Liability for User-Generated Content Online
Principles for Lawmakers
July 11, 2019

Policymakers have expressed concern about both harmful online speech and the content moderation practices of tech companies. Section 230, enacted as part of the bipartisan Communications Decency Act of 1996, says that Internet services, or "intermediaries," are not liable for illegal third-party content except with respect to intellectual property, federal criminal prosecutions, communications privacy (ECPA), and sex trafficking (FOSTA). Of course, Internet services remain responsible for content they themselves create.

As civil society organizations, academics, and other experts who study the regulation of user-generated content, we value the balance between freely exchanging ideas, fostering innovation, and limiting harmful speech. Because this is an exceptionally delicate balance, Section 230 reform poses a substantial risk of failing to address policymakers' concerns and harming the Internet overall. We hope the following principles help any policymakers considering amendments to Section 230.

***Principle #1*: Content creators bear primary responsibility for their speech and actions.**

Content creators—including online services themselves—bear primary responsibility for their own content and actions. Section 230 has never interfered with holding content creators liable. Instead, Section 230 restricts only who can be liable for the harmful content created *by others*.

Law enforcement online is as important as it is offline. If policymakers believe existing law does not adequately deter bad actors online, they should (i) invest more in the enforcement of existing laws, and (ii) identify and remove obstacles to the enforcement of existing laws. Importantly, while anonymity online can certainly constrain the ability to hold users accountable for their content and actions, courts and litigants have tools to pierce anonymity. And in the rare situation where truly egregious online conduct simply isn't covered by existing criminal law, the law could be expanded. But if policymakers want to avoid chilling American entrepreneurship, it's crucial to avoid imposing criminal liability on online intermediaries or their executives for unlawful user-generated content.

***Principle #2:* Any new intermediary liability law must not target constitutionally protected speech.**

The government shouldn't require—or coerce—intermediaries to remove constitutionally protected speech that the government cannot prohibit directly. Such demands violate the First Amendment. Also, imposing broad liability for user speech incentivizes services to err on the side of taking down speech, resulting in overbroad censorship—or even avoid offering speech forums altogether.

***Principle #3*: The law shouldn't discourage Internet services from moderating content.**

To flourish, the Internet requires that site managers have the ability to remove legal but objectionable content—including content that would be protected under the First Amendment from censorship by the government. If Internet services could not prohibit harassment, pornography, racial slurs, and other lawful but offensive or damaging material, they couldn't facilitate civil discourse. Even when Internet services have the ability to moderate content, their

moderation efforts will always be imperfect given the vast scale of even relatively small sites and the speed with which content is posted. Section 230 ensures that Internet services can carry out this socially beneficial but error-prone work without exposing themselves to increased liability; penalizing them for imperfect content moderation or second-guessing their decision-making will only discourage them from trying in the first place. This vital principle should remain intact.

***Principle #4*: Section 230 does not, and should not, require "neutrality."**

Publishing third-party content online never can be "neutral."[1] Indeed, every publication decision will necessarily prioritize some content at the expense of other content. Even an "objective" approach, such as presenting content in reverse chronological order, isn't *neutral* because it prioritizes recency over other values. By protecting the prioritization, de-prioritization, and removal of content, Section 230 provides Internet services with the legal certainty they need to do the socially beneficial work of minimizing harmful content.

***Principle #5*: We need a uniform national legal standard.**

Most Internet services cannot publish content on a state-by-state basis, so state-by-state variations in liability would force compliance with the most restrictive legal standard. In its current form, Section 230 prevents this dilemma by setting a consistent national standard—which includes potential liability under the uniform body of federal criminal law. Internet services, especially smaller companies and new entrants, would find it difficult, if not impossible, to manage the costs and legal risks of facing potential liability under state civil law, or of bearing the risk of prosecution under state criminal law.

***Principle #6*: We must continue to promote innovation on the Internet.**

Section 230 encourages innovation in Internet services, especially by smaller services and start-ups who most need protection from potentially crushing liability. The law must continue to protect intermediaries not merely from liability, but from having to defend against excessive, often-meritless suits—what one court called "death by ten thousand duck-bites." Without such protection, compliance, implementation, and litigation costs could strangle smaller companies even before they emerge, while larger, incumbent technology companies would be much better positioned to absorb these costs. Any amendment to Section 230 that is calibrated to what *might* be possible for the Internet giants will necessarily *mis*-calibrate the law for smaller services.

***Principle #7*: Section 230 should apply equally across a broad spectrum of online services.**

Section 230 applies to services that users never interact with directly. The further removed an Internet service—such as a DDOS protection provider or domain name registrar—is from an offending user's content or actions, the more blunt its tools to combat objectionable content become. Unlike social media companies or other user-facing services, infrastructure providers cannot take measures like removing individual posts or comments. Instead, they can only shutter entire sites or services, thus risking significant collateral damage to inoffensive or harmless content. Requirements drafted with user-facing services in mind will likely not work for these non-user-facing services.

