5435&context=flr.
45. Eleanor Ainge Roy and Charlotte Graham-McLay, "Christchurch gunman pleads guilty to New Zealand mosque attack that killed 51," The Guardian, March 25, 2020, https://www.theguardian.com/world/2020/mar/26/christchurch-shooting-brenton-tarrant-pleads-guilty-to-new-zealand-mosque-attacks-that-killed-51.
46. Jenni Marsh and Tara Mulholland, "How the Christchurch terrorist attack was made for social media," CNN, March 16, 2019, https://www.cnn.com/2019/03/15/tech/christchurch-internet-radicalization-intl/index.html.

47. Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Commonwealth of Australia) sections 474.31-32.
48. "Australian government pushes through expansive new legislation targeting abhorrent violent material online," Ashurst, published April 10, 2019, https://www.ashurst.com/en/news-and-insights/legal-updates/media-update-new-legislation-targeting-abhorrent-violent-material-online/.
49. "Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019," Parliament of Australia, accessed March 27, 2020, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201.
50. Evelyn Douek, "Australia's New Social Media Law Is a Mess," Lawfare, April 10, 2019, https://www.lawfareblog.com/australias-new-social-media-law-mess.
51. Janosch Delcker, "Germany's balancing act: Fighting online hate while protecting free speech," Politico, October 1, 2020, https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation/;

    Philip Oltermann, "Tough new German law puts tech firms and free speech in spotlight," The Guardian, January 5, 2018, https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight.
52. Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) (Federal Republic of Germany, 2017).
53. "Overview of the NetzDG Network Enforcement Law," Center for Democracy and Technology, July 17, 2017, https://cdt.org/insights/overview-of-the-netzdg-network-enforcement-law/.
54. Oltermann, "Tough new German law."
55. Reuters Staff, "Facebook deletes hundreds of posts under German hate-speech law," July 27, 2018, https://www.reuters.com/article/us-facebook-germany/facebook-deletes-hundreds-of-posts-under-german-hate-speech-law-idUSKBN1KH21L.
56. Philip Oltermann, "Tough new German law."
57. "Germany: Flawed Social Media Law," Human Rights Watch, February 14, 2018, https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.
58. Delcker, "Germany's balancing act."