CENTER FOR DEMOCRACY & TECHNOLOGY

March 9, 2022

Dear Senator Klobuchar and Senator Grassley:

Since our founding over twenty-five years ago, the Center for Democracy & Technology has devoted its efforts to promoting privacy, free expression, and other human rights online and to securing and protecting an open internet where competition thrives. Competition gives consumers options, which gives companies a free-market incentive to act in the interests of consumers, and to constantly work to improve their products and services in every respect important to consumers. This is no less important in the online marketplace than elsewhere in the economy. Affordability, quality, and innovation all suffer when competition is lacking.

We are therefore encouraged by the progress being made in Congress to update our antitrust laws to address competition problems in the digital marketplace, where a handful of dominant online platforms have too much market power and that free-market incentive is not activated as it should be.

A prominent example of this progress is your bill, S. 2992, the American Innovation and Choice Online Act, which was recently approved by the Senate Judiciary Committee on a strong bipartisan vote. Like its counterpart in the House, H.R. 3816, it would prohibit a covered online platform from preferencing its own products and services sold or provided on the platform by discriminating against products and services of competing businesses who depend on the platform to reach their customers.

As this bill has moved through the legislative process, it has been further shaped to bring its focus more clearly on its goal of promoting and protecting competition, and to clarify and strengthen protections against unintended adverse consequences, thereby placing the bill on stronger and sounder footing at every stage.

We are writing regarding two concerns that would benefit from further attention. First, the bill, in opening up the covered online platforms to competition, could undermine the ability of these platforms to protect personal and business data against unauthorized access and misuse. Second, some of the protections given to platform business users could unduly interfere with the platforms' responsible efforts to curb hate speech, disinformation, or other abusive content, injecting the government into second-guessing these decisions and impeding platforms' ability to counter abuse of their services.

These are very significant concerns, and we are encouraged that you and other Committee Members are taking them seriously, and have been working to address them, already making a number of changes to the bill. We urge you to continue those constructive efforts and remain open to making further changes to improve the bill as it is prepared for consideration by the full Senate.

To that end, we offer the following observations and recommendations:

Privacy and Security Protection

The bill effectively gives virtually any company that competes (or proposes to compete) with a covered platform the right to access and interoperate with the platform and its operating system, hardware, and software, to the same extent as the platform itself. This has a potential to create significant risks, especially considering the many types of sensitive information stored by these platforms, such as location, biometric and password information, and the threat that malware can pose to an operating system.

The bill recognizes these risks, and explicitly provides an affirmative defense for steps a platform might undertake to protect users' privacy and security. But the hurdles to invoke this defense are more substantial than need be to further the bill's pro-competitive purpose. The resulting uncertainty, in combination with the potentially devastating civil penalties, would likely disincentivize a platform from implementing responsible privacy and security protections.[1]

In order to successfully rely on this defense, a platform would have the burden of proving (now, by a preponderance of the evidence) that the conduct at issue was

> narrowly tailored, could not be achieved through less discriminatory means, was nonpretextual, and was reasonably necessary to … protect safety, user privacy, the security of non-public data, or the security of the covered platform.

The bill does not define these terms, and thus they would await interpretation by the courts; but in other contexts, similar proof requirements are difficult to meet. For example, "narrowly tailored" is a key portion of the "strict scrutiny" test that courts apply to state actions that allegedly infringe constitutional rights and is extremely difficult to satisfy.

The undefined but seemingly strict requirements for invoking the affirmative defense are coupled with the prospect of substantial liability – civil penalties amounting to as much as

[1] Although the bill has been helpfully amended in the Senate to clarify that this and other prohibitions apply only when a practice would materially harm competition, this does not adequately address the uncertainty. In practice, the effect on competition would be determined by a court in litigation, in a fact-specific analysis under a rule of reason. And in the case of the interoperability and access requirement in (a)(4), the burden of proof would lie with the platform.

15 percent of the platform's entire United States revenue for the period of time the violation occurred, which could potentially be months or even several years. The bill further provides that corporate officers of the platform can potentially be ordered to forfeit a full year's compensation for a "pattern or practice" – which could be a course of conduct in which the officer has engaged in good faith over some period before it is determined to be a violation.

The combination of a difficult privacy-and-security defense standard and high penalties would likely disincentivize covered platforms from taking responsible steps to protect their users' security and privacy if they might plausibly be alleged to violate one of the prohibitions in the bill – as well as chilling security teams' ability to act quickly. Federal policy should not dissuade platforms from protecting their users' privacy and security.

To be sure, a covered platform may use privacy and security as a pretext for anticompetitive self-preferencing, and the law should guard against that. Thus, the requirement that a platform prove the conduct at issue was "reasonably necessary to" protect privacy and security makes sense as the core of the affirmative defense. But the other elements would create a higher burden that will depend on judgments of the enforcers and the courts, and that goes beyond what is needed.

