WRITTEN TESTIMONY OF

DANIEL FRANCIS

ASSISTANT PROFESSOR OF LAW

NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE U.S. SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

FOR A HEARING ENTITLED

"REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITION TO OUR DIGITAL MARKETS"

MARCH 7, 2023

TABLE OF CONTENTS

I. INTRODUCTION AND EXECUTIVE SUMMARY

Chair Klobuchar, Ranking Member Lee, Members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Daniel Francis. I am an Assistant Professor of Law at NYU School of Law, where I teach and write about antitrust. My academic work currently focuses on ways to reinforce our antitrust laws, in digital and other markets, without sacrificing principle or rigor.[1] I am also a former federal antitrust enforcer: from May 2018 to January 2021, I served in the antitrust arm of the FTC as Senior Counsel, Associate Director for Digital Markets, and ultimately Deputy Director. My work at the FTC focused on digital and platform antitrust, including among other things the Facebook (now Meta) monopolization investigation and litigation, which challenged the acquisitions of Instagram and WhatsApp as well as the application of certain platform policies. Before joining the FTC, I spent a little more than ten years in private practice.

I do not work for or represent any private clients, and I have not done so since joining the FTC in May 2018. I have no brief in testifying today other than my interest in protecting consumers and supporting the antitrust system, particularly in digital markets.

I strongly support vigorous antitrust enforcement, including in digital, platform, and high-technology markets. In particular, I support: (1) significantly increasing the funding and staffing of our antitrust agencies, which have fallen far off the pace (for example, from FY 1979 to FY 2021, the volume of HSR merger filings has increased to more than *four times* what it was in

[1] *See, e.g.*, Daniel Francis, *Making Sense of Monopolization: Antitrust and the Digital Economy*, 84 Antitrust L.J 779 (2022) (proposing a principled reinforcement of monopolization law); Steven C. Salop, Daniel Francis, Lauren Sillman, and Michaela Spero, *Rebuilding Platform Antitrust: Moving on from* Ohio v. American Express, 84 Antitrust L.J. 883 (2022) (proposing a balanced approach to platform antitrust after *AmEx*); Daniel Francis, *Revisiting the Merger Guidelines: Protecting an Enforcement Asset*, Comp. Pol'y Intl. (Nov. 2022) (proposing protection of the guidelines' status as a trusted enforcement tool).

FY 1979, while the FTC's full-time-equivalent ("FTE") staffing utilization declined by more than a third over the same period[2]); (2) increasing support for state antitrust enforcement; and (3) reinforcing our core antitrust statutes to restore vigor and reduce ambiguity, and adding merger review time for the most troubling deals, to save agencies and businesses from kneejerk decisions.

I would also support (4) some regulation of digital platform markets, *if targeted to specific practices and in the interests of consumers*. This could include, among other things: (a) transparency and disclosure obligations in ad-tech markets; (b) consumer transparency obligations to require disclosure of paid advertising that resulted in improved search rankings or preferred placement; (c) a targeted ban on the use of most-favored-nation ("MFN") clauses by digital platforms with significant market or monopoly power, in markets in which the harms from MFNs would generally outweigh their benefits; and (d) market-specific interoperability or portability obligations for businesses with significant market or monopoly power, targeted at markets in which such obligations could be reasonably defined and enforced, and subject to robust defenses to protect consumers, businesses, and platforms.

But I do not recommend enacting AICOA, nor do I recommend enacting OAMA in its current form. In summary, my views are as follows.

A. AICOA

I think AICOA pursues an important and valuable goal—competition in digital markets—but it does so in the wrong way, and at much too high a price for American consumers. The bill centrally demands that our economy's largest platforms should do *less* for consumers and *more*

[2] Even with recent funding increases, projected FTC staffing for FY 2023 will be around 83% of FY 1979 FTE utilization. *See infra* § IV.A.

for other businesses. In the process, I think AICOA will end up deterring beneficial practices and business models, giving a helping hand to bad actors, and triggering a generational landslide of confusion and costs. It aims at Big Tech, but it will hit consumers, and I do not think its uncertain benefits justify its evident costs and risks.

I also fear the broader implications of regulation so obviously aimed at a set of particular businesses. AICOA targets some politically unsuccessful, but very different, businesses for a unique, uniform package of regulatory burdens disconnected from market power tests. Congress has historically refrained from using antitrust or competition policy to pick individual winners and losers in our economy. I deeply fear the present and future costs of leaving that path.

The heart of AICOA is a prohibition against "self-preferencing." But a ban on self-preferencing would prohibit or deter an array of valuable practices that benefit consumers, including through product improvements, feature innovations, new market entry, and low prices. "Self-preferencing" as AICOA defines it includes a host of product improvements that are clearly desirable: adding a Google Maps widget in a Google Search results page; preinstalling Apple Maps on an iPhone; including Microsoft applications with Microsoft Windows; making Prime Video available for free to Amazon Prime subscribers; promoting in-house content on Apple+ and Prime Video; and so on. I cannot imagine why we would want to define an offense that includes such practices! Platforms should be free to improve, integrate, distribute, add, and promote features, products, and services—even when they cannot or would not do so, or would do so less, under a forced-sharing regime covering a limitless array of third parties.

AICOA threatens other harms too. Under AICOA, covered platforms will live under the dangling sword of lengthy investigations and litigations: including the threat of disruptive interim

injunctive relief, which AICOA makes available on a specially lowered threshold, and the prospect that responsible executives will personally have to forfeit their compensation. As a result, platforms will be deterred from protecting consumers by denying access, preinstallation, distribution, and so on to third-party businesses, *even when the platform has reasonable grounds for concern.* Those grounds might be, for example, that an app or product might be buggy or badly interoperable with the platform; low-quality; spammy; objectionable in content (*e.g.*, sexually explicit material or the promotion of terrorism and violence); malicious; controlled or influenced by or vulnerable to a hostile power; very costly to integrate; and so on.

This deterrent effect will bite in cases where AICOA's narrow affirmative defense does not apply—it does not cover most of the grounds just described—as well as in cases where the platform could not or does not want to go fifteen rounds with the FTC to defend the decision, nor to run the risk of a massive fine and an injunction. Forcing executives to bet their own compensation when they say "no" instead of "yes" to a third party magnifies the problem.

Of course, some of those close and borderline cases will involve good actors and great products that will obtain platform access as a result of AICOA. That will certainly be a benefit. But more bad actors will still get through the door, even if the changes are made at the behest of, and in hope of helping, legitimate competitors! I do not think there is much room to doubt that AICOA will result in more bad actors and more bad products—ranging from the malicious and sinister to the merely buggy and spammy—getting access to platforms, data, consumers, devices, and ecosystems. As the Internet of Things expands and more devices go online, this means more bad actors getting easier access to consumers' lives and homes.

I think this is too high a cost. There are plenty of hostile and malicious actors in the world today searching constantly for new ways to access consumers' devices, data, and homes. And it seems a particularly bad time to make our critical digital infrastructure more vulnerable by deterring our most important platforms from protecting their own systems and users. Platform decision-makers should not be given a choice of *either* letting suspicious third-party apps and entities into their ecosystems *or* facing the threat of complaints, investigations, litigations, injunctions, and penalties (and the forfeiture of their personal compensation!).

As I read it, AICOA also presents a sharp challenge to two business models that are associated with real consumer benefit. First, it threatens the operation of free-to-use, ad-supported businesses, where the provision of free services is made possible by preferencing the platform owner's own advertising, or a service that carries it. Deterring businesses from using that model—and driving them toward fee-paying models—does not seem likely to benefit consumers overall. Second, it also threatens closed or partly closed systems which offer users and businesses a secure, seamless option. But cybersecurity experts overwhelmingly emphasize the safety benefits of closed systems, and of platform-owners' power to restrict and deny access to third party code.

I do not think AICOA's qualifying provisions—a harm to competition test and two affirmative defenses—do much to save the legislation. As others have pointed out, AICOA doesn't explain whether this "harm to competition" test is supposed to be a consumer welfare test, an injury-to-rivals test, or something else, nor even whether it is intended to be construed consistently with antitrust jurisprudence. "Competition" does not, alas, have a single obvious meaning. Strategic ambiguity on this point in legislation of this scale and novelty seems highly undesirable.

And in forced sharing cases, I think the "harm to competition" test will be a dead letter in practice. Forced sharing virtually always seems good for competition *after an improvement has already been created*—why not make an already-created benefit widely available?—despite the harm to *future* investments and improvements that will be done by such a mandate. If the intention is to permit any self-preferencing that is reasonably related to incentivizing a procompetitive investment, AICOA should say so—but, of course, this would dramatically narrow the bill.

AICOA's general affirmative defense is too narrow and too demanding to offer much comfort. It does not protect, for example, denials of equal treatment based on: objectionable content (*e.g.*, sexually explicit content, promotion of terrorism or violence); false information; poor quality service; spam; fraud; consumer confusion; threat to the security of other ecosystem participants; and technological, commercial, or other difficulties and costs of integration. The product improvement defense is limited to improvements of "core" functionality (an utterly critical term that is inexplicably left undefined). And even a product improvement is unlawful if its objective "could be achieved" on a non-discriminatory basis: regardless of whether a rational or reasonable platform would be willing in practice to incur the necessary burdens, or whether it would be profitable to do so. And, in any event, a fact-specific defense—that a platform might or might not be able to prove to the satisfaction of an agency or court after months or years of expensive, disruptive investigation (perhaps with interim relief freezing its business in the process, and with penalties and injunctions hanging overhead, *and* with the decision-maker's personal compensation on the line!)—is going to be cold comfort to a platform in practice.

I wonder whether Congress might be centrally concerned with a *much* more specific problem: intentional, targeted, and unjustified discrimination against rivals of the platform

monopoly itself. Here the concern would *not* be that the platform is improving its own product while not doing so for third parties: the concern would be that the platform generally supplies something to the world already (whether or not it treats itself even better), and targets particular rivals for discrimination simply to forestall competition in the platform's own primary market. If this is indeed Congress's concern, it is a *much* narrower phenomenon than the broad array of conduct reached by AICOA. It could be addressed with a single short prohibition that would avoid most of the costs and harms that the existing draft threatens. There are, to be sure, reasons why Congress might not want to go even that far—it is after all not obvious that businesses, even big ones, should always have an affirmative obligation to subsidize and support their rivals—but a narrow ban on intentional, targeted, and unjustified discrimination against rivals of the platform monopoly would be *vastly* less harmful to consumers than the current version.

One final comment. By making existing digital platforms more comfortable for suppliers of complementary products and services—through extensive entitlements to certain kinds of access and favorable treatment—AICOA perversely *suppresses* incentives for competition against the platforms themselves. When the federal government forces a monopolist to treat me better, I become less interested in competing with it or supporting entrants or rivals (from whom I get no such special treatment). AICOA thus tends to perpetuate the dominance of covered platforms, turning would-be disrupters into cosy stakeholders in the status quo, while *also* restraining platforms' own competitive vigor. This seems to have everything backwards.

To sum up: AICOA is built on two premises—that self-preferencing is nearly always harmful, and that a general equal-treatment obligation is better for consumers—and I think each of them is wrong. Platforms should not be penalized for better serving consumers, even when they

cannot, would not, or should not serve other businesses on equal terms, or at all. Competition protected by antitrust, not monopoly entrenched and sedated by regulation, should be our goal.

B. OAMA

I think OAMA provides a better model, with respect to both scope and substance, for digital platform regulation than AICOA. I would support a version of OAMA that was limited to more targeted versions of some of its provisions, and that was supported by more robust defenses for platform conduct that protected consumers, business users, or the platform. But I do not support the bill in its current form.

The positives first. There is plenty to like in OAMA's basic design, including above all its specificity and granularity. OAMA is focused on two specific and reasonably well-defined set of markets that are important to digital competition, in which we might plausibly have a fairly consistent set of concerns. Namely: (1) markets for the sale and distribution of apps; and (2) markets for the provision of app-store services. OAMA seems unlikely to prohibit a wide range of product improvements and innovations. And it clearly reflects some effort to allow platforms to take reasonable measures for good reasons.

On substance, I also would support more targeted versions of some of OAMA's provisions:

- **App pricing MFN ban for app stores with significant market / monopoly power.** I would support a carefully targeted ban on the use of app pricing most-favored-nation ("MFN") clauses by app stores with significant market or monopoly power. Although these commitments can enable better pricing, they can also deter discounting by developers to other channels as a means of encouraging inter-platform competition. For example, if apps become cheaper on one platform than on another, the second platform may come under

competitive pressure to improve its own pricing. Or if a major app developer wants to support and sponsor a new entrant, it may discount to bring that entrant into the market. But an MFN commitment forces developers to share any such discounts with all MFN beneficiaries, thus making discounting more costly and less attractive. And an MFN that benefits an incumbent with market or monopoly power will prevent a developer from discounting to spur some competition against that incumbent.

- **Limited non-use obligation for competitively sensitive nonpublic information, for app stores with significant market / monopoly power.** I would cautiously support a limited ban on an app store's competitive use of competitively sensitive nonpublic business information received directly from the app developer as a condition of operating an app store, for app stores with significant market or monopoly power. As I explain below, I think the non-use obligation in the current draft is much too broad and would harm consumers. Just like supermarkets and other businesses, app stores should be able to use data generated by the store to improve its own products, even in competition with developers. They should also be able to buy and sell data in order to improve their own products and services. But one could reasonably fear that an app store might require developers to supply competitively sensitive nonpublic business information (such as app code, or advance notice of planned features) as a condition of participation on a store, in ways that would eliminate or erode developers' own incentives to invest in apps and app improvements. I am not sure that there is evidence this is a serious problem in practice, but a rule against it might do some good now or in future.

- **Disclosure obligation for preferred-placement advertising.** I would support a disclosure obligation that required app stores to disclose preferred placement in search results or rankings as a result of paid advertising. This would benefit consumers and harm no-one.

But I do not support the rest of OAMA. Most importantly, I fear that forcing covered companies to host third party app stores and in-app payment systems would compromise security and quality in ways that would expose consumers and others to serious harms and dangers. Cybersecurity experts *overwhelmingly* emphasize the dangers of third party app stores and of malicious apps. It is clear that official app stores, empowered with the ability and incentive to guard against hostile code and bad actors of all kinds, are the best hope of defending consumers from a proliferating array of threats. I think it would be a terrible cybersecurity mistake to breach these defenses and give third party app stores, and third party apps, a new weapon to force their way into digital ecosystems. In addition, I would apply a significant market or monopoly power test as a prerequisite for any obligations aimed at protection against competitive harms.

Finally, I also recommend limiting OAMA's enforcement to government authorities. Private enforcement—with the threat of treble damages, injunctive relief, and class actions—increases the risk that OAMA will be used in ways that do not serve the public interest.

*

The remainder of my written testimony is structured as follows: Part II addresses AICOA; Part III OAMA; and Part IV offers an alternative roadmap for supporting competition throughout the economy, including vigorous antitrust enforcement as well as some carefully targeted platform regulation.

II. THE AMERICAN INNOVATION AND CHOICE ONLINE ACT (S. 2992)

I have reviewed a draft of the American Innovation and Choice Online Act ("AICOA"), S. 2992, as reported to the Senate on March 2, 2022, and as further amended in a draft published by Senator Klobuchar, the bill's sponsor, on May 25, 2022.[3] For the reasons explained below, I do not recommend enacting AICOA.

A. Summary

The strongest case for AICOA, as I understand it, depends on two related claims. The first claim is that *platform self-preferencing is generally bad for consumers*. The second claim is that *a ban on self-preferencing would be better for consumers than the status quo*. I do not recommend enacting AICOA because I believe each of those claims is wrong. And I expect that enacting AICOA would harm consumers overall, not help them.

I believe that the first claim is wrong because "self-preferencing" includes a vast array of product improvements, feature innovations, and other practices (including those supporting new entry) that American consumers value enormously. Platform self-preferencing includes many familiar and beneficial practices, including for example: the integration of Google Maps information into Google Search results; the preinstallation of Apple apps on iOS devices; the preinstallation of Microsoft software on Windows computers; the special promotion on the Amazon and Apple+ platforms of their own in-house content; and the closer integration of in-house virtual assistants with platforms or in-house apps with virtual assistants.

[3] Draft available here: https://www.klobuchar.senate.gov/public/_cache/files/b/9/b90b9806-cecf-4796-89fb-561e5322531c/B1F51354E81BEFF3EB96956A7A5E1D6A.sil22713.pdf ("AICOA (May 2022 draft)"). In focusing on the May 25, 2022, draft, I follow the Congressional Research Service. Congressional Research Service, *The American Innovation and Choice Online Act* (Aug. 30, 2022); *see also* https://www.congress.gov/117/bills/s2992/BILLS-117s2992rs.pdf (version as reported May 2, 2022).

These and similar practices are good for consumers, even if the platform in question has market or monopoly power. Sometimes these practices will help to improve the interoperation of two existing products, services, or businesses; sometimes they will involve giving consumers additional benefits; sometimes they will play an important role in incentivizing and supporting entry by platform businesses into new markets. (For example, Apple's incentive to invest in creating and supporting Apple+ content, or Amazon's incentive to invest in creating and supporting Amazon Studios content, was clearly augmented by the opportunities for promotion on their respective platforms.) Indeed, *any* practice by an integrated business that makes products and services work better together is "self-preferencing" unless the business also makes the same improvement available to every other third-party business. It is routine throughout our economy, and I do not think Congress should legislate from the premise that it is a presumptive problem, either in general or in digital markets.

And I believe that the second claim is wrong because a ban on self-preferencing would actively harm consumers, in addition to whatever good it might do. I predict at least five separate kinds of harm. *First*, I expect that the ban would deter improvements and other practices that consumers value, including the practices described above. By telling platforms that they may not implement a product improvement unless they are able and willing to extend it to a limitless class of third parties seeking equal treatment, AICOA would lead to fewer new improvements, withdrawal of existing ones, and resulting consumer harm.

Second, I expect that the ban would deter platforms from protecting consumers, businesses, platforms, and even national security, in close or borderline cases. Under AICOA, denying third-party demands for equal treatment (preinstallation, high search ranking, access to consumer data,

etc.) threatens complaints, investigations, litigations, penalties, injunctions, and the personal forfeiture of compensation. At the *very* least this means significant costs, delays, and uncertainty. Platforms will therefore face an incentive to give in to third-party demands, and grant third parties access on equal terms, *even in cases where there are genuine grounds for concern*, if the platform fears that it may not ultimately be able to prove those grounds, or where the burdens and costs of trying to do so may be significant. (Or where a decisionmaker is just very risk-averse when it comes to putting his or her own salary on the line!) As a result, more bad actors will get access to platforms, consumers, and data. At a time when there is no shortage of hostile and malicious actors in the world seeking to harm the United States and its citizens, it is an odd time to encourage our most important platforms to lower their guard.

