ONLINE SPEECH AND SOCIAL MEDIA

Policymakers should

- maintain the free speech protections of Section 230;
- place responsibility for internet misuse with individuals, not the tools they use;
- prevent anti-competitive uses of the Computer Fraud and Abuse Act; and
- make internet freedom a goal of diplomacy.

The Internet as a Speech Ecosystem

The internet is a varied, thriving, and ever-changing speech ecosystem, teeming with products that carry almost every conceivable form of speech. New websites and social media platforms are frequently launched to compete with current offerings, providing new features and distinct ways of arranging and presenting user speech. Each platform crafts its policies to attract the speech it deems valuable. Different platforms aim to please different audiences and advertisers. Twitch prioritizes live video, eBay highlights well-reviewed sellers, Twitter prohibits hate speech, and Patriots.win only welcomes supporters of Donald Trump. Diversity of opinion marks the system as a whole but not every platform within it.

All internet regulation should be considered and evaluated in light of its effect on the digital speech ecosystem as a whole, rather than its effect on particular companies. When legislation is introduced to correct the failings of specific platforms or business models, it often affects other services in unforeseen and unintended ways.

Unlike new products that individual consumers can adopt or ignore at their leisure, new legislation affects everyone. The costs of complying with new regulations often fall hardest on small or new platforms, which are also less

likely have a voice in the legislative process. Policymakers should take care to avoid unintentionally advantaging incumbent firms by creating new barriers to market entry. The risk of inadvertently doing harm is particularly acute when modifying broad protections that many different sorts of websites rely on, such as Section 230.

Section 230

Section 230, part of the 1996 Telecommunications Act, restates the rights to freedom of speech and freedom of association for the internet. It holds that interactive computer services cannot be treated as the publishers of any information provided by their users. Section 230 also protects intermediaries from lawsuits about their decisions to moderate or refrain from hosting user speech. Shielding websites from liability for users' speech allows them to carry all lawful speech and publish submissions immediately, without automated filtering or time-consuming review. By empowering websites to remove off-topic, unwanted, or "otherwise objectionable" material without facing costly litigation, Section 230 ensures that online communities and service providers can choose whatever rules or standards they think most fitting for their particular corner of the internet.

The massive scale of social media raises the potential costs of litigating suits concerning content moderation. Following Section 230, courts dismiss lawsuits seeking to hold social media platforms liable as publishers. Absent the statute's protections, even small platforms would have to continually vindicate their First Amendment rights. Section 230's procedural shield is invaluable to small or new platforms, which cannot afford costly, repeated litigation.

Section 230 does not give platforms a blank check. It only protects them from liability for user-submitted content—so if platforms help create, or substantially modify, users' speech, they can be held responsible for it. Platforms also remain responsible for their own speech, such as content labels or warnings.

Section 230 includes exceptions for federal criminal law and copyrighted material. As a result, platforms of all stripes strictly prohibit illegal media, such as child pornography, because they face criminal liability for knowingly distributing it. The Digital Millennium Copyright Act creates a notice-and-takedown system to police the unauthorized republication of copyrighted material. At scale, platforms rarely question the notices they receive, and automated filters often mistakenly remove users' original content. This alternative system offers a view of how platforms might treat controversial speech in the absence of Section 230.

For the past 26 years, Section 230 has insulated the internet speech ecosystem from most forms of government interference. Rather than protecting particular platforms or offering separate rules for different sorts of services, it protects all internet intermediaries equally, regardless of their size, purpose, or policies. Agnostic as to medium, Section 230 shields ancient bulletin boards and the latest virtual reality apps. Importantly, it has allowed internet communication to progress freely—each iteration of services receives the same protections as the last. Under this uniform, predictable arrangement, specific platforms may set their own rules. They may choose to cater to mass audiences or provide safe spaces for niche subcultures and can govern their services accordingly. As a whole, today's internet is the "forum for a true diversity of political discourse" that Section 230's drafters envisaged. The statute's liberal, decentralized approach remains the best means of ensuring freedom of speech online. Proposals to eliminate or amend Section 230 would leave Americans with fewer opportunities to speak, now and in the future.

Individual Responsibility Online

That the internet has been a tremendous boon for free speech does not mean that it cannot be misused. Speech may of course be used to plan, coordinate, and commit crimes. While the internet may merely make some crimes more visible rather than more common, it also creates genuinely novel opportunities for abuse.

Law enforcement often struggles to address revenge pornography, swatting (maliciously prompting an emergency response by law enforcement), and criminal stalking or harassment online. Whether the result of a lack of resources, a lack of specialized training, or a lack of appreciation for the severity of digitally delivered harm, the enforcement gap between different varieties of cybercrimes is striking. Harassment that includes interstate terroristic threats or child pornography is taken seriously, elevated to federal law enforcement, and prosecuted. Without these elements, existing laws against stalking and harassment often go unenforced.

Instead of punishing intermediaries, such as social media platforms, for failing to prevent cybercrime, the law should seek to hold individual speakers responsible for their words. Policymakers should reject theories of liability that deem publishing tools "defective" merely because they can be misused. Rather than modify platforms to eliminate opportunities for abuse, which would harm lawful users, policymakers should encourage police to take cybercrime more seriously and to give law enforcement the training necessary to identify and prosecute cybercriminals.

Children and Parents

One group of users who are less responsible for their actions is children. Children are always a special case in policy, and internet policy is no different. However, as in other areas of life, policymakers who want to help children online can best do so by empowering parents, not replacing them.