Narrow tailoring in particular will be extremely difficult for a platform to be confident it can satisfy to enforcers and courts, and is likely to undermine privacy and security. Narrow tailoring is not necessarily a virtue when addressing a data or platform security threat. Rather than implementing a narrowly tailored solution to each new security threat, the safer course may be a broader solution to address not only the specific current threat, but also how that threat is foreseeably evolving. Responsibly taking that safer course should not automatically put the platform in legal jeopardy. Ultimately, courts would be left to sort this out, but they are not well-positioned to assess whether a particular security solution could have been more narrowly tailored and still have addressed the threat at issue. And that is even more the case in the context of the emergency injunctive relief provided in the bill, under which platforms could be blocked from taking security and privacy-protective actions, based on a mere showing of a "plausible claim, supported by evidence," for as long as 120 days – ample time for the data of millions of people to be stolen.

These concerns can be addressed, without compromising the pro-competitive purpose of the bill, by making the following revisions:

- Remove "narrowly tailored" as an element of the affirmative defense. It is essentially already implicit in the core "reasonably necessary" element, but its absolute nature nullifies the "reasonably" part of that other element.

- Shift the burden on the "nonpretextual" and "no less discriminatory means" elements to the government, once the platform has shown that the restriction is reasonably necessary to protect safety, privacy, or security. It is difficult to see how the platform could prove the negative that the action was not pretextual or more discriminatory than

necessary; and in the civil rights and antitrust rule-of-reason contexts, those elements are ultimately the plaintiff's or government's burden to prove, once the defendant has presented evidence to put the matter in issue.

- Consistent with other provisions of subsection (a), place the burden of proof on the government to show material harm to competition from restrictions on interoperability and access, by adding ", in a manner that would materially harm competition" at the end of subsection (a)(4) of the Manager's Amendment, adding a reference to subsection (a)(4) in subsection (b)(1), and removing the reference to it from subsection (b)(2).

- Clarify that the pattern or practice of violations, for which a covered platform's corporate officers are subject to forfeiture, is a knowing pattern or practice, by adding the word "knowingly" before "violating" in subsection (c)(5)(D).

- Re-balance the temporary injunction provision in subsection (c)(5)(C)(ii) by clarifying that (a) notice to the platform is required, with the opportunity for a hearing, before the injunction can take effect; (b) the platform can raise any of the affirmative defenses; and (c) the government must make the usual showing of likelihood of irreparable harm to justify an injunction before a full hearing on the merits.

These revisions would help ensure that the bill does not discourage platforms from protecting user privacy and security, particularly for users who do not have the knowledge or desire to invest the time needed to make their own determinations about how best to protect their privacy and security. It would be preferable if we were not so dependent on private platforms to provide this protection. That is why CDT has long called for comprehensive federal privacy legislation with strong enforcement mechanisms. With such a law in place, business users of the platforms would have their own independent legal obligations to protect user privacy and security, and users would potentially have recourse against them if they failed to do so. Particularly in the absence of such a law, but even after one is eventually enacted, it is essential that the platforms not be inhibited by unnecessary legal uncertainty from helping protect those important consumer interests, when that uncertainty can be alleviated without compromising the pro-competitive purpose of the bill.

Content Moderation

Similarly, the bill as currently approved by the Judiciary Committee could inhibit responsible efforts by a covered platform to curtail hate speech, disinformation campaigns, or other abusive content that may nevertheless be protected by the First Amendment, and thus beyond Congress's ability to regulate. By authorizing the government to take enforcement action against those efforts, the bill risks chilling important moderation decisions that responsibly address abuse and that support the participation of a diverse array of Americans in online life.

Section 3(a)(3) of the Manager's Amendment would make it unlawful to "discriminate in the application or enforcement of the terms of service of the covered platform among similarly situated business users in a manner that would materially harm competition." The Manager's Amendment also broadens the definition of "business user" to now include advertising products or services on a platform, as well as selling or otherwise providing them.

Section 3(a)(3) would thus authorize the Federal Trade Commission, the Attorney General, or any of 56 state and territory attorneys general to charge that a covered platform's decision to remove a post or account or application of any business user for violating the platform's terms of service in fact discriminated against that user. Given the scale at which content moderation operates, honest errors are inevitable. Moreover, content moderation often involves difficult judgment calls on which reasonable people acting in good faith may disagree. As a result, there will be instances in which it will be simple to allege that one business user that was the subject of a corrective action by the platform was treated differently than an allegedly similarly situated business user that wasn't the subject of the same corrective action.