Third, I expect that the ban would threaten the provision of ad-supported business models, many of which involve providing free or low-cost services to millions of Americans through a business model that promotes a platform's own advertising channel. Prohibiting platforms from apps and functions that support those ad services (or even the ad services themselves, depending on the definition of "business user"[4]) strikes at the heart of the underlying business model that makes such free service possible. And if the result is to drive digital businesses to migrate from free-to-use, ad-supported business models to fee-based models, I fear that millions of Americans will pay more, and get less, than they do today. Free access to digital services is a critical tool for giving American families access to knowledge and opportunity. I think it would be unwise to make that model a losing proposition for our most critical digital businesses.

[4] *See infra* note 11.

Fourth, on the most natural reading, I expect that the bill would be read to prohibit or deter "closed systems" in which a business opts to run its system, in whole or part, without third-party participation.[5] Closed systems, or parts of systems, are common in the digital economy. For example, Apple does not allow third-party device manufacturers to participate in its iOS system, and Amazon does not allow third-party music streaming platforms to participate in its Amazon Prime ecosystem. (Outside the world of the covered platforms, it is also common: for example Disney does not generally allow third party content creators to participate in its Disney+ platform, and so on.) Closed systems are overwhelmingly associated with a more secure and more seamless experience for users. Banning that business model seems unwise and harmful.

Fifth, I expect that AICOA would perversely suppress interplatform competition—that is, competition *against* covered platforms in the market in which the "main" platform itself competes—in an effort to support competition *on* covered platforms. Trading partners that are given special benefits on a covered platform have less incentive to create, invest in, or sponsor, competitors of the platform. Instead, they become comfortable stakeholders in the status quo. I appreciate that some might conclude that the current generation of covered platforms will never be displaced, and are therefore happy to make that trade. I do not share that confidence. I think entrenching and perpetuating existing incumbency, and hoping to manage the results, is a mistake.

To be sure, there will be some benefits. AICOA would have some effect in favoring third parties over incumbent platforms in "secondary" markets where platforms also compete, and some third parties will do better as a result. Consumers may or may not benefit from that effect. But I fear that this uncertain benefit would come at much too high a cost. Moreover, to the extent that

[5] *See infra* note 11.

Congress's concern is really with intentional, targeted, and unjustified discrimination by dominant platforms against actual or potential rivals (*e.g.*, an effort to deny rivals access to complementary markets as a means of protecting the platform monopoly), a narrow rule could address that concern with *much* less collateral harm.

The "harm to competition" test in the current draft of AICOA does not much reduce my concerns. For one thing, it is not clear whether it contemplates a "consumer welfare" test drawn from traditional antitrust, or an "injury to rivals" test reflecting AICOA's separate nature and purpose. It cannot be both. This point is too important to leave intentionally unresolved.

Even a welfare-based test does not seem likely to help platforms in forced sharing cases. The harm to competition test, as I read it, invites a court to compare a world with forced sharing against the status quo. But that *ex post* test will *always* tend to find that forced sharing would improve competition compared to no sharing. The harm to competition test will thus become a rubber stamp. This implicates a classic fallacy in the analysis of refusals to deal. Suppose, for example, that a business spends five years and $10 billion to develop a valuable active pharmaceutical ingredient, or technology, over which it obtains a patent. If we come along *after the investment has been made* and ask whether it would improve competition to forcibly share the active pharmaceutical ingredient or technology with rivals, the answer will invariably be yes. More output and lower prices is better than less output and higher prices! So the apparent conclusion is that forced sharing of the asset is good for competition. But the fallacy arises from failing to think about the *ex ante* perspective: that is, the impact of a forced-sharing rule on the decision to invest in the first place. When we impose such a rule, we drain the incentive to invest, with the result that the ingredient or the technology may never be invented in the first place.

I fear just such an effect here. The point is not that *no* innovations will arise: it is that there will be *less* investment and innovation by some of our most important businesses. A forced-sharing rule makes it much less appealing to invest in things that are covered by the rule, so businesses are more likely to do something else with their time and money instead.

Nor do the affirmative defenses allay my concerns. Some important policy justifications are omitted entirely. For example: AICOA does not allow platforms to deny equal treatment to third parties, or their products and services, because they: are buggy or badly interoperable with the platform; are of low quality; contain objectionable content (*e.g.*, sexually explicit content, promotion of terrorism or violence); contain false or inaccurate information; promote spam; constitute or facilitate fraud; are subject to control or influence by, or are vulnerable to, a hostile or malicious entity; or because integration would present unusual technological or other commercial difficulties, or costs.

Remarkably, even product improvements are allowed *only if* they relate to "core" functions (an undefined term!) *and, further, only if* the platform can show that it "could not" achieve the improvement in a less discriminatory way. A platform does not seem to have the option of saying: "OK, it would be technically possible, but no rational platform would go to the trouble and expense of sharing this improvement with all third parties. We would rather not implement it at all than take on that burden, which would wipe out the profit case for doing it in the first place. The whole point of our investment was to make *our* product more valuable, not to subsidize competitors."

Finally: the difficulties and burdens of proving up a fact-heavy defense, with an array of burdens and penalties hanging overhead, will seriously erode the utility of the defense in practice.

*

To be sure: anticompetitive practices and transactions present a serious threat in digital markets, just as they do in other markets that matter to American consumers and workers. But to deter digital platforms, from engaging—*not* in improper collusion, anticompetitive acquisitions, and so on, but *product improvements, feature innovations, and entry*—has it entirely backwards. This kind of thing is exactly what we are spending millions of antitrust enforcement dollars with our left hand in an effort to get platforms to do: compete on the merits by providing valuable combinations of high-quality products and services to consumers for low prices. We should not bash them for it with our right hand when they do so.

Three final general comments. First, the scope of AICOA is exceedingly puzzling. There are serious and profound differences between the business models of the covered platforms, and each covered platform is active in a wide variety of markets. Competitive conditions, and competitive concerns, differ widely across those countless markets. I cannot discern any neutral rationale for including these businesses with respect to all their business lines and excluding other businesses, including other large monopolists, in a single regulatory measure like this one. This approach may give rise to the appearance that these businesses are being singled out not because of any distinctive competition-policy problem (there is plenty of monopoly power, network effects, data, and vertical integration throughout the rest of the economy) but because of political unpopularity. It also runs the twin risks of: (1) "fighting the last war," by focusing on a set of businesses that have already achieved some kind of dominance, rather than relying on antitrust to protect competition with the next wave of digital businesses and across the economy; and, ironically, (2) cementing the position of AICOA's covered platforms, by softening the incentives of other businesses to create or support alternatives.

Second, antitrust enforcement experience teaches us to be exceptionally wary of vague behavioral tools like non-discrimination obligations. They are often, and notoriously, a nightmare to design, to interpret, and to enforce. I do not think anyone should feel enthusiastic about the prospect of agency staff, or a court, trying to figure out whether someone's app isn't prominent enough in the app store, whether an algorithm is producing a search ranking that is "too low," or whether a delay in integration is lasting "too long." Our antitrust agencies have their hands full—more than full, in fact—dealing with mergers and anticompetitive practices, and their time is surely much better spent doing that work. But AICOA doubles down on exactly the kind of thing we normally try to avoid in antitrust enforcement: broad, vague obligations that generate uncertainty, fuel litigation and confusion, and tie up resources.[6] To make it very concrete: I cannot think of any successful FTC or DOJ enforcement action in recent years for violation of a non-discrimination obligation imposed as an antitrust remedy!

Indeed, the current Administration's antitrust agency leadership has repeatedly criticized the effectiveness of complex behavioral remedies to shield consumers from harm, even in specific markets for specific parties with specific remedial concerns in mind (a much easier project than AICOA's wide-angle *ex ante* focus).[7] As Holly Vedova, Director of the Bureau of Competition,

[6] The ABA Section of Antitrust Law—whose members will, no doubt, be litigating AICOA issues for many years if the legislation passes—has pointed out a variety of concerns with vague and undefined terms in AICOA. *See* Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf ("Qualifications like 'preference,' 'limit,' 'materially harm,' and 'materially restrict or impede' inject uncertainty into how the Bill would be administered. These terms are not defined in the Bill and existing antitrust case law cannot be relied upon to supply definitions. . . . If the Bill means to articulate entirely new substantive standards than those applied in current antitrust practice, it should state so explicitly and take steps to further define these concepts to minimize ambiguity. Similar comments apply to concepts like 'products or services . . . that are not part of or intrinsic to the covered platform itself' or 'standards mandating the neutral, fair, and nondiscriminatory treatment of all business users.' . . . The Section recommends that the Bill explicitly define its key terms.").

[7] *See, e.g.*, AAG Jonathan Kanter, *Remarks to the New York State Bar Association Antitrust Section* (Jan. 24, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-delivers-remarks-new-york ("Experience shows that it is often impossible to craft behavioral remedies that anticipate the complex incentives that drive corporate decision-making. This is especially true as market realities evolve over time.").

has recently said that in merger cases "[w]e . . . very strongly disfavor behavioral remedies because not only are they very difficult to enforce, but also because *they never seem to work*."[8]

Third, it may be worth remembering that the rest of the world is closely watching the United States very closely in matters of digital competition policy. Obligations like non-discrimination, forced access to platforms and consumer data, and so on may well inspire other jurisdictions to enact similar, or more intrusive, versions of the same programs. There is no guarantee that such measures will contain robust protections for consumer privacy, intellectual property, or the integrity of commercial data. Congress may have some pause about giving political cover for such legislation elsewhere.

The remainder of my comments on AICOA are in five sections. Section B explains that "self-preferencing" includes a vast array of practices that benefit consumers. Section C explains why banning self-preferencing would harm consumers. Section D explains that the possibility that self-preferencing may be harmful in particular markets does not justify a general ban on the practice—and how a much narrower rule might serve Congress's purposes. Section E explains why AICOA's qualifying provisions—that is, the harm to competition requirement and the affirmative defenses—do not resolve my concerns. Section F explains my concerns with the other provisions in Section 3(a). Section G provides a variety of other comments on the current draft, including comments on AICOA's somewhat arbitrary-seeming scope, and offers technical comments on drafting issues that may be presented by the current bill.

[8] Holly Vedova, FTC, *Update from the FTC's Bureau of Competition* (Feb. 3, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/vedova-gcr-law-leaders-global-conference.pdf (emphasis added).

B. "Self-Preferencing" Includes Many Desirable Practices

I take the core of AICOA to be the rule against self-preferencing by covered platforms. This rule is constituted by two prohibitions: Section 3(a)(1) prohibits a covered platform from "preferenc[ing] [its own] products, services, or lines of business . . . over those of another business user on the covered platform in a manner that would materially harm competition"; and Section 3(a)(2) prohibits a covered platform from "limit[ing] the ability of the products, services, or lines of business of another business user to compete on the covered platform relative to the products, services, or lines of business of the covered platform operator in a manner that would materially harm competition." I read these as alternative formulations of a single principle: a covered platform may not treat its own complementary products and services "on" the platform more favorably than those of rivals that are business users.[9] In other words: self-preferencing is presumptively banned. (I will consider the "harm to competition" criterion, and the affirmative defense, below.[10])

The self-preferencing ban would prohibit many product improvements, and other practices that are obviously good for consumers. Whenever an integrated business spots an opportunity to make two or more of its products, services, or divisions work better together, doing so constitutes self-preferencing unless the business also goes to the effort and trouble of doing the same thing, or offering to do the same thing, with a potentially limitless group of external actors.

Platforms may very often, and very reasonably, be unable or unwilling to extend an improvement, feature, integration, or access point to the whole world. There are many technological, commercial, and policy reasons why sharing an improvement with the world—or

[9] This definition may be broader than Congress intends. *See infra* § II.G.4.

[10] *See infra* § II.E.

even giving all applicants some kind of due process—may be unappealing, expensive, risky, or impossible in a particular case. In such cases, the self-preferencing ban will mean that the platform will not be able to implement the improvement. And if that improvement played an important role in some other beneficial activity—for example, entering a new market or line of business—then the platform's ability and incentive to invest in that activity, also, will be squashed.

It may be helpful to consider some specific reasons why a platform might be willing and able to integrate with an internal partner but unable or unwilling to do so with the entire world. Internal trading partners are usually transparent, reliable, predictable, trustworthy, and incentive-aligned in ways that arms-length third parties often are not, and *all conceivable third parties* never are. It may be enormously time-consuming to design, create, and maintain the necessary technological and commercial relations with third parties (*e.g.*, where terms and prices must be agreed, or technological problems solved, or valuable interests protected, to provide the service to a third party). Scarce resources may be involved: file storage space for preinstalling apps or files; page space for displaying links or apps; user time to search through a list of endless options. It may be difficult or impossible to screen third parties—let alone *all* third parties—in sufficient detail to guarantee the quality of their product or service; the security with which they protect user data; their freedom from control by, influence of, or vulnerability to, adversary governments or other hostile and malicious actors; their commitment to maintaining and upgrading a product or service, including regular updates and software patches to maintain security; their honesty, integrity, and freedom from malicious code, spam, or unwelcome practices; and so on.

Coordinating with third parties (above all, with a limitless class of third parties) will often be vastly more hassle—more costly, more time-consuming, more risky, more burdensome—than

coordinating with other parts of a single business. A platform may very reasonably be unwilling to share commercially sensitive information, intellectual property, trade secrets, know-how, business plans, or other investments with third parties who may have the incentive and ability to use that information strategically against the business. And it may simply be more hassle than it is worth to try to create and maintain equal commercial and technological relationships with a potentially limitless cast of third parties, who may be based anywhere in the world.

So there are many, many reasons why dealing with third parties—let alone dealing with *all comers on equal terms*—might be very costly or impossible for a rational platform. But consumers are benefited, not harmed, when businesses take the opportunity to make their products work better together, even when they do not or cannot extend those improvements to all comers.

Real-world examples of beneficial self-preferencing—by covered platforms and other businesses—are plentiful.[11] For example, drawing on both covered platforms and other businesses:

- **Google Maps / Google Search and Bing Maps / Bing.** Showing a Google Maps result as part of a Google Search result for "superb British cuisine near me" is self-preferencing, because Google Maps is treated more favorably than its competitors on Google Search. Microsoft Bing does the same thing with Bing Maps.

[11] There is a complex puzzle raised by AICOA's text concerning the definition of a "business user." Only "business users" benefit from AICOA's protections against self-preferencing. Thus, if self-preferencing takes place in a market where no business users are allowed—such as a fully closed system or part of a system—we might think that there is no AICOA violation. However, the definition of "business user" is broader than it may appear. Section 2(a)(2)(A) generally defines a business user as "a person that uses or is likely to use a covered platform for the advertising, sale, or provision of products or services." Now suppose that Entity X supplies product A and product B in two totally separate markets. And suppose Entity X is a business user of a covered platform through its supply of product B. Product A is not sold on through the covered platform because the covered platform is closed in the relevant market: *no* third party competition is permitted. But AICOA considers Entity X a business user with respect to both A and B. Thus, the operation of a closed system that excludes product A seems to become an AICOA violation. I cannot tell whether this is a drafting error, an intentional choice, or my misreading! Similarly, the definition of "use" is critical in limiting the set of entities that are "business users." Suppose, for example, my landscaping business has a website that can be viewed through the Microsoft Edge browser, or through iOS devices, which is linked from my product page on Facebook, and which gets traffic from Google Search results… am I for that reason a business user of all those platforms? If so, "business user" is an exceptionally broad concept. If not, it is not clear what narrower meaning is intended. *See infra* § II.G.4.

- **Microsoft applications / Microsoft Windows and Sony or Nintendo video games / PlayStation or Switch.** Including some Microsoft applications along with the Microsoft Windows operating system so that a new user enjoys rich functionality out of the box is self-preferencing, because the Microsoft applications are treated more favorably than their competitors on the Microsoft Windows OS. Likewise, including a Sony or Nintendo game along with a new PlayStation 5 or Switch is self-preferencing, because the Sony or Nintendo game is treated more favorably than competing games.
- **Apple apps / Apple iOS.** Pre-installing some Apple apps, like Apple Maps or Mail, on an iPhone so that a new user can use the phone for tasks is self-preferencing, because the Apple apps are treated more favorably than their competitors on the iPhone.
- **Apple hardware / iOS.** Apple's practice of manufacturing all its own hardware and devices for iOS (iPhones, iPads, etc.) is self-preferencing, because Apple's own manufacturing division is treated more favorably than competing manufacturers. So is the introduction of iOS features that work only, or better, with Apple Watch.
- **Prime Video and Amazon Music / Amazon Prime.** Giving Amazon Prime members included access to Prime Video and Amazon Music is self-preferencing, because Prime Video and Amazon Music are treated more favorably than their competitors by the Amazon Prime program.
- **In-house content / Apple+, Amazon, Disney+, and Netflix platforms.** Giving special promotion to in-house content on the Apple+, Amazon, Disney+, and Netflix platforms (*e.g.*, in a carousel at the top of the screen or page) is self-preferencing, because that content is treated more favorably than content from competing creators (indeed, I understand that Disney+ carries only in-house content).

- **Platform / virtual assistant and virtual assistant / in-house apps (Apple Siri, Amazon Alexa, Google Assistant, Microsoft Cortana).** Enabling new ways—or improving existing ways—for a platform to work with an in-house virtual assistant (such as Siri, Alexa, Google Assistant, or Cortana), or for a platform's virtual assistant to work with in-house apps, is self-preferencing, because the in-house virtual assistant or the in-house apps are treated more favorably than third-party rivals.
- **Google Search / Chrome and Bing / Microsoft Edge.** Offering automatic search in the address bar of a browser through a (changeable) default—as Google does with Google Search in Chrome and as Microsoft does with Bing in Microsoft Edge—is self-preferencing, because those search engines are treated more favorably than their competitors on the Chrome or Edge browsers.
- **In-house security tech / any platform.** Integrating a platform's own security (anti-virus, anti-malware) products into a covered platform is self-preferencing, because those products are treated more favorably than their competitors on the platform.

Combinations and improvements like this are clearly good for consumers. Indeed, these are the very kinds of complementarities that courts and agencies routinely identify as a *benefit*, not a harm.[12] When antitrust enforcers exhort digital platforms to "compete on the merits" rather than using anticompetitive agreements, exclusionary practices, or anticompetitive mergers, this is exactly the kind of thing that they normally have in mind.

