



# Regulating Big Tech: Legal Implications

Valerie C. Brannon, Coordinator  
Legislative Attorney

Updated September 11, 2019

*This Sidebar will be regularly updated to include additional CRS products in the list at the end.*

Amidst [growing debate](#) over the legal framework governing social media sites and other technology companies, several [Members of Congress](#) have [expressed interest](#) in expanding current regulations of the major American technology companies, often referred to as “Big Tech.” This Legal Sidebar provides a high-level overview of the current regulatory framework governing Big Tech, several proposed changes to that framework, and the legal issues those proposals may implicate. The Sidebar also contains a list of additional resources that may be helpful for a more detailed evaluation of any given regulatory proposal.

## Current Regulatory Landscape

The “[big five](#)” tech companies—Alphabet (Google’s parent company), Amazon, Apple, Facebook, and Microsoft—play a [critical](#) role in today’s [marketplace](#) and in [society at large](#). As [commentators](#) have [pointed out](#), the technology industry has largely developed free from any significant federal regulation, particularly when viewed in contrast to potentially analogous industries such as [radio, television, or telephone services](#). There are no omnibus federal laws akin to the [Communications Act](#) or the [Federal Aviation Act](#) governing the industry as a whole. Instead, the internet has largely operated under a [system of self-governance](#). In fact, one federal law has partially shielded online service providers from lawsuits that might otherwise limit their conduct: [Section 230](#) of the Communications Decency Act of 1996 (CDA) [immunizes](#) many online platforms that serve as hosts for user-generated content from some lawsuits that would impose liability on these platforms for their content-publishing activities. Section 230 immunity is not absolute, though. Among other exceptions, the law [does not shield](#) online platforms from prosecution under federal criminal statutes—and does not shield platforms from liability for their *own* content. Nonetheless, Section 230 does broadly protect platforms’ content-hosting activities.

This is not to say, however, that the internet is a [completely lawless zone](#) or that there is no federal regulation of the internet. Individual platforms and their users may be held accountable for actions they take online. For example, the Department of Justice (DOJ) has indicted a [number of sites](#)—including

Congressional Research Service

7-5700

[www.crs.gov](http://www.crs.gov)

LSB10309

[Backpage.com](#)—under various criminal statutes, alleging that the platforms unlawfully facilitated prostitution. Internet platforms may also be subject to liability under certain federal laws such as the [Digital Millennium Copyright Act](#), which generally governs the protection of copyrights online. Additionally, the Federal Trade Commission (FTC) Act’s [prohibition](#) of “unfair or deceptive acts or practices” (UDAP) applies to most internet platforms and users, and the FTC actively enforces this prohibition. Indeed, [reports suggest](#) that the FTC [may soon impose fines](#) on Facebook as part of [an ongoing investigation](#) into whether Facebook’s privacy practices violated a 2011 consent decree that settled UDAP allegations. The FTC has also [indicated](#) that social media influencers’ failure to disclose any connections to marketers of products that they endorse may be a UDAP violation.

Along with internet platforms and users, companies that provide internet access—often [referred](#) to as broadband internet access service (BIAS) providers—are [currently subject](#) to the FTC Act’s UDAP prohibition. However, there have been attempts to more comprehensively regulate BIAS providers through [net neutrality regulation](#). In particular, although it ultimately reversed its decision in 2017, in 2015 the Federal Communications Commission (FCC) issued the [Open Internet Order](#), in which it classified BIAS providers as common carriers subject to various obligations under [Title II of the Communications Act](#). Among other things, the 2015 Order would have [prohibited](#) BIAS providers from blocking or throttling (i.e., degrading) lawful internet traffic or from engaging in “paid prioritization” (i.e., favoring some internet traffic over other traffic in exchange for consideration). Further, while the Open Internet Order was still in effect, the FCC issued a [rule](#) under its Title II authority that would have required BIAS providers to comply with various data protection requirements, such as [consumer consent](#), [data security](#), and [data breach notification](#) requirements. However, Congress subsequently [overturned](#) this rule pursuant to the [Congressional Review Act](#).