Legislation that would require platforms to identify underage users or automatically pair children's accounts with those of their parents, such as the Kids Online Safety Act, expects too much of these services. Age gating is difficult to implement effectively without compromising users' privacy. Requiring a credit card to access adult content was ruled unconstitutional in *Reno v. ACLU*. Algorithms can't be trusted to reliably deduce age from user behavior and rely on intrusive monitoring to gather data. Children often borrow, buy, or steal adult credentials. Instead of counting on platforms to get these settings right, activating a children's mode or linking a parental account should happen on device. Relying on parents' or family members' physical access to children's devices minimizes opportunities for abuse.

More broadly, platforms should never be required to adopt responsibilities that they will be unable to fulfill. Parents or other family members will always be the best supervisors of children's activity online, and misplaced expectations of platform-provided safety are dangerous in their own right.

Drawing hard lines between children, teens, and adults will always be difficult. Young people mature at different rates and often use the internet to avoid being treated as children. Existing norms around children's internet use are idiosyncratic—conventional wisdom discourages children's social media use, but parents routinely allow their children to play social video games intended for adults. Here, the existing Children's Online Privacy Protection Act—which requires parental consent to collect data from users under age 13—largely goes unenforced. Proposals to protect teens by raising the COPPA age threshold from 13 to 15 would only further decrease compliance.

Platform-specific solutions risk staying one step behind the changing tastes of youth. As their parents joined Facebook, teens left the platform for Instagram and are lately moving to TikTok as policymakers investigate Instagram for potential violations of consumer protection law. Improving digital literacy among parents, children, and teens is a better path forward than trying to keep up with this moving target via the blunt instrument of regulation. Internet education efforts should emphasize that users are content creators and curators rather than mere passive consumers.

CFAA Abuse

Along with protecting children, another increasingly popular rationale for internet regulation is to encourage competition. However, before imposing new obligations on platforms to foster or enhance competition, policymakers should eliminate existing regulations that inhibit competition. The 1986 Computer Fraud and Abuse Act (CFAA) criminalizes accessing a computer without authorization or exceeding authorized access to a computer. The statute was intended to punish computer hacking, but its civil provisions are sometimes abused by dominant firms to squelch competition.

Both computer code and platform policies control access to computer systems. When new services try to utilize the features or data of existing platforms —for example, by letting users access their Facebook feed via another app— these new services violate Facebook's policies. However, instead of simply leaving it to Facebook to prevent these unwanted uses of its service, the CFAA empowers Facebook to sue its competitors for unauthorized or excessive access to Facebook's systems, as it did with Power Ventures, a social media aggregation startup.

The Supreme Court's 2020 *Van Buren v. United States* decision narrowed criminal applications of the CFAA but has not prevented its use as a cudgel by incumbent firms. The threat of an expensive CFAA lawsuit is often enough to cow hobbyists and scare off investors, chilling competition and limiting consumer choice. In March 2021, Activision shuttered a popular video game stats tracking website with the threat of CFAA lawsuits.

It is time for Congress to fix the problem by removing the civil causes of action for unauthorized and excessive access from the CFAA. The CFAA was intended to prevent hacking, not interoperable internet services. If unauthorized access damages a computer system, other CFAA provisions and many preexisting torts can still provide redress.

Foreign Regulation

Like the internet itself, efforts to regulate digital platforms reach across borders. When platforms serve many markets around the world, speech restrictions in one country can shape the rules of products and services created and enjoyed by Americans. Although Congress is sometimes accused of dithering while the European Union "leads" on technology regulation, the European approach illustrates the pitfalls of unthinking tinkering. The European Digital Markets Act, which comes into effect in 2023, mandates interoperability

between messaging services at the expense of privacy and security. This is not a lead that America should follow. Indeed, in the coming years, one of the most important jobs for internet policymakers will be shielding American websites from foreign regulation.

Foreign governments increasingly demand that American platforms filter content and surveil users as a condition of market access. America cannot set the domestic policies of foreign nations, but it can make internet freedom a focus of its foreign policy. Policymakers should support efforts to treat censorship obligations—such as Turkey's laws against "anti-Turkish speech" and its requirement that platforms appoint a representative for handling government takedown requests—as nontariff barriers to trade and make liberal internet speech governance more central to American diplomacy. The inclusion of Section 230–like intermediary liability protections in the 2020 United States–Mexico–Canada Agreement was a victory for this approach. Policymakers should attempt to replicate this success in other trade deals. There are few formal levers that can be used to prevent erstwhile American allies such as Turkey from punishing American platforms that fail to toe its line. However, policymakers need not tolerate these actions and could give greater consideration in foreign-aid disbursement decisions.

Above all else, policymakers should avoid strangling America's golden goose with regulation. Foreign censorship demands often go unenforced, and even regulated American platforms carry culture and are shaped by American values. For the rest of the world, regulating American platforms is a second-best alternative to homegrown replacements. Foreign governments resent the dominance of American digital infrastructure, but most have been unable to cultivate domestic alternatives.

Conclusion

In debates about updating American internet regulation, proposals to amend or repeal Section 230 have sucked up most of the oxygen in the room. However, altering Section 230 would upset a delicate speech ecosystem, leaving Americans with fewer opportunities to speak. Instead, preserving Section 230 while reforming the CFAA, better equipping law enforcement to fight cybercrime, and opposing foreign censorship will improve what needs fixing without upsetting what works. These important reforms have not received the attention paid to Section 230, but they are the best steps policymakers can take to make the internet safer, more competitive, and more free.

Suggested Readings

Duffield, Will. "Circumventing Section 230: Product Liability Lawsuits Threaten Internet Speech." Cato Institute Policy Analysis no. 906, January 26, 2021.

Mueller, Milton. "Challenging the Social Media Moral Panic: Preserving Free Expression under Hypertransparency." Cato Institute Policy Analysis no. 876, July 23, 2019.

Samples, John. "Why the Government Should Not Regulate Content Moderation of Social Media." Cato Institute Policy Analysis no. 865, April 9, 2019.

—Prepared by Will Duffield