[12] *See*, *e.g.*, Princo Corp. v. Int'l Trade Comm'n, 616 F.3d 1318, 1335 (Fed. Cir. 2010) (noting that procompetitive effects can include "greater product interoperability"); SD3, LLC v. Black & Decker (U.S.) Inc., 801 F.3d 412, 435 (4th Cir. 2015) (noting that joint ventures may have "decidedly procompetitive effects" including by promoting "greater product interoperability"). *See also*, *e.g.*, U.S. Dept. of Justice & FTC, *Antitrust Guidelines for the Licensing of Intellectual Property* (2017) § 5.5 (noting that certain licensing practices can be procompetitive when, among other things, they permit "integrating complementary technologies"); Statement of Interest of the United States, Cont'l Automotive Sys. Inc. v. Avanci, LLC, Case No. 3:19-CV-02933 (N.D. Tex. filed Feb. 27, 2020), 5 (listing "interconnectivity and interoperability" as "key benefits" of industry standards).

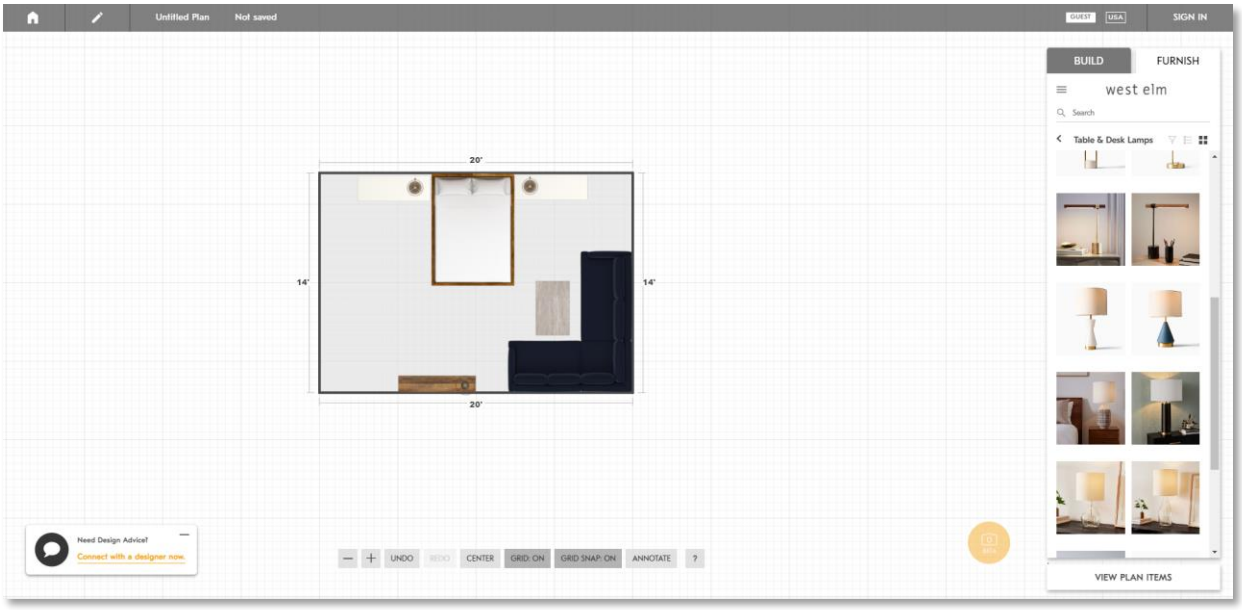
Nor is self-preferencing unique to digital platforms. Far from it: self-preferencing is utterly ubiquitous in our economy. Most businesses in the economy are vertically integrated to at least some extent: that is, they perform more than one function in a supply chain within the bounds of the firm. And most such businesses treat their internal divisions more favorably than arms-length trading partners in at least some ways. After all, businesses often do not allow their full-time employees to perform work on a spot labor market for their rivals: instead, they usually reserve their upstream labor input for their own use. They often do not commonly allow competitors to advertise on their own facilities, to have equal time on their productive machinery, to claim equal shelf space in their retail outlets, to have equal time using the company's delivery trucks, or to have equal space in their warehouses. Some manufacturers may choose to operate retail facilities (whether digital or brick-and-mortar) that offer *only* their own-brand goods, while others might choose to make limited provision to sell other manufacturers' output as well.

Ultimately: *no business deals on equal terms with the whole world.* Nor would it be possible to do so. Apart from anything else, resources are scarce. There is a limited amount of shelf space in a supermarket, a limited number of pixels on a computer screen, a limited volume of storage space on a device hard drive, and limited time for a business to maintain commercial and technological relations with third parties.

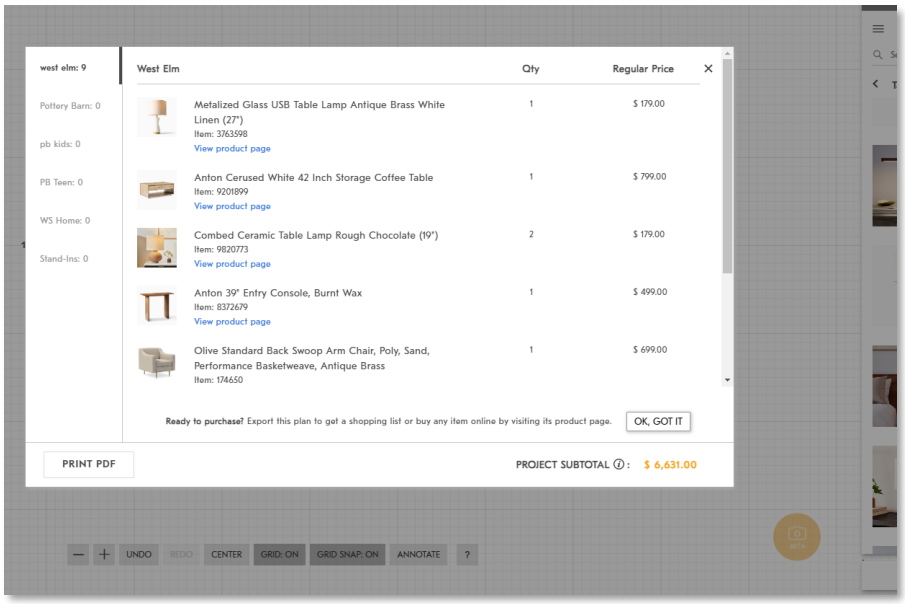
To make this very concrete—and to demonstrate how ubiquitous self-preferencing is and how desirable it can be—let's take an example from Main Street. The furniture retailer West Elm has a room planner on its website that allows consumers to build up a 2D and 3D image of a room, so consumers can figure out what will fit in their homes.[13] The planner has a "Furnish" menu on

[13] https://www.westelm.com/pages/ideas-and-advice/room-planner/.

the right hand side that shows images of furniture sold by West Elm (and other brands under common ownership like Pottery Barn). Consumers can drag and drop these furniture items onto the room planner, whereupon—because West Elm knows the dimensions, available colors, and shapes of all its own furniture—they turn into 2D and 3D versions that can be moved and recolored.



After the consumer has finished furnishing the room, clicking "View Plan Items" brings up a digital checkout with an opportunity to buy the items.



This is, of course, self-preferencing: the in-house furniture store is preferred over all other rival furniture stores. It is clearly beneficial to consumers. And of course West Elm would not do this kind of thing if it had to make this platform available to all other furniture suppliers on equal terms: the technological and commercial burdens would be absurd. Nor would it make commercial sense to do so: it makes sense to offer consumers the room planner service for free *because* it is a desirable form of distribution for West Elm's furniture business.

One sometimes hears broad claims that digital markets are different, and that practices that might be untroubling for, say, a supermarket monopolist, may be harmful for a tech monopolist. Certainly, the digital nature of some products and services—as well as platform dynamics, network effects, data, and the other peculiarities of some digital markets—can be important in some cases in some ways. But there is no general reason to think that online markets *in general* are more monopolized than brick-and-mortar ones.[14] For example, plenty of supermarkets, grocery stores,

[14] For a good recent discussion, *see* Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023), 6 et seq., https://ssrn.com/abstract=4347768.

and other suppliers in rural communities enjoy much larger shares of their respective markets than Amazon's 38% of e-commerce[15] (with e-commerce itself less than 15% of all retail sales[16])—and the barriers to buying from an alternative supermarket may be very much higher.[17]

Most importantly: *a product improvement is still a consumer benefit even when it is introduced by a digital monopolist!* The integration of Google Maps content into a Google Search result is still a consumer benefit even though Google may have monopoly power in search. The inclusion of Microsoft applications with the Windows operating system is still a consumer benefit even though Microsoft may have monopoly power in PC operating systems. And so on. Indeed, some digital markets may offer *more* opportunities for complementarities and interoperabilities—given the suitability of software for updates and integration—than some brick-and-mortar markets do. And the broader the user base of the improved product, the greater the resulting social benefit.

I have focused so far on product improvements that involve integration, but a self-preferencing ban would also deter other beneficial practices. For example, self-preferencing—in the form of some kind of special promotion or distribution—often plays a role in incentivizing and supporting a platform's fresh entry into a new market. Indeed, the possibility of such promotion (and the opportunity to drive value and demand for the integrated business) may be central to the decision to invest in the first place. For example, Amazon and Apple+ (and Disney+ and Netflix, for that matter) all engage in special promotion of their own in-house content on their own

[15] Statista, *Market share of leading retail e-commerce companies in the United States as of June 2022* (June 2022), https://www.statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/

[16] U.S. Census Bureau News, *Quarterly Retail E-Commerce Sales 4th Quarter 2022*, https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[17] It is worth remembering that in some communities, supermarkets exercise true monopoly power. In a rural community with just one supermarket, residents—including residents who may not own cars—may find it much more burdensome to travel a long distance to an alternative food store than they do to type a different URL into their browser.

platforms. The incentives of Amazon, Apple, and Netflix to invest in new content creation were clearly augmented by the opportunity to use their respective platforms to promote, and drive demand for, that content.[18]

Consumers seem to have benefited as a result. Apple has invested in shows like *The Morning Show*, *Severance*, *For All Mankind*, and *Ted Lasso*. Netflix has invested in shows like *The Crown*, *Stranger Things*, *The Witcher*, and *Formula 1: Drive to Survive*. Amazon has invested in shows like *The Lord of the Rings: The Rings of Power*, *The Legend of Vox Machina*, and seasons 4-6 of *The Expanse*. And so on. (Your own preferences may vary!) If these platform owners had been prohibited from promoting their own content on their respective platforms, the costs and risks of these investments would have been greater, and their incentives to invest reduced.

In addition: self-preferencing also includes certain kinds of low pricing by integrated businesses. Integrated businesses routinely find it rational to price an internal transfer between divisions at lower than the price it charges to unintegrated purchasers. (I am setting aside the vast practical difficulties associated with cost accounting within the firm, to isolate the theoretical point.) Some of this effect can arise from differences in transaction costs: the fact that it is often cheaper—less costly, less risky, less burdensome—to deal with another part of the corporate enterprise than to deal at arms' length. A second effect can arise from the fact that the supplier of, say, an input, has an extra incentive to lower its price to an internal trading partner because it will share in that trading partner's own profits. This is sometimes called the elimination of double

[18] Disney seems differently situated, as Disney was a content creator first. In Disney's case, though, the value of self-preferencing probably goes the other way. The value of Disney's content, including newly acquired brands like Marvel and Star Wars, certainly helped to drive demand for the Disney+ platform. No doubt the incentive to build out the platform was influenced by the opportunities for special promotion of this content. But the underlying point—that the combination of complementary assets is a powerful engine for consumer benefit—holds here too.

marginalization: the point is that each component of the firm is not optimizing its own profit in a vacuum because the other component benefits from a price reduction. The result is that it prices lower. This effect can certainly give the integrated firm an advantage over rivals that buy inputs from the merged firm, but consumers benefit from the lower price, compared to a world in which the business had not entered at each level. (Of course, if the business has achieved integration through a vertical *merger* rather than building out its own capacity, the effects are more ambiguous: in that case, there may also be a loss of competition to weigh against the benefits. But that is not this case! We are just talking about new organic entry.)

To sum up: a ban on self-preferencing would deter a wide array of beneficial practices.

C. Banning Self-Preferencing Would Inflict Consumer Harms

A ban on self-preferencing would threaten harm to consumers in multiple ways. In particular, it would deter platforms from: (1) implementing product improvements and other beneficial practices; (2) protecting users in close cases; (3) using certain ad-supported business models; (4) operating closed ecosystems. And it would also: (5) deter interplatform competition *against* covered platforms.

1. A Ban Would Deter Product Improvements

First, and most obviously, a ban on self-preferencing would deter platforms from engaging in the beneficial practices described in the previous section, including various forms of product improvements, feature innovations, new market entry, and lower pricing.

Suppose, for example, that a product design team at a covered platform has spotted an opportunity for a product improvement that involves linking two of the platform owner's products

or services together in some way. The business is deciding how to allocate time and resources, including whether and to what extent it will invest in the proposed product improvement. The product design team will understand that an obligation to extend equal treatment to rivals will often be costly. Recall that "equal treatment" here could take any of a wide variety of forms, such as: (1) pre-installing rivals' software or applications on devices; (2) including rivals' products or services in bundles that are sold or made available to users; (3) including links or buttons to rivals' products on a webpage or in a system menu; (4) making rivals' apps or products available on a store; (5) linking or integrating rivals' hardware or software to or with a platform; (6) creating options for rivals' products or services to be set as a default for some function or other on the platform; (7) giving equally prominent placement or ranking to rivals' products, icons, apps, or websites in or on screens, menus, results, marketing communications, etc; (8) establishing and maintaining a flow of data or information, including personal, financial, or other consumer data; (9) providing access to sensitive information, technology, business plans, or user data; and so on.

Regardless of the nature of an improvement, providing it for third parties may require time, money, energy, technical challenges, exposure to brand risk, and personnel—perhaps on an ongoing basis. It may require commercial negotiations, and/or policy formulation, about the terms of the relationship and about collateral obligations needed to protect user data, system integrity, or the quality of the product. It may require screening or auditing the third parties on an ongoing basis for an array of policy concerns like data privacy, spam, bugs, hostile or malicious code, or technical integrity and compatibility. It may require ongoing communications with the third party (or with others like consumers) regarding complaints or technical questions. And even if the platform does not ultimately grant access, some kind of due process may have to be afforded third parties to comply with the equal-treatment of obligation: including third parties with low-quality, high-risk,

or objectionable products. (Of course, sometimes equal treatment will be easy: the point is that it may often not be.) The product design team considering the proposed improvement will foresee these costs and hassles, and they will make investment in the proposed improvement less appealing.

The point should be clear. Instead of running an innovative business, our product team could find itself planning for life as a *de facto* utility, serving all comers on equal terms. But, whereas traditional utilities like water companies generally supply a single undifferentiated product to a finite local community, the product team in our example is dealing with a potentially limitless collection of unknown applicants presenting a rich and unknown variety of challenges.

To make this very concrete, take the example of the integration of Google Maps with Google Search. What would it mean to make that integration available on equal terms to all other third-party mapping products? The universe of such mapping products is potentially limitless, including: low-quality products that work badly, crash, are not often updated or corrected,[19] or convey inaccurate information; products and product owners that would compromise data security, user privacy, or carry malicious code or surveillance tools; products that are "spammy" and drown the user with low-quality advertisements, pop-ups, and junk content; products owned or controlled directly or indirectly by threats to national security and to user welfare; and products that are burdensome or difficult to integrate.

[19] Regular updates are a crucial means of protecting users against threats. *See*, *e.g.*, Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 14 ("[T]he number of security vulnerabilities discovered each year is on the rise. Many of these vulnerabilities are being found through rigorous testing by quality assurance and penetration testers. However, a significant number are also being discovered and exploited by rogue actors — with many of them identified only after a breach has been observed and proof-of-concept code has been shared openly. Keeping internet-connected devices and applications up to date is the best way to defend against the growing number of vulnerabilities — but many are not or cannot be updated — As a result, they remain vulnerable to botnets, often serving as gateways for more sophisticated attackers to gain a foothold into a network.").

And to make it more concrete still: is Google required to accord equal treatment in Google Search results to "Russian Hacker Maps"—a hypothetical mapping product produced at the direction of Vladimir Putin's government and operated by a nominally private entity in the interests of that government—integrating it into Google Search in just the same way as Google Maps? Is Apple required to preinstall it on the iPhone if it wants to preinstall Apple Maps?

Surely not, of course. *But now suppose that Russian Hacker Maps is sophisticated enough to call itself "USA Trusty Maps," and to disguise its ownership and control through a Delaware corporation or two.* Are Google and Apple really required or expected to accord equal treatment to "USA Trusty Maps" until they have investigated sufficiently to have discovered the link to the Russian state apparatus? How much investigation can we possibly expect them to perform?

The answer is that, of course, no detailed investigation is possible. There are currently something like 3.5 million apps on the Google Play Store and 1.6 million apps on the Apple App Store.[20] The vast hassle and expense of grappling with problems like this one will not encourage platforms to undertake detailed investigations: instead, it will simply deter them from integrating Google Maps, or preinstalling Apple Maps, in the first place. Consumers lose.

It is also worth pointing out that equal treatment obligations may also have some "second order" effects resulting from *actual compliance* with AICOA by a platform. This includes congestion, confusion, and quality degradation. It is not obvious that consumers would really be benefited overall if Google replaced the single high-quality Google Maps mapping function with, say, a lengthy "choice menu" inviting consumers to choose from among an endless list of mapping

[20] Statista, Number of apps available in leading app stores as of 3rd quarter 2022 (Oct. 2022), https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

providers of variable quality. (After all, who could be excluded?) Less sophisticated users in particular may face a series of complex choices among similar-sounding options that they are ill-equipped to navigate, ending up with a worse or unsafe product as a result.

We would have no time at all for an idea like this in almost any other context. Suppose that anyone who cared to set themselves up as a supplier of food or consumer products had an affirmative presumptive right to be carried on Walmart's shelves, subject to narrow defenses for which Walmart bore the burden of proof, on pain of injunctions, penalties, and compensation forfeiture. We would all be horrified—even if we thought Walmart was going to be a monopolist until the end of time. We would fear that the shopping experience would be fatally compromised by a deluge of low-quality products, and the costs of sorting through them to find the few that Walmart would have chosen to carry. And we would *deeply* fear for the well-being and safety of consumers. But this is precisely the result that AICOA threatens.

2. A Ban Would Deter Platforms from Protecting Consumers

Just as a self-preferencing ban would deter beneficial product improvements, so too it would also deter, on some important margins, *desirable* denials of service.

Recall, as we noted above, that the universe of third parties seeking equal treatment is potentially limitless. Some of those parties and their products will be technologically unreliable or unstable and prone to crashing; some will provide false or inaccurate information; some will just be badly designed, poorly maintained, or not updated; some will be saturated with spam; some will be vehicles for objectionable content, like sexually explicit conduct or the promotion of terrorism and violence (and some will disclose this fact, while others will conceal it); some will

contain computer viruses or other malicious code; some will be operated by criminals in search of personal information; some will be compromised by national-security threats; and so on.