## Proposals for New Regulations

As noted above, commentators and politicians have increasingly expressed concern about how technology companies have regulated themselves thus far. For example, to the extent that these companies serve as platforms for creating and sharing content, [many](#) have alleged that the platforms allow (or even [promote](#), intentionally or unintentionally) the proliferation of false or harmful content. On the other hand, [some](#) have [argued](#) that these platforms have gone too far in policing content posted on their sites and have improperly taken down or otherwise filtered valuable content. Another significant source of [criticism](#) comes from how these companies handle user data: inadequate corporate privacy practices and intentional intrusions into private computer networks have [exposed](#) the personal information of millions of Americans. In some cases, companies [intentionally collect](#) or [use](#) personal data in ways that may not comport with many users’ privacy expectations. And underlying these concerns is the [idea](#) that relatively few companies have come to occupy [significant market positions](#), creating the [specter](#) of [monopoly power](#) and leaving consumers with [little option](#) but to accept the terms of these major services if they want to participate in modern life.

Scholars and elected officials have proposed a wide variety of regulations to address these concerns. Perhaps most widely discussed, in late March, Mark Zuckerberg, the founder and chief executive of Facebook, [called for](#) “regulation in four areas: harmful content, election integrity, privacy and data portability.” While Zuckerberg’s proposals were [met](#) with [some skepticism](#), his suggestions are only some of the many policy proposals that would tackle a variety of issues concerning Big Tech. The table below introduces just a few of these proposals. This Sidebar does not evaluate the merits of these proposals, which have been [subject](#) to [significant policy debate](#). Instead, the Sidebar focuses on the various legal issues these policy proposals may raise.

| General Policy Area                        | General Policy Proposals, Examples of Proposed Federal Legislation or Regulation or Existing State or International Laws  |
|--|---|
| <b>Section 230 Immunity</b>                | <p>Repealing or amending the CDA's <a href="#">Section 230</a> to limit the immunity provided to internet platforms that host others' content</p> <p>e.g. - The <a href="#">Biased Algorithm Deterrence Act of 2019</a> would provide that social media services "shall be treated as a publisher or speaker" of certain user-generated content if they display it "in an order other than chronological order"</p>   |
| <b>Content Moderation</b>                  | <p>Creating an <a href="#">independent body</a> to set <a href="#">standards</a> for content moderation, and possibly to <a href="#">review</a> sites' decisions about what kind of content to allow on their platforms</p>   |
| <b>Foreign Influence in U.S. Elections</b> | <p>Requiring <a href="#">platforms</a> to make disclosures and statements of attribution or "disclaimers" to users, including identification of who paid for certain political <a href="#">advertisements</a></p> <p>e.g. - The <a href="#">Honest Ads Act</a>, incorporated with some changes into <a href="#">H.R. 1 (116th Cong.)</a> and reintroduced as a stand-alone bill in the Senate as <a href="#">S. 1356 (116th Cong.)</a>, would extend federal campaign finance law disclosure and disclaimer requirements to online platforms for paid internet and paid digital communications</p>  |
| <b>Misinformation</b>                      | <p>Requiring platforms to identify or ban <a href="#">bots</a> or <a href="#">inauthentic accounts</a></p> <p>e.g. - California passed a <a href="#">law</a> in 2018 making it unlawful to use "an automated online account" to transmit certain communications</p> <p>e.g. - The <a href="#">DETOUR Act</a>, <a href="#">S. 1084 (116th Cong.)</a>, would prohibit large online services from conducting experiments on or manipulating users absent disclosure and informed consent</p>   |
| <b>Data Privacy and Protection</b>         | <p>Limiting platforms' ability to use consumers' data, or imposing <a href="#">statutes of limitations</a> on how long platforms may use data</p> <p>Requiring <a href="#">opt-outs</a> from or <a href="#">opt-ins</a> into certain uses of data</p> <p>Requiring platforms to be more <a href="#">transparent</a> about how they use consumer data</p> <p>e.g. - The <a href="#">California Consumer Privacy Act</a> and the European Union's <a href="#">General Data Protection Regulation</a> are aimed at protecting users' data in various ways</p> <p>e.g. - The <a href="#">Do Not Track Act</a>, <a href="#">S. 1578 (116th Cong.)</a>, would require the FCC to implement a system to allow consumers to opt out of tracking, and punish companies that disregard consumers' preferences</p> |
| <b>Antitrust</b>                           | <p><a href="#">Applying antitrust law</a> to "break up Big Tech"</p> <p>e.g. - DOJ and FTC are <a href="#">reportedly considering investigating</a> certain tech companies</p>  |
| <b>Industry-wide Duties</b>                | <p>Treating online platforms similarly to other <a href="#">media companies</a> or <a href="#">public utilities</a> that the FTC and FCC would regulate and imposing a <a href="#">duty to deal</a> (i.e., requiring platforms to neutrally serve consumers on a first-come, first-served basis), or <a href="#">duties of care</a> (e.g., requiring platforms to prevent or mitigate harms to users)</p> <p>e.g. - The <a href="#">Save the Internet Act of 2019</a>, <a href="#">H.R. 1644 (116th Cong.)</a>, would reclassify BIAS providers as common carriers by reinstating the FCC's Open Internet Order</p>   |