The requirement that it be shown that the alleged discrimination would materially harm competition, while a helpful focusing clarification of the bill's purpose, is not adequate to prevent abusive weaponization of this government enforcement power. It is easy to foresee claims that, for example, the alleged discrimination was a symptom of systematic bias that harms competition.[2] As indicated above, the effect on competition would ultimately be determined by a court in litigation, in a fact-specific analysis under a rule of reason.

As we have seen in the wake of FOSTA-SESTA,[3] such lawsuits would not have to be successful in court to be effective at chilling platforms' responsible content moderation decisions. Just the increased risk of lawsuits over those decisions, and of investigations that might or might not lead to enforcement actions – including the ability of government officials to conduct discovery concerning them – could further discourage platforms from taking much-needed steps to combat hate and disinformation on their services.[4] We have already seen efforts at the state level to use investigatory authority to pressure a platform to ease up on content moderation with which the attorney general disagreed politically.[5] Further, some

---

[2] Taylor Soper, Parler Files Lawsuit Against Amazon After Getting Kicked Off Amazon Web Services, GeekWire (Jan. 11, 2021), https://www.geekwire.com/2021/parler-files-lawsuit-amazon-getting-kicked-off-amazon-web-services/.

[3] *See* Fosta in Legal Context, Columbia Human Rights L Rev. 52:3, 1084-1158 (2021), http://hrlr.law.columbia.edu/files/2021/04/1084_Albert.pdf.

[4] *See, e.g.*, Free Press, Provision in Senate Antitrust Bill Would Undermine the Fight Against Online Hate and Disinformation, https://www.freepress.net/news/press-releases/provision-senate-antitrust-bill-would-undermine-fight-against-online-hate-and-disinformation.

[5] *E.g.*, AG Paxton Issues Civil Investigative Demands to Five Leading Tech Companies Regarding Discriminatory and Biased Policies and Practices, Jan. 13, 2021, https://www.texasattorneygeneral.gov/news/releases/ag-paxton-issues-civil-investigative-demands-five-leading-tech-companies-regarding-discriminatory; *see* Twitter, Inc. v. Ken

states are passing laws to facilitate the ability of their AGs to use their enforcement authority to coerce platforms to carry content they would otherwise moderate as dangerously false, hateful, or abusive.[6] These laws have each been preliminarily enjoined under the First Amendment, but they reflect a clear desire by some states to bring aggressive litigation against social media services' content moderation practices under claims of discrimination.

The fights over whether and how online services moderate user-generated content can be messy and fierce. But a bill seeking to promote competition in the tech industry is not a place to attempt to resolve them.

As with the privacy and security concerns, this concern can be readily addressed. Section 3(a)(3) as written is the source of the concern. Indeed, it is the only part of the bill that does not address the bill's core goal of stopping anticompetitive self-preferencing by covered platforms. It could be removed without compromising that goal. Alternatively, language could be included in the subsection, or as a rule of construction, making clear that decisions concerning content moderation are out of scope – and in conjunction with that, perhaps narrow the prohibition to focus on instances in which one business user pays the platform for discriminating against another business user.

However it does so, Congress should amend the bill so that it does not through a back door create disincentives to content moderation or even force platforms to host business users that traffic in disinformation or other harmful content.

Incorporating our recommended revisions will focus the bill more clearly, and avoid unnecessary collateral risks to other important values, without compromising its important purpose of strengthening our laws against anticompetitive self-preferencing by large online platform gatekeepers. Indeed, increased competition can be well-aligned with privacy, security, and free expression online by providing consumers with choices among competing services that have strong incentives to continually improve to meet consumer needs. We respectfully urge you to adopt our recommendations.

We look forward to working with you and others on the Committee and in Congress to address the problem of entrenched market power, so that the online marketplace can function

---

Paxton, Brief of Amici Curiae Center for Democracy & Technology et al in support of Plaintiff-Appellant Twitter, Inc. Urging Reversal, https://cdt.org/wp-content/uploads/2021/07/2021-07-23-Twitter-Ken-Paxton-26-CDT-Amicus-Br.pdf.

[6] *See, e.g.*, CDT, Florida Social Media Law Prioritizes Politicians Over the Public, June 17, 2021, https://cdt.org/insights/florida-social-media-law-prioritizes-politicians-over-the-public/; CDT Joins Amicus Brief in Netchoice v. Paxton, Oct. 8, 2021, https://cdt.org/insights/cdt-joins-amicus-brief-in-netchoice-v-paxton/.

in a manner that gives consumers, and all who seek to reach them, the benefits of competition and the choices and innovation it fosters.

Sincerely,

Samir Jain, Director of Policy
George Slover, General Counsel & Senior Counsel for Competition Policy
Emma Llansó, Director of Free Expression Project
Eric Null, Director of Privacy & Data Project

cc: Members, Senate Judiciary Committee
Hon. David N. Cicilline
Hon. Ken Buck