We can call this entire group "bad actors." They need not be subjectively culpable or malicious—although many certainly will be—just harmful overall to consumers.

Today, platforms can deny access—whether through individual determinations or through the application of general policies—when they have concerns that they might be dealing with bad actors, regardless of whether the platform could (or would be willing to) produce a robust evidentiary showing to support its decision.

But a self-preferencing ban would profoundly change this situation. Bad actors would presumptively enjoy a right to equal treatment with the platform's own products and services. Certainly, the current draft contains some affirmative defenses, but as explained below these are very limited (including because they are subject to a demanding less-discriminatory-alternative test, do not cover many important policy grounds, are fact-intensive, and place hefty burdens on the denying platform). A platform will not be particularly enthusiastic about going ten rounds with the FTC over whether some aspect of its security policies, or quality standards, are unduly high. And, as noted below, the platform will know that an agency investigation may involve the application of interim injunctive relief on a specially-lowered standard,[21] as well as the risk of litigation and penalties. Complaints will mean the threat of serious disruption, delay, and cost.

This problem will be seriously exacerbated by the prospect of compensation forfeiture pursuant to Section 3(c)(6)(D). I cannot imagine a more effective way to undermine platform

[21] *See infra* § II.G.7.

security than threatening to take compensation away from individual decision-making executives if they deny access one time too often.

Certainly, it helps that AICOA enforcement is not in the hands of private parties and competitors, but rather with federal and state enforcers.[22] But this does not resolve the concerns. First, and most importantly, the *threat and risk* of complaints, investigations, interim relief, and litigation will have plenty of deterrent effects before an enforcer gets anywhere near the issue. Negotiating parties will make many, many demands of covered platforms, backed by threats of complaints (including to State AG offices, which may have different perspectives from the federal enforcers). Only one State AG is needed to open an investigation! Second, every enforcer investigates plenty of cases that turn out not to be suitable for prosecution. Even an investigation may well mean plenty of trouble, burden, cost, and delay—especially given the specially lowered threshold for interim injunctive relief in AICOA. Third, each of the 50+ government enforcers may turn out to have very different views about the best reading of AICOA or about the most suitable cases for investigation. And, fourth, even government enforcers might themselves not in every conceivable case take the most pro-consumer views of AICOA's meaning and terms—even with the best of intentions.

The point is that on some very important margins, the creation of a general background duty to deal will incentivize the platform to cave in in close or borderline cases, and to grant access that it would otherwise have denied. This will include cases where the platform has concerns but does not think it would be able to prove them on the balance of probabilities, as well as cases in which the platform simply does not want to go through an extensive (and expensive) defense of

[22] *See* letter dated July 7, 2022, from Fiona Scott Morton and Steven Salop to Senators Klobuchar and Grassley, https://som.yale.edu/sites/default/files/2022-07/AICOA-Final-revised.pdf.

the bounds of, and evidentiary support for, its various rules and decision. On the margin, more bad actors will gain access to the platform, to data, and to consumers.

Bad actors of various kinds are plentiful on digital platforms and plentiful in the world.[23] It is not at all clear why we would want to make it harder for platform owners to keep their platforms clean, and ensure the quality and safety of their offerings, at this time.[24] The ongoing explosion of online-enabled devices (the "Internet of Things") means that digital vulnerabilities are an increasing threat not just to consumers' devices and data, but also to their homes.[25] As the UK's National Cyber Security Center has warned, for example: "voice assistants represent an

[23] *See, e.g.*, Crowdstrike, 2023 Threat Report, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 2 ("[A]dversaries have become more sophisticated, relentless and damaging in their attacks. As a result, a number of disruptive trends emerged in 2022 that threaten productivity and global stability. . . . nation-state attacks coincided with organizations struggling to manage an explosive landscape of vulnerabilities that amplified systemic risk."); Sophos 2023 Threat Report, https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf, 3 ("[A]dversaries have not stopped trying to discover and exploit vulnerabilities, and in fact seem to have stepped up efforts designed to subvert the security of every vendor's firewalls, switches, and network access points."), 6 ("Access brokers, ransomware, information-stealing malware, malware delivery, and other elements of cybercrime operations have lowered barriers to entry for would-be cybercriminals.").

[24] I note that an array of former military and intelligence leaders have expressed concerns regarding AICOA's implications for national security. *See, e.g.*, Glenn S. Gerstell, *Before we regulate Big Tech, let's make sure we don't hurt national security*, THE HILL (May 19, 2022) ("Mandating that a third party has the right to connect and operate seamlessly with a platform's own systems could, for example, mean that the platform couldn't scan for or block malicious code; the platform does indeed have to "discriminate" against bad software. Yet, depending on the interpretation of the bills' provisions, that might be unintentionally outlawed. Obviously, curtailing a platform's ability to prevent a computer virus from infecting that platform or its users, or allowing disinformation to be posted and disseminated, can't be good for our national security."); Robert C. O'Brien & Jeh Johnson, *The Big Tech Battlefield*, NEWSWEEK (May 19, 2022) ("Legislation pending in both the House and Senate would require non-discriminatory access to U.S. digital platforms for all 'business users,' including foreign ones. This could potentially require U.S. platforms to broadcast the false propaganda of autocratic regimes—a step backward in U.S. efforts to combat harmful foreign disinformation and even attempts by our adversaries to influence our own elections. Other parts of [AICOA] would constrain U.S. companies from removing malicious actors and integrating cybersecurity tools to their platforms, possibly leaving U.S. tech infrastructure vulnerable to America's foreign adversaries. These national security risks have been acknowledged by the legislation's sponsors. Nevertheless, they have not been addressed as part of any meaningful review of the legislation for their implications to U.S. national security."); Letter to Hon. Nancy P. Pelosi & Hon. Kevin O. McCarthy from Robert Cardillo, John D. Negroponte, Dan Coats, Leon Panetta, et al., https://www.documentcloud.org/documents/21062393-national-security-letter-on-antitrust ("The recent U.S. Innovation and Competition Act (USICA) has the potential to put us on strong footing to compete with China. . . . .Recent congressional antitrust proposals that target specific American technology firms would degrade critical R&D priorities, allow foreign competitors to displace leaders in the U.S. tech sector both at home and abroad, and potentially put sensitive U.S. data and IP in the hands of Beijing. . . . [W]e believe more deliberate analysis is needed to examine the detrimental impact these bills could" have on our strategic competition with China. Congress should not proceed with current legislative proposals before understanding the full range of potential consequences.").

[25] *See, e.g.*, Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 7 ("Cybercriminals have shifted their focus to IoT and mobile devices"), 14 ("From 2019 to 2020, there was a 100% growth in IoT device infection rates.").

attractive target for attackers, who could use them to steal personal data and listen in on victims' conversations."[26]

Moreover, serious threats are commonly disguised as benign apps, and sometimes slip into even official app stores. Nokia's 2021 Threat Intelligence Report explains some of the sophisticated ways in which major threats disguise themselves in an effort to reach users:

> The number of Trojans [a form of hostile tool used by criminals and malicious actors] targeting banking information through Android mobile devices has skyrocketed, putting millions of users around the world at financial risk. Malware app developers are getting better at bypassing the security measures intended to keep harmful apps out of official app stores . . Banking Trojans can arrive on smartphones in a variety of ways, often disguised as common and useful apps.
>
> [. . .]
>
> FluBot is typically disguised as a package tracking app from a major courier company. The user receives an SMS message indicating that a parcel is being delivered and is offered a download link to a bogus tracking app.
>
> [. . .]
>
> TeaBot comes disguised as a video app (or other useful app) to trick the user into installing it. When run, the app acts as a remote access Trojan, allowing its distributor to exercise considerable control over the infected device.
>
> BlackRock was first discovered in 2020 and is typically disguised as an Android or Google update, distributed through a third-party app store. Like other banking Trojans, it uses login screen overlays and SMS message capture to acquire banking credentials, but it also tries to gather additional personal information from the phone and installed apps, including dating, shopping, lifestyle and productivity apps.
>
> Cerberus has been around since 2019 and is "leased" to malicious actors wishing to distribute it to collect banking credentials in their region. It operates similarly to other Android banking Trojans, but more modern versions also leverage TeamViewer to allow the author to gain remote access to the device.
>
> Mandrake is a highly sophisticated spyware package focused on gaining access to financial information and credentials. This Android threat has been around for five years and has seen bug fixes and feature enhancements added to it over that time. Typically, Mandrake gets installed via a benign-looking dropper app in Google

[26] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 11.

> Play or a third-party app store. Once installed, the dropper app installs Mandrake disguised as a system application, such as a firmware update.
>
> Banker.GXB may be disguised as a variety of useful tools, including power managers, storage cleaners, performance boosters and horoscope utilities, originally found in the Google Play store in 2018. Like other banking Trojans, Banker.GXB impersonates legitimate banking applications and steals SMS messages. Unlike most banking apps, which never provide their promised functionality, Banker.GXB apps at least provide the appearance of performing their intended function to avoid suspicion.[27]

As Congressman Eric Swalwell has pointed out, and as I describe further below,[28] AICOA's "modest defenses" would "require an unwieldy amount of evidence for each and every action the platform makes to protect our national security. This is especially concerning where decisions must be immediately made to limit widespread damages . . . [and the result would] blunt platforms that are working closely with intelligence communities to strengthen our homeland."[29]

To be clear, I do not mean to suggest that *only* bad actors will benefit. The self-preferencing ban will doubtless allow some more non-bad actors to gain equal access too, and that could be good. But I doubt the social harm from letting, say, Russian Hacker Maps (whether or not re-branded "USA Trusty Maps") onto the Apple App Store, or Russian Hacker Word Processor onto Windows PCs, or Russian Hacker Camera App onto the iPhone, would be offset by the social benefits of admitting three or ten or fifty other small independent software developers as well.

3. A Ban Would Challenge Some Free-to-Use, Ad-Supported Services

Third, a ban on self-preferencing may challenge certain free-to-use, ad-supported business models that allow consumers to enjoy valuable services without paying a fee. In particular, a ban

---

[27] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 17–18.

[28] *See infra* § II.E.1. (affirmative defense), § II.G.10 (exceptions).

[29] Eric Swalwell, *The federal government must address national security concerns in antitrust reforms* (May 10, 2022), https://cyberscoop.com/the-federal-government-must-address-national-security-concerns-in-antitrust-reforms/.

may encourage a shift toward fee-paying, subscription-based models, and that shift may leave users with less money in their pocket.

Today, many digital services are provided by platforms to users for free (or at a low cost), supported by advertising. That system can work successfully *as long as the business can ensure that consumers of the services are also exposed to the advertising mechanism*. But if the business may not promote its own advertising to service users, then it may be unable to expose consumers to the advertising. It may then no longer make sense to provide the service for free. The result may be that the business is pushed toward a fee-paying, subscription-based model.

The point is that reserving exclusive access for a platform's own advertising business seems to constitute the preferencing of the platform owner's own advertising business, or of a product or service that carries or supports it, on the platform. For example, Google sells advertising beside Google Search results and in Gmail inboxes; Meta sells advertising space in the Facebook and Instagram content feeds; Twitter sells advertising space in the Twitter news feed through "promoted tweets"; Amazon sells advertising space in the Amazon product search results through sponsored ads; and so on. Doing so appears to constitute self-preferencing of these platforms' own advertising businesses over those of actual and potential rival advertising businesses on the platform—at least as long as those advertising businesses constitute "business users."[30] And Google's willingness to make the Android operating system available for free is presumably in at least some relationship with the fact that Google's own apps—which support its advertising business—are typically preinstalled on Android devices. Banning that would strike right at the heart of the free-to-use business model.

[30] *See infra* § II.G.4.

My own view is that American families benefit *hugely* from the widespread availability of free digital services.[31] Free-to-use internet search, mapping and navigation, email, video sharing, personal social networking services, microblogging, and so on: at a minimum, it is not unreasonable to think that that is a more than fair trade for getting advertisements for products and services that are of real interest to us, instead of those that are not! Of course, there is plenty of room to take a different view: some would no doubt prefer to pay subscriptions and be free from digital ads. Moreover, without a doubt, digital advertising raises real and serious concerns relating to data privacy and data security: these concerns deserve careful attention from legislators.

But the core point for competition policy is that consumers are probably doing better overall because businesses can choose to offer, and consumers can choose to accept, a free service that comes with an advertising channel bundled in. Congress may want to carefully weigh the consequences of a self-preferencing ban that would challenge that business model.

4. A Ban Would Threaten Closed Ecosystems

Many platform operators choose to "close" some complementary markets on their platforms: that is, to reserve some complementary activity on a platform *wholly* for the platform owner, without third-party competition at all. For example: I understand that Apple does not generally allow third-party smartphones or tablets into its iOS ecosystem, nor third-party app stores; Amazon does not allow third-party music or content stores on the Amazon Prime platform in competition with Amazon Music or Prime Video; and so on. And, looking beyond the covered

[31] *See generally, e.g.*, Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-Being*, 116 Proc. Nat'l Academy of Sci. 7250 (2019); Erik Brynjolfsson, Avinash Collis, W. Erwin Diewert, Felix Eggers & Kevin J. Fox, *GDP-B: Accounting For The Value Of New And Free Goods In The Digital Economy*, NBER Working Paper 25695 (Mar. 2019); The Economist, *How much would you pay to keep using Google?* (Apr. 25, 2018), https://www.economist.com/graphic-detail/2018/04/25/how-much-would-you-pay-to-keep-using-google.

platforms, I understand that Disney and Paramount generally do not carry third-party content, or much third-party content, on the Disney+ and Paramount+ platforms. I understand that the major console manufacturers—Nintendo, Sony, and Microsoft—do not allow third-party online game stores, nor do they allow third-party consoles in their own ecosystems.[32] And so on.

The current draft of AICOA appears to prohibit fully or partly closing a digital platform, because closure is simply an extreme example of self-preferencing, as long as at least one excluded business was a business user of the covered platform.[33] But a ban on closed systems seems undesirable.

There are many good reasons why a business might choose to operate on a closed model. Among other things, a closed system allows the business owner to ensure and vouch for the quality and consistency of the user experience from end-to-end, without running the risk that consumers will have bad experiences because of third-party actions, or the risk that the integrity and quality of the system will compromised by hostile, incompatible, or just bad-quality code. Closed systems, in which the platform owner either allows no entry or directly supervises all third-party entry, have long been widely understood to be more secure than open systems: this has long been a key advantage of the iOS smartphone ecosystem, for example.[34] For example, a 2021 cybersecurity

[32] There is some cross-platform interoperability at the individual game level. *See, e.g.*, Wes Fenlon, *Sony charges for crossplay support to protect PSN revenue, documents show*, PC GAMER (May 4, 2021). But third party OEMs cannot build consoles to run, say, Nintendo Switch games in the way that they can build devices to run the Android mobile OS, or Windows-compatible PCs.

[33] *See infra* § II.G.4.

[34] *See, e.g.*, *Can iPhones get viruses? Here's what you need to know*, MARKETS INSIDER (Mar. 4, 2019) (describing the "walled garden" of iOS and noting: "For the vast majority of everyday users, there's virtually no risk of viruses on the iPhone."); Steve Sande, *Why Apple's "walled garden" is a good idea*, ENGADGET (July 29, 2010) ("Many developers and users of Apple's iOS devices bemoan the 'walled garden' of the App Store approval process, but it appears that the company's measures have prevented mass data theft from iPhones, and iPads."). Of course, no system is *free* from threats: and bad actors target iOS as they do any other platform. The point is that more openness means more risk, and that iOS is generally safer for that reason.

threat report published by Nokia notes that the closed model of Apple's iOS has been instrumental to its security, by comparison with Google's more open Android ecosystem:

> While Google has taken an open approach to app development and distribution, Apple has always maintained a proprietary approach, allowing downloads only through the official App Store. *As a result, Apple products have generally been considered the most secure mobile computing platform.*[35]

It goes on to point out that "Android devices make up 50.31% of all infected devices," with iOS far behind.[36] And, as you might expect, Apple trumpets this disparity in making its own case for the closed model: "Over the past four years, Android devices were found to have 15 to 47 times more malware infections than iPhone."[37] It is not clear why Congress would want to prohibit businesses from offering—and consumers from choosing—this valuable business model.

Of course: if closed systems are *permitted* under AICOA (perhaps because the definition of "business user" was narrowed), then a self-preferencing ban would encourage systems that were previously open, but which relied on some distinctive promotion for the platform owner's own products, to consider closing entirely as an alternative. I am not sure that either Congress or consumers would welcome that result.

5. A Ban Would Suppress Interplatform Competition

AICOA would have a particularly perverse impact on competition with the digital platforms themselves: namely, it would *discourage* and suppress inter-platform competition.

---

[35] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18.

[36] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).

[37] Apple, *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading* (Oct. 2021), https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf, 2.

The economic point is a simple one. By guaranteeing trading partners specially favored treatment on covered platforms, AICOA would make those platforms a particularly cosy place for businesses that would otherwise have stronger incentives to create, sponsor, or deal with *rival* platforms. After all, why go to the trouble of developing or supporting a rival platform when the terms of dealing with an incumbent like Google or Amazon have been made specially favorable by AICOA? And even if a promising rival *does* emerge, potential trading partners will have less incentive to switch over and take a chance on it, because that rival—unlike the incumbent—will not be subject to AICOA's obligations to provide equal treatment, preinstallation, favorable search rankings, interoperability, and so on. Thus AICOA would turn potential competitors, and sponsors of competitors, into stakeholders in the status quo.

I think it would be a profound mistake to sacrifice competition *with* today's generation of digital platforms, in the hope that society can make do with competition *on* those platforms. And the mistake would be worse still if we weaken even on-platform competition too by restraining the platforms themselves from competing vigorously in such markets.

I think our best hope for dynamic digital markets lies in a world in which Google, Meta, Apple, Amazon, and Microsoft must continue to compete just as vigorously as they can against existing and new rivals—including each other—constrained by robust antitrust enforcement and constant changes in technology and demand. Entrenching their dominance by turning would-be rivals into cosy collaborators, while limiting platforms' own vigor, seems to have everything backwards.

D. The Risk of Harmful Self-Preferencing Does Not Justify a Total Ban

1. Harmful Self-Preferencing is Possible But Elusive

Of course, one can imagine forms of self-preferencing that do not involve genuine or arguable product improvements and which may harm consumers. (I will set aside behavior that would violate existing antitrust law.[38])

Commentators have often focused on search ranking manipulation. Suppose, for example, that an e-commerce website degrades the search rankings for all third-party products, bumping its own products to the top, above rivals' higher-quality products. Or suppose that a search engine degraded the search rankings for all vertical search competitors, bumping its own to the top above higher-quality offerings from rivals.