## Possible Legal Issues

**Section 230.** The CDA's [Section 230](#), discussed above, immunizes online service providers from a wide variety of federal and state lawsuits. When crafting new laws regulating technology companies, Congress could allow governments or private parties to hold service providers liable for their decisions to publish or restrict access to certain types of content. Congress may consider creating an express exemption from Section 230, akin to the [Allow States and Victims to Fight Online Sex Trafficking Act of 2017](#), which expressly provided that Section 230 immunity would not apply in federal civil actions and state criminal

prosecutions that mirror specified federal offenses. Without an express exemption to Section 230, legal questions could arise as to how new laws imposing liability on service providers for publishing certain content interact with Section 230's general immunity provisions.

**First Amendment.** Any of the general proposals discussed in this Sidebar could raise First Amendment concerns, depending on the precise contours of a given regulation. Internet platforms may raise a variety of [free speech challenges](#) to federal regulation. The Supreme Court has [said](#) that “the creation and dissemination of information are speech,” suggesting that a broad array of internet content could be constitutionally protected. A law that regulates internet content on the basis of “[the topic discussed or the idea or message expressed](#)” or that imposes different burdens based on the [speaker](#) may be subject to heightened scrutiny under the Free Speech Clause of the First Amendment. However, there are certain, limited [categories of speech](#) that the government may regulate more readily because of their content. For example, these categories may define the scope of the [government's ability to restrict online content promoting terrorism or violence](#), given that categories of speech such as incitement and true threats have long received more limited First Amendment protection. Apart from government acts prohibiting certain types of speech, regulations that compel additional speech may also raise free speech concerns. Disclosure requirements may be seen as “[content-based regulation\[s\] of speech](#),” although courts may be more likely to uphold [disclosure requirements in the context of commercial speech](#). Disclosure requirements that apply to [political speech or communications related to elections](#) may be subject to a different analysis.

**Data Privacy and Protection.** The legal paradigms governing the security and privacy of personal data are complex and technical, and lack uniformity at the federal level. Should Congress consider a comprehensive federal data protection law, its legislative proposals may involve numerous decision points and legal considerations. Issues may include the law's conceptual framework (i.e., whether it is [prescriptive](#) or [outcome-based](#)), its [scope and definition](#) of protected information, the role of the FTC or another [federal enforcement agency](#), or external [constitutional constraints](#) on Congress's ability to regulate data privacy.

**Common Carrier Classification of BIAS Providers.** As mentioned above, legislative proposals such as the [Save the Internet Act](#) would reinstate the FCC's Open Internet Order and reclassify BIAS providers as common carriers under Title II of the Communications Act. The FCC's Open Internet Order was subject to a number of legal challenges, although it was ultimately [upheld](#) by the U.S. Court of Appeals for the D.C. Circuit. (The D.C. Circuit [denied](#) a petition to reconsider this decision *en banc*, over the [dissent](#) of then-Judge Brett Kavanaugh.) These challenges included concerns about whether the FCC's actions were consistent with the Communications Act; whether the FCC had sufficiently justified its decision to reclassify BIAS providers; and whether some of the rules violated the First Amendment. While some of these concerns may be obviated by congressional action, there may be additional legal considerations raised by any new regulation in this area. For instance, reclassifying BIAS providers as common carriers may create legal uncertainty over the nature of their data protection obligations, as it would remove them from the [FTC's jurisdiction](#).