---

[1] We are addressing neutrality only in content publishing. "Net neutrality," or discrimination by Internet access providers, is beyond the scope of these principles.

Individual Signatories

Affiliations are for identification purposes only

1. Prof. Susan Ariel Aaronson, Elliott School of International Affairs, George Washington University
2. Prof. Enrique Armijo, Elon University School of Law
3. Prof. Thomas C. Arthur, Emory University School of Law
4. Farzaneh Badiei, Internet Governance Project, Georgia Institute of Technology (research associate)
5. Prof. Derek Bambauer, University of Arizona James E. Rogers College of Law
6. Prof. Jane Bambauer, University of Arizona James E. Rogers College of Law
7. Prof. Annemarie Bridy, University of Idaho College of Law
8. Lydia de la Torre, Santa Clara University School of Law (fellow)
9. Prof. Brian L. Frye, University of Kentucky College of Law
10. Prof. Elizabeth Townsend Gard, Tulane Law School
11. Prof. Jim Gibson, University of Richmond, T. C. Williams School of Law
12. Prof. Eric Goldman, Santa Clara University School of Law
13. Prof. Edina Harbinja, Aston University UK
14. Prof. Gus Hurwitz, University of Nebraska College of Law
15. Prof. Michael Jacobs, DePaul University College of Law (emeritus)
16. Daphne Keller, Stanford Center for Internet and Society
17. Christopher Koopman, Center for Growth and Opportunity, Utah State University
18. Prof. Thomas Lambert, University of Missouri School of Law
19. Prof. Stacey M. Lantagne, University of Mississippi School of Law
20. Prof. Sarah E. Lageson, Rutgers University-Newark School of Criminal Justice
21. Prof. Jyh-An Lee, The Chinese University of Hong Kong
22. Prof. Mark A. Lemley, Stanford Law School
23. Thomas M. Lenard, Senior Fellow and President Emeritus, Technology Policy Institute
24. Prof. David Levine, Elon University School of Law
25. Prof. Yvette Joy Liebesman, Saint Louis University School of Law
26. Prof. John Lopatka, Penn State Law
27. Yong Liu, Hebei Academy of Social Sciences (researcher)
28. Prof. Katja Weckstrom Lindroos UEF Law School, University of Eastern Finland
29. Prof. Daniel A. Lyons, Boston College Law School
30. Prof. John Lopatka, Penn State Law
31. Geoffrey A. Manne, President, International Center for Law & Economics; Distinguished Fellow, Northwestern University Center on Law, Business & Government
32. Prof. Stephen McJohn, Suffolk University Law School
33. David Morar, Elliott School of International Affairs, George Washington University (visiting scholar)
34. Prof. Frederick Mostert, The Dickson Poon School of Law, King's College London
35. Prof. Milton Mueller, Internet Governance Project, Georgia Institute of Technology
36. Prof. Ira S. Nathenson, St. Thomas University (Florida) School of Law
37. Prof. Christopher Newman, Antonin Scalia Law School at George Mason University
38. Prof. Fred Kennedy Nkusi, UNILAK
39. David G. Post, Beasley School of Law, Temple University (retired)
40. Prof. Betsy Rosenblatt, UC Davis School of Law (visitor)
41. Prof. John Rothchild, Wayne State University Law School
42. David Silverman, Lewis & Clark Law School (adjunct)

43. Prof. Vernon Smith, George L. Argyros School of Business and Economics & Dale E. Fowler School of Law, Chapman University
44. Prof. Nicolas Suzor, QUT Law School
45. Prof. Gavin Sutter, CCLS, School of Law, Queen Mary University of London
46. Berin Szóka, President, TechFreedom
47. Prof. Rebecca Tushnet, Harvard Law School
48. Prof. Habib S. Usman, American University of Nigeria
49. Prof. John Villasenor, Electrical Engineering, Public Policy, and Law at UCLA
50. Prof. Joshua D. Wright, Antonin Scalia Law School at George Mason University

Institutional Signatories

1. ALEC (American Legislative Exchange Council) Action
2. Americans for Prosperity
3. Center for Democracy & Technology
4. Competitive Enterprise Institute
5. Copia Institute
6. Freedom Foundation of Minnesota
7. FreedomWorks
8. Information Technology and Innovation Foundation
9. Innovation Economy Institute
10. Innovation Defense Foundation
11. Institute for Liberty
12. The Institute for Policy Innovation (IPI)
13. International Center for Law & Economics
14. James Madison Institute
15. Libertas Institute
16. Lincoln Network
17. Mississippi Center for Public Policy
18. National Taxpayers Union
19. New America's Open Technology Institute
20. Organization for Transformative Works
21. Pelican Institute
22. Rio Grande Foundation
23. R Street Institute
24. Stand Together
25. Taxpayers Protection Alliance
26. TechFreedom
27. Young Voices