This is a dangerous game for a platform to play. Manipulation of this kind would inflict a double harm on a platform's market position: (1) it would make the platform less valuable to third-party business users (like merchants or publishers), by reducing their sales or traffic, and (2) it would make the platform less valuable to consumers, by serving up lower-quality results. And, in many platform cases, each of these first-order impacts would in turn have a second-order impact on the other side. That is: as frustrated users turned away from an e-commerce site that was manipulating its results, value for merchants would decline yet more; as merchants dropped off the platform, users would find less value there as well.

[38] This could plausibly include unlawful uses of exclusivity and tying. The application of tying law to self-preferencing is tricky and case-specific: certainly, the inclusion of a free product or service in a package can be analyzed as tying, but on almost any plausible view, merely adding a new function to a product without more would almost certainly not violate antitrust law on a tying theory or otherwise. *See* United States v. Microsoft Corp., 253 F.3d 34, 90–91 (D.C. Cir. 2001). EU competition enforcers have at times taken a different view. Case T-201/04, Microsoft Corp. v. Commission (imposing liability on Microsoft for supplying Windows Media Player along with Windows).

Importantly, trading partners do not have to know that the platform is manipulating anything for self-preferencing to drive them into the arms of rivals. They just have to know their own experience: say, their satisfaction with search results, or their sales or traffic.

Thus, we would usually expect that the platform would earn more profit by *avoiding* manipulation and instead by trying to maximize output and activity on the platform, which it can then monetize by charging users on one or both sides. This way it maximizes its own profits.

But we can imagine at least two theories of anticompetitive harm from manipulation and equivalent behaviors. On one theory—let's call it "Platform Moating"—the platform is aiming to protect the primary platform monopoly by cutting off actual and potential rivals from platform services so that they find it harder to develop into competitors of the main platform. On the other theory—let's call it "Platform Leveraging"—the platform is aiming to acquire a second monopoly in the complementary market.

Self-preferencing that is harmful in the first way—that is, Platform Moating—is likely to be confined to some rare and special cases. For one thing, the platform is lowering quality to *all* customers on both sides: it is annoying consumers who are being steered away from what they really want, as well as trading partners who are getting fewer sales on the platform. By self-preferencing, the platform is actively driving both sets of annoyed customers to seek and support, or become, platform rivals.

By hypothesis, of course, the platform is doing this in order to hit the trading partners who are competitive threats of the platform, but these are likely to be few in number compared to the number of impacted businesses (because most platform customers are not even possibly platform competitors). Moreover, these may be the very competitors who are *most* likely to be able to

manage without the platform, or to give a significant boost to rivals. Self-preferencing gives them a hefty nudge to make the jump into platform competition *and* it incentivizes other users to sign up as their customers. So a platform would have to be really sure it was worth the trade on some unusual facts to think of this as a particularly appealing means of protecting platform monopoly. Nevertheless, "unusual" doesn't mean "never," and it is possible to imagine cases of this kind.

Cases in this first category also seem likely to overlap in practice with cases where the platform prefers its own products or services but has a legitimate basis for doing so: for example, because the platform has more information about its own offering, more control over it, or better ability to guarantee quality. Moreover, with respect to search rankings in particular, it is important to appreciate that there is no "objectively correct ranking principle" that explains how to weigh the benefits of in-house knowledge and control against other things that might plausibly matter to consumers. For example, an e-commerce platform like Amazon or Walmart.com is better able to make sure the quality and timeliness of products that it controls, than of products that are supplied by third parties. Likewise, Apple has greater control over the quality, security, and update frequency of its own apps than of those of app stores. One might think these perfectly sensible reasons to elevate this in-house content in search results or other placement rankings. (Of course, others can disagree! The point is that there is no "objective" position here.)

The second theory—Platform Leveraging—applies to markets where the platform believes that it can plausibly obtain market or monopoly power in the complementary market by degrading platform service and that it will do better by doing so. If the secondary market is materially broader—in that there are many sources of supply beyond the reach of the platform—then the goal of market power in the secondary market is probably unattainable and this strategy will just reduce

the platform's profit (by substituting the platform's less efficient output for the third party's superior output). It is most likely to be a concern in markets where scale economies are vital and the platform itself is a very important input into (or distributor of) most or all activity in the market.

The difficulty with cases of this second kind is *not* that they will almost never exist: it is, rather, that they often be very difficult to distinguish from product-improvement cases and it is very hard to craft a rule that doesn't punish a ton of beneficial conduct. The platform is giving higher-quality supply to its own unit and lower-quality supply to third parties. How should we tell whether this involves a good, desirable improvement of the platform's own products or services or a bad, wasteful degradation of rivals' products or services in the hope of a second monopoly?

Take, for example, a games console manufacturer that also makes games. Suppose it develops a technology for making its own-developed games ultra-realistic on its own console, and does not share that technology with third-party game developers. (Perhaps the technology involves projecting the user's face onto an in-game character, and the manufacturer does not want to get into the business of screening and supervising third party developers' data security, or implicitly warranting that security to users.) How can we tell if this is good or bad self-preferencing? Should it matter if the manufacturer had *first* tried to make the feature available to other developers, only to later find that it was too expensive, risky, burdensome, or unpopular with users, to do so? Should we make legality of identical conduct turn on subjective intention: that is, on whether the key executives were literally thinking "we will make our games better" or "we will make rivals' games worse"? What if executives had different subjective purposes in signing off on the course of action? I am not sure there is any good way to do this sensibly: at a minimum, it subjects product improvements to all the burdens of investigation and litigation described above.

Take a real example. With the release of iOS 15, Apple eliminated some support for certain Siri tools that had been previously made available to third-party developers, through an API deprecation.[39] On the face of it, this is equally consistent with a recognition by Apple that the company's product-improvement plans were not compatible with support for these tools (*i.e.*, a good product improvement reason), and with a naked desire to harm rivals that relied on these tools (*i.e.*, a bad rival-injuring reason). So it will often be in practice.

Finally, there is a question of remedy. The idea that self-preferencing can be meaningfully "prohibited" supposes that platforms will be willing, or can be made, to directly subsidize competitive threats. But this will often be untrue. Suppose that we can correctly identify bad self-preferencing of both kinds (*i.e.*, Platform Moating and Platform Leveraging), and that we prohibit them when they happen. The problem is that it is not at all obvious whether the platform is likely to level up, benefiting consumers by extending the improvement to rivals' products, or level down, harming consumers further by withdrawing the improvements from its own products. In at least some of the most important cases, a platform may prefer not to make a product improvement if it would have to share it and thus to directly sponsor competitive threats to its own main cash cow. And if the improvement is already in place, it may simply be withdrawn or support may be terminated. Platforms may reasonably decline to invest in on-ramps for their rivals.

2. A Narrower Rule Could Address Harmful Self-Preferencing

The most promising cases for regulatory intervention on the grounds of dissimilar treatment probably involve specific acts of intentional, targeted, and unjustified impairment of particular rivals of the core platform monopoly: not merely rivals in the complementary market.

[39] *See* https://developer.apple.com/support/deprecated-sirikit-intent-domains.

For example, suppose that the operators of Google Search one day decided to banish Yelp from search results solely because it is a competitive threat to some aspect of Google's business. Or suppose that the operators of Twitter deactivated the functionality of links to rival microblogging networks and no other websites. Regardless of whether conduct like this is illegal, under most circumstances it does not serve consumers' interests.

We could imagine a category of high-risk denials. Such denials would be: *intentional* (in that they are not the incidental effect of a broader policy or policy change), *targeted* (in that they involve specifically targeting individual competitors, while leaving intact service to all non-targeted trading partners, rather than just preferring the platform's own business over third parties), *unjustified* (in that there are not supported by any procompetitive justification *other than* the proposition that a business is entitled to decline to affirmatively support its rivals), and *monopolizing* (in that they tend to increase monopoly power in a primary platform market).

It is not entirely clear that Congress would really want to try to prohibit even this, to the extent that antitrust does not already do so. Reasonable minds can differ about whether a business should be forced to actively subsidize its rivals, either individually or as a category. They might also differ regarding whether a business should be able to "price in" the fact that supporting a rival will bite into the business's own profits, and thus charge a profit-maximizing price that is higher than the platform charges to non-rival trading partners. One might reasonably fear that banning discrimination of this kind will lead to platforms keeping improvements for themselves that they would otherwise share with non-rival trading partners (*i.e.*, self-preferencing as an alternative to targeted discrimination against rivals). One might also fear pushing courts and agencies into figuring out whether a platform had unlawfully discriminated against rivals by providing

inadequate assistance, too-limited connectivity, insufficiently rapid service and support, insufficiently prominent promotion, and so on.

But, even with all that said, it is clear that the balance of harms and benefits of a ban on intentional, targeted, and unjustified discrimination amounting to monopolization against actual or potential rivals tips differently from the case of self-preferencing. And if Congress desires to protect against this threat, then it can do so with a much narrower rule.

Reasonable minds can differ here: my own instinct is that Congress should probably not create even this much narrower rule. I think naked discrimination of this kind is pretty rare, and the close cases that will emerge in practice will present all the challenges and concerns described above, including the risk of punishing product improvements. Nor do I think there is a principled basis for creating a different rule in the context of digital platforms, when this phenomenon is common to the entire economy. I also think there is room to apply Section 2 of the Sherman Act to at least some such practices, including when an anticompetitive condition is used to deter entry or expansion. But a rule of this kind would surely be *much* better than a general rule against self-preferencing, and I could imagine it doing helpful work in some of the most troubling cases.

E. AICOA's Qualifying Provisions Do Not Resolve Concerns

1. The Harm to Competition Criterion Is Likely to Be Ineffective

The current draft of AICOA prohibits self-preferencing if conducted in a manner that "would materially harm competition," and creates an affirmative defense to other violations if a defendant can establish that the conduct would *not* result in "material harm to competition."[40]

[40] AICOA (May 2022 draft), Section 3(a)(1), 3(a)(2), 3(b)(2).

I do not think this language resolves the concerns identified above. To be sure, it is much better to include this language than not to do so! It could be understood as a reference to antitrust's concept of an anticompetitive effect or tendency that injures welfare: that is, increased prices, reduced output, reduced quality, etc. If this is its purpose, AICOA should explicitly say so.

But there are two problems.

The first is that "harm to competition" is just not a phrase with a single self-executing meaning. It *could* be interpreted to mean welfare harm in a manner we would associate with traditional antitrust; or it could be interpreted to mean "injury to rivals," This reading would be more than plausible, given that AICOA is not an antitrust statute, that "harm to competition" is not a phrase that appears in the antitrust statutes (unlike, say, "where . . . the effect . . . may be substantially to lessen competition") and that it makes no reference to a principle of consistent interpretation. And if the latter, it is no kind of limit at all.

The failure to take an explicit view on this is a serious and glaring problem with the current draft. It creates profound ambiguity at the heart of the bill. At all costs, the provision should be defined: either it's a consumer-welfare test, or it's an injury-to-rivals test. It cannot be both.

Many distinguished commentators have made this point. For example, Professor Doug Melamed—former acting head of the DOJ Antitrust Division under President Clinton—has noted:

> Plaintiffs will no doubt argue, and courts might agree, that Congress did not intend to incorporate existing antitrust concepts and that "harm to competition" means any reduction in competition by, for example, causing a weak and insignificant rival to exit from an intensely competitive market. Plaintiffs will argue that Congress could have specified that the bill incorporates the antitrust notion of injury to competition but that Congress chose not to do that, and they will emphasize that the whole point of the bill was to supplement the antitrust laws with stronger prohibitions.

> The bill could be very harmful if it is construed to require, not increased market power, but simply harm to rivals. The U.S. has in the past tried laws that insulate weak firms from competition provided by more efficient firms. The results have been increased costs, reduced output, and harm to consumers and suppliers.[41]

And Professor Herbert Hovenkamp has made the same point:

> If competition is defined in an economically sensible way to refer to reduced market output and higher prices, then the statute might end up limiting its reach to conduct posing a realistic threat of competitive harm. If it means something else, such as merely injuring a rival or placing it at a disadvantage on that particular platform as opposed to the market as a whole, then it could end up doing a great deal of harm. . . . If the AICOA is redrafted, this provision more than any other needs clarification. Is its principal purpose to protect competitors, without regard for market output, prices, innovation or other indicia of consumer harm? Or is the statute intended to promote the antitrust function of ensuring that markets are competitive?[42]

Second, in forced sharing cases, as I read it, the "harm to competition" test invites application against the wrong baseline *even if it is understood in the sense of welfare harm*. It implicates a well-known fallacy in the law of refusal to deal. On the most natural reading of the text, the "harm to competition" seems to be measured against a world in which the relevant preference (or access, or interoperability, or search ranking) is extended to all third parties. In other words, a court or agency is invited to see that some benefit (say, a low price, or a product improvement) is being conferred on an internal trading partner, and is then asked to consider whether competition would be materially improved if that benefit were provided on equal terms to all. *But the answer to that question will virtually always be yes*. Through an *ex post* lens, it maximizes short-run competition to require that investments already created be shared at marginal cost.

---

[41] A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

[42] Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023) 23–24, https://ssrn.com/abstract=4347768.

The inference of competitive harm is fallacious because it misses the *ex ante* question. In a great many cases, the product improvement would never have been made if the government was going to come along and compel universal sharing, with all its burdens.[43] It always looks *short-run* procompetitive, after the fact, to compel sharing at marginal cost (which may be at or near zero) to maximize output. But doing so would often inflict serious harm on incentives to invest.[44]

Nor is it obvious how the court is supposed to assess the *long run* question that includes the *ex ante* perspective. Is the court supposed to ask whether this platform would have introduced this feature if it had known that equal access would be mandated after the fact? Whether other future investors will be chilled by an imposition of liability? How is an agency or court supposed to balance this in practice? If a court is supposed to do this kind of ex ante analysis, AICOA should state that clearly, and provide some kind of guidance on how it is to be done.

To sum up: I fear that the harm to competition requirement will collapse into simply asking whether the innovation is valuable to the third party seeking access, and whether static welfare will be improved in the short run by forced sharing. If so, then it will be a rubber stamp. And if the intention is to have a court or agency decide whether the self-preferencing plays a reasonably

---

[43] *See, e.g.*, Howard A. Shelanski, *Unilateral Refusals to Deal in Intellectual and Other Property*, 76 Antitrust L.J. 369 (2009).

[44] *See, e.g.*, Jorge Padilla, Douglas H. Ginsburg & Koren W. Wong-Ervin, *Antitrust Analysis Involving Intellectual Property and Standards: Implications from Economics*, 33 Harv. J. L. & Tech. 1, 8, 10 (2019) ("After an [intellectual property right] has been created, it is often most efficient to make it widely available — full dissemination and disclosure of an innovation is socially optimal ex post. But if dissemination or disclosure is made mandatory, then the incentives are likely not there to create [intellectual property] in the first place. As such, ex ante, the ability to exclude and limit dissemination and disclosure is socially optimal. In other words, the core right to exclude is often critical to induce innovators to invest in costly and risky R&D. . . . [O]ne can imagine the value that society loses when pharmaceutical companies charge prices for pills that far exceed the cost of manufacturing those pills. But . . . this . . . examines only the static view of monopoly pricing, and ignores the dynamic view."); Glen O. Robinson, *On Refusing to Deal with Rivals*, 87 Cornell L. Rev. 1177, 1191–92 (2002) ("Surely it cannot be enough for a firm to assert that it would be desirable for them to use their competitor's property and then shift the burden to the competitor to prove that the suggested arrangement is not efficient. . . . When a Wal-Mart comes to town, it is a safe bet that many smaller retailers that sell similar merchandise will suffer. Those who think that small retailing serves a vital community function may lament this new competition, but sensible people are unlikely to propose the remedy of forcing Wal-Mart to provide floor space to its smaller competitors so that they may enjoy the benefits of Wal-Mart's magnetic pull on consumers. Turning Wal-Mart into a wholesaler of retail space . . . would be a counterproductive strategy if competition is what we are seeking.").

important role in incentivizing the platform to introduce, maintain, or improve the feature in question, then at a minimum that should be directly stated, and some guidance given to an agency or court attempting to apply that test. And Congress should understand that this will considerably narrow the scope of any self-preferencing prohibition.

2. AICOA's General Affirmative Defense Is Too Narrow and Too Demanding

The current draft of AICOA creates a general affirmative defense against core self-preferencing as well as all the other violations established in Section 3(a)(3)–(10). A defendant establishes this defense if it establishes that the conduct is "reasonably tailored and reasonably necessary"—such that the objective "could not be achieved through materially less discriminatory means"—to: (A) prevent a violation of, or comply with, law; (B) protect "safety, user privacy, the security of nonpublic data, or the security of the covered platform"; or (C) "maintain or substantially enhance the core functionality of the platform."[45] An exception to the definition of "business user" also excludes entities that are a "clear national security risk."[46]

This provision aims at a good purpose: to prevent AICOA from biting on conduct that is justified. The problem is that this provision is likely to be all that stands between a platform and liability for a *product improvement* (!) or other commonplace beneficial behavior, and it is much too weak a shield to do that work. I have four main concerns.

a) The Less Discriminatory Alternative Test Seriously Weakens the Defense

First, this defense is unlikely to be much help at all in many cases, because it requires the defendant covered platform to show that the conduct in question "could not be achieved through

[45] AICOA (May 2022 draft), Section 3(b)(1).

[46] AICOA (May 2022 draft), Section 2(a)(2).

materially less discriminatory means." It does not seem to matter that the platform *would not rationally* have gone to the burdens and expense of, say, sharing an improvement or feature innovation with the whole world, including because doing so would have been very costly or risky or otherwise unappealing or implausible. If it "could" have been done in a non-discriminatory way, then there's no defense *even if* the effect of the challenged conduct is clearly good for consumers.

For example, suppose that a covered platform preinstalls an app or integrates a function. A rival complains that this is unlawful self-preferencing in violation of Sections 3(a)(1) and 3(a)(2). The platform responds that this is a "core" product improvement under Section 3(b)(1). *But now the rival responds that the defense does not apply because there was a less discriminatory alternative: namely, preinstalling or integrating the rivals' app too!* So the defense hangs by a thread: unless the covered platform can affirmatively show that it was not (technically? commercially? conceivably?) possible to preinstall or integrate the rival's product, the defense is no help. The fact that it would have been very expensive, or very time-consuming, or very difficult, or just unprofitable to do it in a less discriminatory way, seems to be no help.

b) The Defense Omits Many Important Justifications

Second, by specifying a narrow set of grounds that may justify self-preferencing, the defense offers no protection for denials that—surely!—ought to be protected. For example, the defense does not appear to protect a platform that declines to give equal treatment to a product, service, or entity for reasons of:

- objectionable content (*e.g.*, sexually explicit content—including in products, services, or apps aimed at or marketed to children; promotion of terrorism; promotion of violence or criminality)[47];
- inaccurate, false, or outdated information;
- poor quality service or a bad, buggy product;
- spam (*i.e.*, objectionable, intrusive, and unwelcome advertising or valueless content);
- fraud, deception, and exploitation;
- threat of consumer confusion;
- threat to the security of *other* ecosystem participants (not the platform itself);
- law enforcement or national-security concerns that do not involve an entity that has already been specifically designated by the federal government as subject to sanctions or as a "national security, intelligence, or law enforcement risk[]"[48] and which do not rise to the level of a "clear" national security risk[49];
- unusual technological, commercial, or other difficulties or costs of integration; or
- lack of information regarding, or ability to investigate, a possible concern (*e.g.*, the ultimate ownership and control of an app, or the way in which an app will use data).