**Antitrust.** [Antitrust law](#) offers several tools that might apply to the regulation of Big Tech. For example, the Clayton Act [prohibits](#) any merger that could “substantially [] lessen competition, or [] tend to create a monopoly” and could theoretically be used to [unwind](#) arguably problematic mergers, like the Facebook–Instagram merger from 2012 or Alphabet's acquisitions of Waze and Nest in 2013 and 2014, respectively. Similarly, [Section 2](#) of the Sherman Act makes it unlawful to monopolize or to conspire to monopolize a marketplace. Some have [argued](#) that Facebook or Alphabet have engaged in exclusionary conduct that justifies monopolization charges under Section 2, which could be used to break those companies up or force them to change certain anticompetitive business practices.

Ultimately, any antitrust litigation against these firms would raise complicated legal and empirical questions. For instance, while the government can unwind a [past merger](#) under the Clayton Act, it would

have to [show](#) how the merger meaningfully decreased competition in a particularly defined marketplace. Depending on the merger in question, this would raise a number of novel legal questions surrounding [market definition](#) in dynamic technology industries. For example, some [commentators](#) have questioned whether Facebook’s market should be defined with reference to potential members of its social network, advertising on the internet, or advertising writ large. These matters and other difficult questions would persist in a monopolization prosecution. Significantly, in a monopolization case, the government generally has to show that a defendant possesses [market power](#), which is usually defined as the ability to profitably raise prices above competitive levels. [Some](#) have [pointed out](#) that because many tech companies do not charge users for their services, demonstrating a monopoly may be more complicated. Further, a showing of market power often requires proof that the defendant-firm is insulated from new rivals by [barriers to entry](#). Alphabet CEO Larry Page has argued that the firm’s potential competitors are “[only a click away](#).” However, others, including [European antitrust authorities](#), have argued that many digital markets possess certain structural features—including increasing returns to scale, economies of scope, and network effects—that make entry uniquely difficult. [Commentators](#) do not agree on how to resolve these tensions. Any antitrust approach would pose numerous [practical](#) challenges, such as how to “unscramble” entities that have been merged for a significant period of time. These issues, and others, would likely need to be considered if antitrust law were to be employed to regulate big tech.

---

**The following CRS Products provide more information on the issues discussed above:**

---

CRS Legal Sidebar LSB10306, *Liability for Content Hosts: An Overview of the Communication Decency Act’s Section 230*, by Valerie C. Brannon

CRS Report R45650, *Free Speech and the Regulation of Social Media Content*, by Valerie C. Brannon

CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion

CRS Report R45713, *Terrorism, Violent Extremism, and the Internet: Free Speech Considerations*, by Victoria L. Killion

CRS Report R45700, *Assessing Commercial Disclosure Requirements under the First Amendment*, by Valerie C. Brannon

CRS Report R45320, *Campaign Finance Law: An Analysis of Key Issues, Recent Developments, and Constitutional Considerations for Legislation*, by L. Paige Whitaker

CRS In Focus IF10758, *Online Political Advertising: Disclaimers and Policy Issues*, by R. Sam Garrett

CRS In Focus IF11207, *Data Protection and Privacy Law: An Introduction*, by Stephen P. Mulligan, Chris D. Linebaugh, and Wilson C. Freeman

CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh

CRS Legal Sidebar LSB10303, *Enforcing Federal Privacy Law—Constitutional Limitations on Private Rights of Action*, by Wilson C. Freeman

CRS Insight IN10879, *Data, Social Media, and Users: Can We All Get Along?*, by Chris Jaikaran

CRS Report R40616, *The Net Neutrality Debate: Access to Broadband Networks*, by Angele A. Gilroy

CRS In Focus IF10955, *Access to Broadband Networks: Net Neutrality*, by Angele A. Gilroy

CRS In Focus IF11234, *Antitrust Law: An Introduction*, by Jay B. Sykes

CRS Report R45910, *Antitrust and “Big Tech”*, by Wilson C. Freeman and Jay B. Sykes

---