And if the existing terms "safety, user privacy, the security of nonpublic data, or the security of the covered platform" are intended to cover some of the foregoing grounds, that should be made clear.

[47] As I note below, it is not clear to me how the First Amendment or Section 230 is intended to interact with the prohibitions in Section 3(a), nor what the optimal relationship would be. *See infra* II.F.1.

[48] AICOA (May 2022 draft), Section 3(c)(8)(A)((iii).

[49] AICOA (May 2022 draft), Section 2(a)(2).

c) The "Core" Limitation Is Undesirable

Third, by limiting the platform-enhancement defense to "core" functionality, the defense does not protect even a clear product improvement that merely enhances *non-core* functionality. Strikingly, the term "core" is not defined, and there does not appear to be any very good way to tell what it means even directionally. Does it improve the "core" functionality of an app store to add or promote an app? Does it improve the "core" functionality of Windows to include a media player or a word processing app? Why would the defense not extend to *any* mere functionality improvement, whether the improved function was core or not? Does the introduction, integration, or improvement of a product, service, app, or function count as the improvement of the "core functionality" of a platform? How can we tell? Moreover: is the "maintain or enhance" test applied against a counterfactual in which the platform does not implement the improvement at all, or one in which it shares it with all third parties? (If the latter, it will invite the same *ex post* fallacy described above.) And is the word "substantially" in "substantially enhance" intended to do any limiting work: and, if not, why is it included?

There does not seem to be any good reason for limiting this defense to "core" functions, however defined. The "core" test should almost certainly be removed: any measure reasonably related to the maintenance or improvement of a function should not be an AICOA violation.

d) Fact-Intensive Defenses Are Likely to Be Little Comfort

Fourth, the defenses are likely to be heavily fact-intensive, and the burden is with the platform to prove that they justify a denial by a preponderance of the evidence.[50] This means that

[50] AICOA (May 2022 draft), Section 3(b)(4).

if the platform has grounds for concern, but cannot ultimately prove those grounds on a preponderance of evidence, there will be no defense. And if a platform *fears* that it cannot do so, or does not want to face the expense of doing so, then the defense will not help it in the first place.

For all these reasons, I fear that the general affirmative defense will be a paper shield in practice. Given the breadth of AICOA's basic prohibitions, and the number and variety of things that those prohibitions will catch that they should not, the general affirmative defense in Section 3(b)(1) is far too narrow and weak to allay my concerns regarding the bill.

F. Other 3(a) Provisions Raise Numerous Concerns

Although my focus has been on the core self-preferencing rules, because I take these to be the central thrust of AICOA, the bill also creates an array of other rules. These also present a series of risks to consumers and others. The following discussion illustrates some of those concerns.

1. The TOS Discrimination Ban Harms Consumers and Implicates Content Moderation (Section 3(a)(3))

Section 3(a)(3) prohibits a covered platform from "discriminat[ing] 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." This is similar in thrust to the rule against self-preferencing, but it involves the preferencing of *third parties* other than the platform itself, and it takes place within the four corners of the platform's "terms of service."

As a threshold matter, it is not quite clear what useful work "terms of service" is doing or why discrimination within the terms of service should be treated differently from those outside those terms. The phrase "terms of service" is not defined. The rule would seem to treat identical

practices differently depending on whether they fall within what the platform has chosen to designate "terms of service." That does not seem like the right outcome!

That issue aside, a general non-discrimination obligation inflicts consumer harms by preventing platforms from offering good terms when they could or would not do so across the board. For example, suppose that a covered platform is able and willing to offer a high-volume, high-quality trading partner some kind of benefit, such as low fees, cooperation on a new product feature, or inclusion in a "trusted partner" program of some kind. Those are efficient and desirable things! But the risk of liability simply deters the platform from doing so. (This is the classic problem that causes the Robinson-Patman Act to hurt consumers.[51])

Of course, there are circumstances under which it might be appropriate to impose a non-discrimination obligation in a particular market for a particular reason. Usually these involve a policy decision that competition cannot take place and that a regulated monopoly is, exceptionally, the next-best alternative. But that determination is generally made on a market-by-market basis, and in full awareness of the costs and risks. Applying it across the board to all practices by covered platforms does not even arguably fit this description.[52]

Separately: it is not at all clear to me how this provision is intended to interact with the practice of content moderation (including banning, blocking, and ranking), the law of the First

[51] *See generally, e.g.*, Herbert Hovenkamp, *Antitrust Modernization Commission: Written Testimony on the Robinson-Patman Act* (July 2, 2005), https://govinfo.library.unt.edu/amc/commission_hearings/pdf/Hovenkamp.pdf.

[52] The customary case for public-utility-style regulation does not seem a very promising fit with most digital markets. Network effects may reward scale, but real competition is often sustainable given the presence of product and service differentiation, ad-supported platform services, multihoming, and the fact that users can connect to new and existing rivals. Uber can co-exist with Lyft; Amazon with Walmart, Target, eBay, and Etsy; Google with Bing; Apple's iPhone with Google's Android; Microsoft Windows with Mac OS; Microsoft Word with Google Docs; and so on. Of course, market power and monopoly are still possible and a serious concern, here as elsewhere in the economy. My point is that there is no reason to give up on competition and embrace the sedentary model of regulated monopoly.

Amendment, Section 230, or the control of spam or content that might be thought objectionable (*e.g.*, sexually explicit material, or the promotion of terrorism or violence).[53] The text of Section 3(a)(3) strongly hints that content moderation will be a violation, assuming that content moderation involves applying or enforcing terms of service. At a minimum, some such practices seem to fall within Section 3(a)(3). As a result, Section 3(a)(3) is mostly naturally read to require that any moderation be non-discriminatory (*i.e.*, not disadvantage "similarly situated" business users).

If some content moderation practice is, or is held to be, discriminatory among similarly situated business users, and if the harm to competition criterion is satisfied (more than plausible if the covered platform is an important input to or distributor of content in the relevant market), then a presumptive violation is established. And, as noted above, control of spam or objectionable content is *not* a basis for the affirmative defense. I have no idea at all whether the First Amendment, Section 230, or anything else would protect a platform in such a case.

The concrete case might look something like the following. A business user of a covered platform generates content that is controversial: regarded by some as spam or irresponsible falsehood, and by others as important political speech. Or perhaps a business user generates sexually explicit content. A covered platform suppresses or removes the business user's website, posts, content, or account. The business user complains—to a federal enforcer or a State Attorney General—that this constitutes discrimination because other businesses are not being treated in the same way. And it claims harm to competition because distribution on the platform is competitively important in the market in which the business user competes. The enforcer agrees and brings an

[53] *See*, *e.g.*, Free Press, Provision in Senate Antitrust Bill Would Undermine the Fight Against Online Hate and Disinformation (Jan. 20, 2022), https://www.freepress.net/news/press-releases/provision-senate-antitrust-bill-would-undermine-fight-against-online-hate-and-disinformation (Section 3(a)(3) "would make it difficult or impossible for covered companies to deplatform and remove from their sites any business that traffics in hateful, racist, violent or otherwise harmful content").

action under AICOA as a Section 3(a)(3) violation. And now the platform does not seem to have access to the affirmative defense. Everything will then turn, I think, on: (1) what "similarly situated" means (is *any* discrimination allowed as long as the platform can articulate a reason? How is a court to tell what constitutes a "good" or "bad" reason, or a relevant similarity, under Section 3(a)(3) of AICOA?); and (2) whether other laws, such as the First Amendment or Section 230, would apply. It is not at all clear what the drafters of AICOA intend.

Reasonable minds may feel differently about the optimal rule here. So, too, may reasonable federal enforcers, and reasonable State Attorneys-General, empowered to enforce AICOA. To avoid serious confusion and divergent enforcement, Congress may wish to clarify the intended operation of these rules. It is worth remembering that spam, in particular, confronts every digital platform that allows users and businesses to create and share content.[54]

2. The Access and Interoperability Mandates Threaten Users (Section 3(a)(4))

Section 3(a)(4) imposes a strikingly broad duty of forced access and interoperability. All business users must be accorded equal "access" and "interopera[bility]" to "the same platform, operating system, or hardware or software features that are available to the [platform's competing or potentially competing] products, services, or lines of business . . . except where such access would lead to a significant cybersecurity risk[.]"

[54] *See*, *e.g.*, Mike Masnick, *Very, Very Little Of 'Content Moderation' Has Anything To Do With Politics* (May 25, 2022), https://www.techdirt.com/2022/05/25/very-very-little-of-content-moderation-has-anything-to-do-with-politics/ (noting, for example, that more than half of Facebook's content moderation in Q4 2022 related to spam, and most of the other half related to fake accounts).

As a threshold matter, this provision centrally rests on the terms "access" and "interoperate" which are, rather strikingly, not defined by the bill. Figuring out what these terms mean will be a time-consuming and expensive task for businesses, agencies, and courts.

Moreover, on most plausible readings, this obligation seems to require handing over the keys to a platform, device, or ecosystem to a really striking extent, with only the final proviso for very limited comfort.[55] For example, Apple has "access" to an iPhone's camera, microphone, GPS locator, and so on, as well as tremendous data regarding users and their behavior. This provision seems to presumptively require Apple to fork over whatever hardware access is used by a product like the phone function, Apple Maps, or Apple's mail software to any manufacturer of a competing app. (Nor is it obvious what a "software feature" is. Is information about consumer behavior, preferences, or location a "software feature"? What about an algorithm applied to such data?)

The premise seems to be that if consumers are willing to trust, say, Apple with access to the phone hardware, then they must be willing to trust any conceivable supplier of a third-party app, peripheral, service, or product. I think this is misconceived, and that it misses a critical "trust gap" that often will separate a known and trusted platform owner from an unknown and untrusted

[55] Others have made this point. *See*, *e.g.*, Mark Jamison, Congress Could Weaken U.S. Competitiveness with These Two Bills, AEI (Aug. 21, 2022), https://www.aei.org/op-eds/congress-could-weaken-u-s-competitiveness-with-these-two-bills/ ("Given the platforms' regulatory hurdles and delays, it is likely that the Russian actors could have planted malware designed to stealthily collect U.S. and Ukraine metadata, steal software, intercept and alter data flows, surveil Americans and Ukrainians, disrupt the platforms' attempts to prevent misuse, and compromise platform functions. The regulations would also have required the U.S. platforms to provide data to a wide range of stealth Russian-supported companies. American lives and interests would have been put at risk, as would the lives and interests of American allies."); Krisztian Katona, *AICOA's Data Security, Privacy, and Content Moderation Issues Call for Risk Assessment* (June 7, 2022), https://www.project-disco.org/privacy/060722-aicoas-data-security-privacy-and-content-moderation-issues-call-for-risk-assessment/ ("Complying with this requirement to grant access to any platform, OS, hardware, or feature means giving unfettered access to any putative competitor. Leading cloud services would seemingly need to grant access to back-end infrastructure and physical hardware−the same infrastructure and hardware that supports essential sectors like healthcare, energy, and banking and finance, to say nothing of state and federal governments. Similarly, device manufactures regularly restrict access to APIs that grant full read/write access to the device–that is necessary to perform backups but can easily be abused in ransomware attacks–or that grant access to sensitive information like health data or mobile payments. These private APIs keep sensitive data and permissions secure and opening them up to all comers represents a major privacy and security risk.").

third party supplier. Many consumers may reasonably trust, say, Apple or Amazon, without equally trusting every third-party app developer or goods seller that happens to be on the platform. Doubly so if the government is going to come along and *force* app developers and goods sellers onto the platform that the platform itself would have reasonably decided to keep out! And it is not at all clear to me what "interoperate" means.

The proviso at the end ("except where such access would lead to a significant cybersecurity risk," introduced in the May 2022 draft), seems to be a response to this glaring problem, but it is too vague and cursory to do that work. What is a "significant cybersecurity risk" and who must prove that access "would" lead to such a risk? The definition of "significant" and "cybersecurity" are critical but unexplained. Is this proviso intended to cover all undesirable uses of information, including not just those that involve criminal behavior or national security threats, but also uses that will expose users to spammy advertising, unwelcome contacts, or compromise their privacy? If so, that should be made very clear. Likewise, the relative burdens of proof of the plaintiff and defendant are critical. What if the platform merely has some grounds for concern and cannot or would not exhaustively investigate?

Nor are the legitimate concerns limited to cybersecurity. Forcing access to any "platform, operating system, or hardware or software features" is a dramatic incursion, with obvious implications for commercial confidentiality, platform integrity, and the platform's own resources. May a platform decline to provide such access on the ground that access of this kind would reveal competitively sensitive information, require expensive supervision, or threaten the efficient operation of the system? The answer appears to be no: that may not be a good idea.

3. The No-Conditioning Rule Is Vague and Threatens Ad-Supported Models (Section 3(a)(5))

Section 3(a)(5) bans certain conditioning practices. In particular, it prohibits a covered platform from conditioning "access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator that are not part of or intrinsic to the covered platform."

As a threshold matter, and importantly, it is not at all clear what "part of" or "intrinsic to" might mean here, in the context of an integrated platform with multiple features and functionalities. Those terms are not defined in the statute. (Nor, again, is "access.") This presents a difficult problem of interpretation: this provision purports to require unbundling of platform services but without any guidance as to what this would involve or how far it is supposed to go. Are Apple's App Store or In-App Payment mechanism "part of" or "intrinsic to" the iOS platform? Is iOS "intrinsic to" the iPhone or vice versa? Is Siri intrinsic to iOS? Are Amazon's warehousing or fulfilment services "part of" or "intrinsic to" the Amazon.com website? It is in the nature of software products of all kinds, and platforms in particular, to perform multiple functions. This provision seems to invite a landslide of uncertainty and miserably extended litigation: costs that will ultimately land on consumers. And it may just incentivize platforms to repackage two "separate products" into an integrated "single product," benefiting no-one.

That aside, this provision amounts to a *per se* rule against technological product tying of a kind that modern antitrust has long—and very wisely—left behind. Antitrust courts used to believe that "tying arrangements service hardly any purpose beyond the suppression of competition,"[56] but

[56] Standard Oil Co. of California v. United States, 337 U.S. 293, 305 (1949).

today virtually everyone agrees that supplying products together can often significantly benefit consumers and competition—even though tying can *also* sometimes cause harm. Above all, it makes no sense to automatically ban tying and integration among digital and software products, as the D.C. Circuit, sitting *en banc*, expressly recognized in the iconic pro-enforcement *Microsoft* decision:

> [T]here are strong reasons to doubt that the integration of additional software functionality into [a computer operating system] falls among [the category of *per se* illegal practices]. Applying *per se* analysis to such an amalgamation creates undue risks of error and of deterring welfare-enhancing innovation. . . . [J]udicial experience provides *little basis for believing that, because of their pernicious effect on competition and lack of any redeeming virtue, a software firm's decisions to sell multiple functionalities as a package should be conclusively presumed to be unreasonable and therefore illegal* without *elaborate inquiry* as to the precise harm they have caused or the business excuse for their use.[57]

The prohibition on conditioning also threatens free-to-use business models that allow non-ad-bearing apps or services to be provided free of charge through bundling with ad-supported apps. For example, a business may make and distribute an operating system for free because that operating system comes preloaded with apps that support monetization through advertising. It does not seem to be in the public interest to prohibit such business models.[58]

In addition, the prohibition also threatens to deny platforms the ability to reflect, in search rankings, the platform's knowledge of quality (and ability to guarantee it). For example, suppose that an e-commerce platform instituted a program pursuant to which it accorded greater prominence in search rankings to products for which it could directly guarantee stock and rapid fulfilment because it was, itself, providing warehousing and fulfilment services. This would direct consumers to products and services that the platform had reason to think were especially desirable.

[57] United States v. Microsoft Corp., 253 F.3d 34, 90–91 (D.C. Cir. 2001) (en banc) (emphasis added).

[58] *See supra* § II.C.3.

If this were prohibited on the ground that the platform was conditioning preferred status on buying its warehousing and fulfillment services, the result may not be in consumers' interests.

4. The Data Non-Use Obligation Prohibits Desirable Conduct (Section 3(a)(6))

Section 3(a)(6) bans a covered platform from using "nonpublic data . . . obtained from or generated on the covered platform by the activities of a business user or by the interaction of a covered platform user with the products or services of a business user to offer, or support the offering of, the products or services of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform."

This prohibition directly prohibits platforms from better serving consumers. Virtually every business uses data generated by its activity—including, for appropriate businesses, activity that involves selling third-party products and services—to better understand and better satisfy consumer demand. An e-commerce platform uses information about what consumers do and do not want in order to better satisfy demand. A supermarket uses data about demand for products (including products manufactured by third parties); an auctioneer uses data about demand for goods (including goods to which it never takes title); a car dealer uses data about demand for cars (including those to which it never takes title); and so on. *Accurate information about demand allows businesses to compete better and more accurately, leaving consumers better off*.[59]

This provision ties platforms' hands to prevent third-party suppliers from facing "too much" competition, and consumers lose out as a consequence. It rests on the erroneous conclusion that data about, say, a merchant's sales on Amazon "belongs to" that merchant and does not

[59] Doug Melamed has made this point. A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

"belong to" Amazon. It also prohibits platforms from buying data from business users for competitive purposes: but such a ban clearly harms competition and consumers.

To be sure, there are some very narrow circumstances where a data obligation may be anticompetitive, rather than procompetitive, but they do not involve the platform's access to information about its own activity. The most plausible version of this concern probably involves a platform agreeing to deal with a trading partner only so long as the trading partner commit to provide information or data relating to their own current or future competitive activity, to which the platform would not otherwise have access, and which would reduce the trading partner's incentive to invest in competition with the platform. Such a plan would usually violate the Sherman Act, and could safely be prohibited in the interests of consumers. As I note below, in the context of OAMA, I think such a prohibition could be framed by prohibiting a covered platform from making competitive use of competitively sensitive nonpublic business information *received directly from the third party* as a condition of operating a multisided platform or app store.[60] But the no-data rule in Section 3(a)(6) would reach *vastly* more broadly. It should be eliminated.

5. The "Access Own Data" Obligation Should Be Clarified (Section 3(a)(7))

Section 3(a)(7) prohibits a covered platform from "materially restrict[ing] or imped[ing] a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the products or services of the business user, such as by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user."

[60] *See infra* § III.B.2.

It is hard to know what to make of this provision without a clearer sense of what it is supposed to require—and figuring that out across the many affected markets seems certain to involve extended uncertainty and expensive litigation. What exactly must be shared: simply information about the fact of a transaction? Identity of customers, including personal data of those customers? If, say, Apple has GPS information about where the consumer was when a purchase was made on an iPhone, or if Amazon has information about the search that led to a purchase, must information that be shared? If an advertiser buys an advertisement on a platform, does this provision allow the advertiser to obtain the identity of each user that viewed the ad (as that engagement was "generated by" the ad itself)? Is a content creator such as a video-maker on YouTube or a developer of a mobile game entitled to information about every user that downloads it? If a platform analyzes activity on its platform through a proprietary method, and by doing so gains valuable insights about consumer demand, must it share the results of that analysis with all the relevant third parties, on the ground that the analysis output is "data generated . . . by [their] activities"? And so on.

The point is not that transparency is bad: it can often be good. The point is that the nature of a desirable and workable obligation varies wildly from one market to the next. Indeed, an appropriately specific obligation to provide data or information, tailored to a specific market or set of markets in mind, could be procompetitive, as I note below.[61] Accordingly, I recommend Congress more precisely specify the meaning of this provision. I would support reasonably tailored transparency obligations in specific markets where the risks were low and the benefits clear.

[61] *See infra* § III.B.3., § IV.D.

6. The Free Uninstall, Free Default Rule Appears Dangerously Overbroad (Section 3(a)(8))

Section 3(a)(8) prohibits a covered platform from "materially restrict[ing] or imped[ing] covered platform users from uninstalling software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator, unless necessary—(A) for the security or functioning of the covered platform; or (B) to prevent data from the covered platform operator or another business user from being transferred to the Government of the People's Republic of China or the government of another foreign adversary." Foreign adversary is defined, through Section 2(a)(8) and 47 U.S.C. § 1607(c), as "any foreign government or foreign nongovernment person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

This provision prevents a platform from effectively hard-wiring certain software functions into the platform if the function is being executed by means of a separate "software application." This may not lead to logical results, because it does not affect the platform's ability to including multiple functions in a single product or service. Thus, for example, it would appear to presumptively prevent Microsoft from making the Edge browser a non-uninstallable "application," but would not prevent Microsoft from making browser functionality an integral part of the Windows operating system. It is not obvious whose interests are protected by encouraging a platform operator to spend time and money re-combining products and services in a slightly different way.

It is also not clear what the prohibition on inflexible "default settings" is intended to accomplish, outside what I take to be easy cases (*e.g.*, a default search provider for address-bar search). Every feature and function on a covered platform works a certain way: is AICOA really intended to apply to treat these as "defaults" and require that consumers be able to choose third-party options for any function? Or is something a default *only* if the platform owner builds in an option to switch to a third party in the first place? If so, this rule may just encourage platforms to eliminate the option and make everything an integrated function rather than a menu with a default.

Also unclear is a simpler issue: what does this provision actually require? What is the obligation of a platform with respect to email defaults on an iPhone, search defaults on a browser bar, camera apps on an operating system, mapping apps on search results, transaction handling software on any platform? What is a platform required to do: create a default menu that includes all known suppliers? Accept and review applications and screen them for quality? Must some kind of appeal be provided? What if adding a third party to the list requires something sensitive: for example, a mapping app requires location information, a camera app requires access to the camera, a transaction handling app requires credit card information. It is not remotely clear what is contemplated, permitted, or prohibited.

The purpose of the final condition seems to be to allow businesses to prevent a user (or an intermediary like a device original equipment manufacturer) from changing defaults to point to a service owned or controlled by the PRC or "another foreign adversary." But how is the platform owner to know what services are in fact under the thumb of an entity that qualifies as a foreign adversary? Digital services and products offered by a foreign power are unlikely to prominently identify themselves. Also, what about hostile and malicious actors here at home?

In practice, it is not at all clear how a platform is supposed to be able to protect against a user—or an intermediary like a device manufacturer or a retailer, whether knowingly or otherwise—redirecting a default or other function to point to a service that is terribly unsafe or unsound. Forcing a platform to allow a GPS mapping function, search function, camera function, or mail function to be reassigned to Russian Hacker Maps, Russian Hacker Search, Russian Hacker Video Sharing, or Russian Hacker Email does not seem like a step forward for the American consumer: even if those apps are masquerading under the name "USA Trusty Maps" and so on. And the same is true of Domestic Hacker Maps!

Nor is it clear why this limitation is confined to the "government" of foreign adversaries. Is the intention really to force platforms to grant equal access to privately owned entities—whether or not they are provably state-influenced—established in foreign adversary nations? And, finally, the vagueness of the "foreign adversary" definition in 47 U.S.C. § 1607 leaves a covered platform in an uncomfortable position of figuring out whether an agency or court will agree that a particular country is "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

7. The UX / Search Preferencing Ban Replicates the Harms Described Above (Section 3(a)(9))

Section 3(a)(9) prohibits a covered platform from, "in connection with any covered platform user interface, including search or ranking functionality offered by the covered platform, treat[ing] the products, services, or lines of business of the covered platform operator more favorably relative to those of another business user and in a manner that is inconsistent with the neutral, fair, and nondiscriminatory treatment of all business users[.]"

This is a version of the general self-preferencing ban, but it lacks the harm to competition criterion, and is subject to the second of AICOA's affirmative defenses. My comments regarding this provision accordingly duplicate those above regarding self-preferencing, except to note that it is very broad. It forbids self-preferencing with respect to any user interface including, but not limited to, search rankings: thus, Amazon could not specially promote Amazon Studios at the top of its own page; Apple could not specially promote Apple+ content on its page, and so on. It would accordingly prohibit much product improvement and integration, including special promotions in connection with new market entry, and many page-design choices.

Moreover, to the extent that this provision also introduces the concepts of "neutrality" and "fairness," I suggest removing those provisions or defining them very clearly. It is notoriously difficult to assign anything like a consensus meaning to these two concepts, and AICOA surely does not need to import those difficulties. It is not clear that there is any such thing as a "neutral" or "fair" search ranking or user interface design.

I separately note that this provision, like Section 3(a)(3), presents the issue of content moderation. Among other things, the First Amendment appears to be implicated by government supervision of what a platform publishes and promotes: regulating web page design and search-result presentation may neither be wise nor Constitutional.[62] As I note above, AICOA's

[62] *See*, *e.g.*, Zhang v. Baidu.com, Inc., 10 F. Supp. 3d 433, 435 (S.D.N.Y. 2014) ("[T]he First Amendment protects as speech the results produced by an Internet search engine."); e-ventures Worldwide, LLC v. Google, Inc., Case No. 214-CV-646, 2017 WL 2210029, at *4 (M.D. Fla. Feb. 8, 2017) ("Google's actions in formulating rankings for its search engine and in determining whether certain websites are contrary to Google's guidelines and thereby subject to removal are the same as decisions by a newspaper editor regarding which content to publish, which article belongs on the front page, and which article is unworthy of publication. The First Amendment protects these decisions, whether they are fair or unfair, or motivated by profit or altruism."); *see also* Eugene Volokh & Donald M. Falk, *Google First Amendment Protection For Search Engine Search Results*, 8 J. L. Econ. & Pol'y 883 (2012).

relationship with the First Amendment, Section 230, and the law of content moderation is unclear, at least to me—I have no expertise at all in those areas of law—and could at least be clarified.[63]

8. The Anti-Retaliation Provision Is Desirable (Section 3(a)(10))

Section 3(a)(10) prohibits a covered platform from "retaliat[ing] against any business user or covered platform user that raises good-faith concerns with any law enforcement authority about actual or potential violations" of law.

This is a sensible provision. If AICOA is enacted, a provision of this kind is desirable.

9. AICOA's Supplementary Affirmative Defense Does Not Resolve Concerns

Section 3(b)(2) is an affirmative defense to conduct that would otherwise violate Section 3(a)(4)–(10). It is identical to the first affirmative defense, except that the defendant may also establish it by demonstrating, by a preponderance of the evidence, that the conduct has not resulted in and would not result in material harm to competition. In effect, this defense reflects the fact that harm to competition is *not* an element of the affirmative offenses in Sections 3(a)(4)–(10), but that lack of harm to competition can be shown by the defendant as a defense.

My reaction to this affirmative defense mirrors my reaction to the first affirmative defense, above.[64] Because I think the "harm to competition" test will amount to a rubber stamp for plaintiffs, I do not think that test will narrow the application of Sections 3(a)(1)–(3), and the fact that the burden is flipped to the defendant will make this even more of a problem than it is for Sections 3(a)(1)–(3).

[63] *See supra* § II.F.1.

[64] *See supra* § II.E.2.

In particular, I am concerned that the affirmative defense is subject to an unduly strict less-discriminatory alternative test that will wipe it out in many cases; is limited to improvements to "core" functionality, which is both narrow and undefined; fails to include many important policy grounds; and is heavily fact-dependent and requires the defendant to prove them by a preponderance of the evidence.[65] As a result, like the other affirmative defense, I expect that it will be a paper shield in practice.

G. Additional Comments

1. AICOA's New and Vague Terms Invite Endless Confusion and Litigation

AICOA introduces a forest of terms and concepts that are new, vague, and undefined, but which perform absolutely critical functions in defining the operation of the bill. To pick some specific examples:

- the definition of "business user" in Section 2(a)(2)(A), which is utterly foundational to AICOA's scope and reach, including the meaning of "use" and the scope of the status of being a "business user" for a company that is a business user with respect to one of its activities (if a business advertises on an internet website that can be found through Google, viewed on an iOS or Android device or a Windows PC, has it for that reason become a business user of Google, iOS, Android, and Windows? And if not, why not?);
- the scope of the exemption for "clear national security risk[s]" from the definition of "business user" in Section 2(a)(2)(B)(i), which will be a critical frontier of

[65] AICOA (May 2022 draft), Section 3(b)(4).

platforms' ability to protect national security (why must the risk be "clear" rather than "reasonable suspicion" or similar, and why are other forms of security threats not included?);

- the definition of "critical trading partner," including the definitions of the phrases "restrict or materially impede . . . access" of a (single?) business user to users or customers, or to a "tool or service . . [a] business user needs to effectively serve . . . users or customers," in Section 2(a)(6);
- the utterly central concept of "preference" in the signature prohibition in Section 3(a)(1) and elsewhere;
- the equally central concept of "material harm to competition" in Section 3[66];
- the definitions of "access" and "interoperate" in Section 3(a)(4), and of "materially restrict[ing], imped[ing], or unreasonably delay[ing]" access or interoperability, in Section 3(a)(4), which will define platforms' universal service obligations;
- the definition of "significant cybersecurity risk" in Section 3(a)(4), which is the ground on which denying access or interoperability will *not* constitute a presumptive violation;
- the terms "part of" and "intrinsic to," which define the scope of the rule against conditioning in Section 3(a)(5);
- the obligation to offer search rankings and user interfaces that are "neutral, fair, and nondiscriminatory" in Section 3(a)(9); and

[66] *See supra* § II.E.1 (explaining concerns).

- the scope of the critically important defense for "substantially enhanc[ing]" the "core functionality" of the platform in a way that "could not be achieved through materially less discriminatory means" in Section 3(b)(1), 3(b)(1)(C), which will be all that stands between a vast range of product improvements and liability.

The combination of the vagueness and the centrality of these and similar terms will put consumers, businesses, agencies, and courts in the unhappy situation of having to make this large and complicated plane while it is in the air. Antitrust doctrine has wrestled painfully for almost 133 years with the concepts at the heart of Sections 1 and 2 of the Sherman Act ("restraint of trade" and "monopolize") and for almost 109 years with the operative test in Section 7 of the Clayton Act (whether the effect of a merger or acquisition "may be substantially to lessen competition or tend to create a monopoly"). Those terms remain battlegrounds today in antitrust. And there is virtually no agreement at all today—less than there has been in decades!—about what Section 5 of the FTC Act means when it empowers the FTC to prohibit "unfair methods of competition." But each of these pillars of antitrust is pretty brief and concise.

AICOA will introduce a swathe of new, undefined, but critically important terms into competition enforcement and compliance, which will impact a vast number of negotiations and commercial activities throughout our economy (including in some of our most valuable and innovative markets). For the most part, the terms identified above do not exist in antitrust doctrine. And for those that seem to nod at an antitrust-like meaning—"harm to competition" is a prominent example—AICOA very pointedly does *not* clarify whether it is intended to adopt a consumer-welfare definition from antitrust, or different standards of its own, such as an injury-to-rivals standard. The resulting uncertainty, counseling and litigation costs, will delight only the lawyers,

and the businesses that can successfully use the threat of those costs to extract negotiating concessions. Those resources are surely better spent supporting antitrust enforcement, leveraging more than a century of investment, rather than beginning again from the ground up.

2. AICOA's Scope Appears Arbitrary

a) The "Covered Platform" Definition Does Not Seem Principled

I take Sections 2(a)(5)–(6) to define a "covered platform" as an "online platform" (as defined in Section 2(a)(9), discussed in the next section) that:

1. **has many US users**, by having, during a relevant 12-month period, *either* 50 million monthly active US-based users *or* 100,000 monthly active US-based business users (even if these thresholds are satisfied only for a moment);

and

2. **satisfies a bigness test by sales, market capitalization, or worldwide user base**, through:
    a. being owned or controlled at any point during a relevant two-year period (apparently even if that person no longer owns or controls the relevant platform?) by a person with net annual sales of $550 billion, *or*
    b. having an average market capitalization above $550 billion for a 180-day period during a relevant two-year period; *or*
    c. having at least one billion worldwide monthly active users at any point during a relevant 12-month period;

and

3. **is a "critical trading partner"** for the sale or provision of any product or service offered on or directly related to the online platform, through being "a person that has the ability to restrict or materially impede the access" of:
    a. "a business user to the users or customers of the business user," *or*
    b. "a business user to a tool or service that the business user needs to effectively serve the users or customers of the business user."

This is a rather strained definition, and it gives the impression of arbitrariness. Specifically, it leaves a reader with the sense that it has been written to specifically target certain businesses. My understanding is that at this time,[67] it is likely to cover at least: Alphabet Inc. (Google) (270 million U.S. users[68]; market cap $1.15 trillion[69]); Amazon.com, Inc. (163.5 million U.S. Prime members[70]; market cap $965.6 billion[71]); Apple Inc. (125 million U.S. iPhone users[72]; market cap $2.33 trillion[73]); Meta Platforms Inc. (Facebook) (239 million U.S. users[74]; 2.9 billion monthly active users worldwide[75]); and Microsoft Corp. (market cap $1.86 trillion[76]; and no doubt there are more than 100,000 business users of Microsoft's platforms).

[67] Figures last checked February 28–March 2, 2023.

[68] Statista, Google - Statistics & Facts (Jan. 2023), https://www.statista.com/topics/1001/google/.

[69] https://finance.yahoo.com/quote/GOOG/.

[70] Statista, Number of Amazon Prime users in the United States from 2017 to 2021 with a forecast for 2022 to 2025 (June 2022), https://www.statista.com/statistics/504687/number-of-amazon-prime-subscription-households-usa/. Of course, the text relies on an inference that at least 1 in 3 Prime members is a monthly active user.

[71] https://finance.yahoo.com/quote/AMZN/.

[72] Statista, Number of iPhone users in the United States from 2012 to 2022 (Mar. 2022), https://www.statista.com/statistics/232790/forecast-of-apple-users-in-the-us/.

[73] https://finance.yahoo.com/quote/AAPL/.

[74] Statista, Number of Facebook users in the United States from 2018 to 2027 (June 2022), https://www.statista.com/statistics/408971/number-of-us-facebook-users/.

[75] Statista, Number of monthly active Facebook users worldwide as of 4th quarter 2022 (Feb. 2023), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[76] https://finance.yahoo.com/quote/MSFT/.

Walmart.com (408 monthly active users[77]; market cap $383.3 billion[78]) approaches the threshold but does not appear to hit it. And it is not clear to me whether Visa Inc (> 300 million U.S. cards in circulation,[79] and surely more than 100,000 U.S. business users; more than 1.1 billion worldwide credit cards issued[80]; market cap $462 billion[81]); and Mastercard (> 319 million cardholders[82]; 992 million consumer credit cards issued, plus 122 million commercial cards (including credit and debit)[83]; market cap $333.9 billion[84]) qualify. (I understand that "payment" has been removed from the definition of online platform, but I'm not sure that this quite does it: are not Visa and Mastercard "online services" that "enable" the "sale" of goods within the meaning of the definition?) The Alibaba e-commerce platform (market cap $242.4 billion[85]) and the Tencent entertainment giant (>80 million Fortnite players[86]; market cap $449.6 billion[87]) do not appear to qualify.

It is important to appreciate what a departure AICOA would be for U.S. competition policy. I am not aware of any other instrument of U.S. competition policy that differentiates on the basis

[77] Statista, Worldwide visits to Walmart.com from December 2021 to May 2022 (June 2022), https://www.statista.com/statistics/714568/web-visits-to-walmartcom/.

[78] https://finance.yahoo.com/quote/WMT/.

[79] Statista, Largest credit card companies in the United States in 2019 and 2020, by number of active accounts (Nov. 2022), https://www.statista.com/statistics/605634/leading-credit-card-companies-usa-by-number-of-card-holders/; https://www.fool.com/the-ascent/research/credit-debit-card-market-share-network-issuer/.

[80] Visa Inc. Q1 2021 Operational Performance Data, https://s1.q4cdn.com/050606653/files/doc_financials/2021/q1/Visa-Inc.-Q1-2021-Operational-Performance-Data.pdf.

[81] https://finance.yahoo.com/quote/V/.

[82] Statista, Number of Mastercard credit cards in the United States and worldwide from the 2nd quarter of 2019 to 4th quarter of 2021 (Jan. 2022), https://www.statista.com/statistics/618137/number-of-mastercard-credit-cards-worldwide-by-region/.

[83] Mastercard 2022 Form 10-K, https://www.sec.gov/ix?doc=/Archives/edgar/data/1141391/000114139123000020/ma-20221231.htm, 7.

[84] https://finance.yahoo.com/quote/MA.

[85] https://finance.yahoo.com/quote/BABA/.

[86] Statista, https://www.statista.com/statistics/1238914/fortnite-mau/ (May 2020), https://www.statista.com/statistics/1238914/fortnite-mau/

[87] https://finance.yahoo.com/quote/TCEHY/

of market capitalization or other measure of bigness. Nor am I aware of any instrument of competition policy that has so many hallmarks of an effort to pick out specific businesses for special treatment. I think that our tradition is a point of pride for our legislative and regulatory practice: we do not pick winners and losers by name, or through criteria reverse-engineered with them in mind, nor do we single out politically unsuccessful businesses for special adverse treatment. I fear that breaking that tradition could have unhappy consequences. The unpopularity of the tech targets today may not break down along partisan lines, but with a little imagination one could imagine the same device being used in the future to target big businesses that have fallen out of favor with only one party, with AICOA cited as an example. That would be unfortunate.

Above all, it is not clear why the same regulatory response is appropriate for all the businesses that satisfy AICOA's thresholds and no others. For example, if the bill's concern is with durable monopoly power, why is there no requirement of durable monopoly power—or even market power—and no limitation to markets in which such power is present?[88] Why is the raw number of users or business users, annual sales, or market capitalization, relevant at all to the presence or absence of competitive concerns? If the concern is digital monopoly power, or digital platforms, why is the bill focused on a set of businesses that can be understood as having won the "last war," rather than others with monopoly power that may be smaller in absolute terms today but which enjoy considerable power in their respective markets? And what is the competitive concern that is common to the—very diverse—businesses that satisfy this definition, and not to

[88] As the ABA Antitrust Section observes: "[F]inding or designating a platform to be a 'covered platform' does not require or establish that it has market power in any relevant market. Size, in the sense of number of users or market capitalization, is not by itself evidence of market power. A firm may be large, as measured in these terms, yet lack the power to influence prices or exclude competitors." Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf.

other businesses? What is the basis for thinking that the competitive concerns in e-commerce markets are the same as those in search markets, or mobile operating-system markets, or app-store markets, or social networking markets, and so on?

And if bigness is really the concern, why are other big enterprises in other areas of the economy not included? Tesla's market cap is $650.8 billion; NVIDIA's is $578.5 billion; UnitedHealth's is $444.7 billion.[89] They perform important work in markets, including high-tech markets, that matter to the U.S. economy. They are big! And their businesses could be understood in some respects as platforms: particularly Tesla and UnitedHealth. Why not include them too?

In addition, the definition of "critical trading partner" is strikingly broad and vague. It appears to encompass any business that offers a desirable means of reaching customers for even a single business user! In particular, the concepts of "restrict," "impede," "need," and "effectively" invite confusion and endless, agonizing litigation. Critical trading partner status seems just to mean "very valuable." Suppose, for example, that Amazon enables third-party merchants to do much better than they were doing before Amazon came along, or than they would be doing if Amazon did not exist. Has Amazon become, for that reason, something that the merchants "need[] to effectively serve [their] users or customers"? If so—and I assume the intention is that it would indeed satisfy the definition—then a "critical trading partner" just means a business that supplies a valuable service. This criterion is wholly disconnected from concerns with competition, anticompetitive practices, or market and monopoly power.[90]

[89] https://finance.yahoo.com/quote/TSLA/; https://finance.yahoo.com/quote/NVDA/; https://finance.yahoo.com/quote/UNH/.

[90] *See, e.g.*, Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023) 4, https://ssrn.com/abstract=4347768 ("[N[othing in the statute requires any showing that the covered firm's trade in the particular product under examination be dominant. For example, Amazon would very likely be designated a critical trading partner on the basis of its overall retail business. At that point its prohibitions would attach to its sale of, say, groceries, even though Amazon's share of the grocery market is a little over 1%. The same thing would apply to Microsoft's search engine Bing. While Microsoft is large enough to be a covered platform, and

The message that AICOA sends to other businesses that may, also, plan to invest in creating a valuable service is not an encouraging one. We should not encourage businesses to fear that they will succeed their way into regulatory punishment.

b) A Bigness Criterion Simply Invites Divestiture

Making the definition of a covered platform contingent on bigness suggests a reasonably easy path for any covered platform that believes, or finds, that it cannot run its business under the obligations of Section 3(a). Simply divide your business into two or three—along lines that cannot be predicted in advance and would have nothing to do with competition, and will do nothing to reduce monopoly or market power in any market—and carry on as before. I cannot see how this outcome would help anyone.

The underlying point is that bigness is not a proxy for competitive concerns or for monopoly power. This is one reason why antitrust has long avoided using size criteria, focusing instead on market and monopoly power in particular markets.

3. "Online Platform" Includes Things that Are Neither Online nor Platforms

Section 2(a)(9)(A) defines an online platform very broadly as "a website, online or mobile application, operating system, digital assistant, or online service that enables—(i) a user to generate or share content that can be viewed by other users on the platform or to interact with other content on the platform; (ii) the offering, advertising, sale, purchase, or shipping of products or services, including software applications, between and among consumers or businesses not

very likely a critical trading partner in its Windows operating system, Bing struggles in the search engine market, with a roughly 3% market share of consumer search. This failure to distinguish between the overall footprint of firms that operate platforms and the market shares of their products largely undermines the AICOA's value as a tool for improving competition.").

controlled by the platform operator; or (iii) user searches or queries that access or display a volume of information[.]" Section 2(a)(9)(B) excludes certain wire and radio services from the definition.

This definition of "online platform" embraces a startling range of products and services that would not ordinarily be called either platforms or even online! Specifically, it includes many businesses and services that are not multisided platforms: for example, a simple file storage folder could constitute a platform if it was a website or application that enables users to search or query information. So could a mobile application that contained an offline encyclopedia, or a library of audio or video materials that can be accessed through the web (audio and video materials are information too!). Nor must the service be "online" in the sense of "accessed via the internet": being a "mobile application," an "operating system," or a "digital assistant" is enough.

I assume that this is not a drafting error: that Congress indeed prefers not to limit the definition to multisided platform businesses or to services that are supplied in real-time on the internet. As a result, it may be better to re-label the term "digital service" rather than "online platform."

4. "Business User" Is Overbroad and Vague

Section 2(a)(2) defines a "business user" to include "a person that uses or is likely to use a covered platform for the advertising, sale, or provision of products or services." That person then appears to be a business user for *all* purposes. This is an exceptionally broad definition that may exceed what Congress has in mind. As I read it, it covers virtually every business that advertises on the internet or uses digital services. If I advertise on a website, and that website is accessible through Google and can be viewed on an iPhone, or a Windows PC, I seem to have become a business user of Google, iOS, and Windows with respect to all my lines of business. If I write my

advertising copy on Microsoft Office, I am a business user of Microsoft Office with respect to all my business lines. And so on. Surely that cannot be what Congress has in mind! As this demonstrates, the definition of "use" is critical—as is the scope of the status of being a "business user" (*i.e.*, whether my use of a covered platform as to *one* of my business lines makes me a "business user" as to all of my business lines).

Thus, for example, a landscaping business appears to constitute a "business user" of an iPhone and the iOS system because the landscaping services will be advertised or sold over websites, or even phone calls, viewed or conducted through the smartphone. Or a component supplier would be a "business user" of that same iPhone if it, too, advertised over internet websites that could be viewed through the iPhone: inviting the creative argument that the component supplier was the victim of self-preferencing if Apple decided to use its own components rather than those of the component supplier in the iPhone. Surely none of this is what Congress intends! The point is that vague definitions invite arguments of exactly this kind (as well as much closer and harder cases). When profits are at issue, such arguments will certainly proliferate and drown courts and agencies. Lawyers, not consumers, will benefit. The definition of "business user" should almost certainly be narrowed.

5. "Influence" May Be a Better Term than "Control"

Section 2(a)(4) effectively defines "control" at the 25% ownership level. But 25% seems an awfully low threshold for "control" as that term is traditionally understood: it is possible to satisfy this definition without being able to determine the competitive behavior of the "controlled" entity. Indeed, as many as four different entities can have "control" on this definition. Regardless of one's views on the core principles of AICOA, it may be worth revising this threshold upward

so that it more closely approaches "control" in the traditional sense, or just re-labeling it "material influence" to improve transparency.

6. The Possibility of FTC Rulemaking Is Unclear

Section 3(c)(1)(A) provides that the FTC shall enforce AICOA as it enforces Section 5 of the FTC Act. This raises the prospect that the FTC, at least under current leadership, may pursue AICOA rulemaking pursuant to purported powers under Section 6(g) of the FTC Act.

There is considerable doubt regarding whether Section 6(g) of the FTC Act authorizes rulemaking. For one thing, it is very far from clear that, if Congress had intended to create a broad unfair-methods rulemaking power, it would have done so through the following language:

> The Commission shall also have power—
>
> [. . .]
>
> (g) Classification of corporations; regulations
>
> From time to time classify corporations and (except as provided in section 57a(a)(2) of this title) to make rules and regulations for the purpose of carrying out the provisions of this subchapter.

For another thing, current Supreme Court guidance does not generally appear to favor the inference of broad or novel agency powers in broadly similar circumstances.[91] However, to avoid uncertainty regarding Congressional intent on the question of AICOA rulemaking, Congress may wish to make this clear in the institutional provisions of any version of AICOA that may be passed.

[91] *See* Alabama Ass'n of Realtors v. Dept. of Health and Human Servs., 141 S.Ct. 2485 (2021); West Virginia v. EPA, 142 S.Ct. 2587 (2022); *but see* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672 (D.C. Cir. 1973) (upholding FTC rulemaking in a mixed competition / consumer protection case, albeit on grounds that are less widely accepted today).

7. The Interim Relief Provisions Are Too Generous

Section 3(c)(6)(C)(ii) provides that temporary injunctive relief may be awarded for a period of up to 120 days if "there is a plausible claim, supported by substantial evidence raising sufficiently serious questions going to the merits to make them fair ground for litigation, that a covered platform operator violated this Act; that the conduct alleged to violate this Act materially impairs the ability of business users to compete with the covered platform operator; and a temporary injunction would be in the public interest."

This is a specially *lowered*—that is, plaintiff-friendly—standard. As a general matter, the Supreme Court says that "A preliminary injunction is an extraordinary remedy never awarded as of right," and that "[i]n each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief."[92] Specifically, the Court has instructed that: "A plaintiff seeking a preliminary injunction must establish that [1] he is likely to succeed on the merits, that [2] he is likely to suffer irreparable harm in the absence of preliminary relief, that [3] the balance of equities tips in his favor, and that [4] an injunction is in the public interest."[93] Lower courts routinely apply this instruction.[94] In the

[92] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 24 (2008).

[93] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 20 (2008).

[94] *See, e.g.*, H&R Block, Inc. v. Block, Inc., 58 F.4th 939, 946 (8th Cir. 2023) ("[A] party seeking a preliminary injunction must demonstrate: (1) the threat of irreparable harm; (2) the state of the balance between the harm and the injury granting an injunction will inflict on other parties; (3) the probability it will succeed on the merits; and (4) the public interest."); Commonwealth v. Biden, 57 F.4th 545, 550 (6th Cir. 2023) ("We consider four factors in determining whether a preliminary injunction should issue: (1) whether the moving party has shown a likelihood of success on the merits; (2) whether the moving party will be irreparably injured absent an injunction; (3) whether issuing an injunction will harm other parties to the litigation; and (4) whether an injunction is in the public interest."); Dream Defs. v. Governor of the State of Fla., 57 F.4th 879, 889 (11th Cir. 2023) ("A district court may grant a preliminary injunction only if the moving party shows: (1) "it has a substantial likelihood of success on the merits;" (2) "it will suffer an irreparable injury unless the injunction is granted;" (3) "the harm from the threatened injury outweighs the harm the injunction would cause the opposing party;" and (4) "the injunction would not be adverse to the public interest."); Singh v. Berger, 56 F.4th 88, 95 (D.C. Cir. 2022) ("A preliminary injunction is an extraordinary remedy that requires a moving party to make a "clear showing" that (1) it has a likelihood of success on the merits, (2) the balance of equities favors preliminary relief, (3) an injunction is in the public interest, and (4) it will likely suffer irreparable harm before the district court can resolve the merits of the case.").

Second Circuit, a party seeking a preliminary injunction must show: (1) irreparable harm *plus* (2) either (a) a substantial likelihood of success on the merits or (b) *both* sufficiently serious questions going to the merits *and* a balance of hardships that tips in the favor of the party seeking an injunction.[95]

But under AICOA a movant need only show that it is plausible—*not* likely—that there was a violation, a material impairment of ability to compete, and that an injunction is in the public interest. There is no irreparable harm requirement at all, and no consideration of the impact on the platform or associated equities or hardships. This is obviously a much more favorable standard for an injunction-seeker than even the Second Circuit's standard.

AICOA thus creates a specially lowered standard for preliminary injunctive relief, despite the Supreme Court's guidance. But it is not clear why this is remotely appropriate. Preliminary injunctive relief in an AICOA case will almost certainly involve forcing the platform to deal with some third party or category of third parties—including sharing data or access to digital infrastructure—and/or freezing the launch of some new innovation or feature, for up to four months. During this time, a competitor may steal a march to market on some new product generation in a product-improvement; a bad actor may obtain access to user data or commercially sensitive information; and so on. This seems undesirable.

[95] Ventura de Paulino v. New York City Dep't of Educ., 959 F.3d 519, 529 (2d Cir. 2020) ("Ordinarily, to obtain a preliminary injunction, the movant has to "show (a) irreparable harm and (b) either (1) likelihood of success on the merits or (2) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly toward the party requesting the preliminary relief.""); New York ex rel. Schneiderman v. Actavis PLC, 787 F.3d 638, 650 (2d Cir. 2015) ("A party seeking a preliminary injunction must ordinarily establish (1) "irreparable harm"; (2) "either (a) a likelihood of success on the merits, or (b) sufficiently serious questions going to the merits of its claims to make them fair ground for litigation, plus a balance of the hardships tipping decidedly in favor of the moving party"; and (3) "that a preliminary injunction is in the public interest."); *see also* Citigroup Glob. Markets, Inc. v. VCG Special Opportunities Master Fund Ltd., 598 F.3d 30, 38 (2d Cir. 2010) (holding that this standard survives *Winter*).

It is worth considering the effect, not just of this interim-relief prohibition, but of its *threat* value in commercial negotiations. The prospect that an investigation will involve interim relief of this kind will be a powerful threat point for a third party bargaining with the platform, or even a government authority (such as a federal agency or State AG) earnestly but unwisely challenging reasonable conduct by the platform.

8. Forfeiture Is a Dramatic Remedy Given AICOA's Breadth

Section 3(c)(6)(D) provides that a "pattern or practice" of violating AICOA may result in forfeiture of a year's compensation by any appropriate corporate officer.

My main concern with this provision is that it will seriously exacerbate the risk that platforms will err on the side of favoring businesses (and their demands for access), over consumers (and their need for protection). AICOA already creates plenty of other reasons for a platform to fear that restricting third-party access will lead to plenty of hassles, costs, and business risks, even when there are reasonable grounds for concern and even when important consumer interests are hanging in the balance—as they often will be. But decisionmakers will become a *lot* more solicitous of third party interests when saying "no" instead of "yes" could result in the sacrifice of personal compensation.

I also fear that this provision is unduly punitive. To be sure: there may be cases in which forfeiture of compensation is an appropriate response to corporate wrongdoing. Clear and naked wrongdoing like fraud, bribery, flagrant and knowing violations of law seem to fall into this category. But—given the extraordinary breadth and vagueness of its terms, and the fact that a violation may involve nothing more than a product improvement—an AICOA violation is surely not one of them. Indeed, as currently written, it may be hard to find any major tech company that

is *not* engaged in a pattern or practice of violating AICOA! Moreover, it is very far from clear how to comply with the statute. Congress may not want to make a leadership role in a tech company a poisoned chalice in quite this fashion.

Accordingly, I would eliminate this provision.

9. The Limitations Period Is Unduly Long

Section 3(c)(7) provides for a six-year statute of limitations. This is strikingly long, above all for offenses that are so broadly and vaguely defined. Antitrust violations are subject to a four-year statute of limitations for challenges brought by injured persons and State Attorneys-General: something similar seems right for AICOA.[96]

10. The Exceptions Are Too Narrow

a) Intellectual property

Section 3(c)(8)(A)(i)–(ii) provides that nothing in Section 3(a) shall "require a covered platform operator to divulge or license any intellectual property, including any trade secrets, business secrets, or other confidential proprietary business processes, owned by or licensed to the covered platform operator," or "to prevent a covered platform operator from asserting its preexisting rights under intellectual property law to prevent the unauthorized use of any intellectual property owned by or duly licensed to the covered platform operator." Similarly, Section (c)(8)(B) protects actions that are "reasonably tailored to protect [certain copyright and trademark] rights of third parties." Thus, AICOA seems to create an absolute defense to a claim under Section 3(a) if

[96] 15 U.S.C. § 15b.

equal treatment (or other compliance) would necessarily involve an IP license, or if the action is reasonably tailored to protect certain third-party IP rights.

This is welcome to the extent that it helps to narrow the broad reaches of Section 3(a). But it creates a very sharp disconnect between IP rights, which are specially protected under AICOA, and all other property and contract rights, which are subject to enforced sharing under Section 3(a). It is not obvious why this disconnect is appropriate, or why AICOA does not reflect similar concerns about forced sharing outside the IP context.

b) Federal government blacklist

Section 3(c)(8)(A)(iii) provides that nothing in Section 3(a) shall "require a covered platform operator to interoperate or share data with persons or business users that are on [a federal government blacklist]." Again, this is a welcome qualification: it is certainly better to include it than not to do so. But plenty of entities, and categories of entities, will give grounds for serious concern—including on national security grounds—without appearing on a government blacklist.

c) Foreign adversaries

Section 3(c)(8)(A)(v) provides that nothing in Section 3(a) shall be construed "in a manner that would likely result in data on the covered platform or data from another business user being transferred to the Government of the People's Republic of China or the government of a foreign adversary." This is another welcome qualification. But it is exceedingly narrow. The real danger is probably not, or not exclusively, that an entity visibly affiliated with an adversary government seeks equal treatment. The real danger is that, in practice, platforms will generally not be in a position to know whether or not an adversary government lurks behind—or has control or

influence over or access to—an entity, or a category of entities seeking access to covered platforms. And this provision seems little or no help in responding to that real-world problem.

III. THE OPEN APP MARKETS ACT (S. 2710)

I have reviewed a draft of the Open App Markets Act ("OAMA"), as reported to the Senate on February 17, 2022.[97] For the reasons explained below, I do not support OAMA in its current form. But I would support a narrower version.

A. Summary

OAMA exemplifies a much more promising approach to digital-markets regulation than AICOA. It is focused on a specific and reasonably well-defined set of markets that are similar to one another: markets for the sale and distribution of apps, and for app-store services. It is unlikely to prohibit or deter a wide array of product improvements and feature innovations. And it clearly aims to provide significant room for platforms to take reasonable measures for good reasons.

On substance, also, I generally support at least three of the bill's ideas.

First, most-favored-nation clauses ("MFNs") are commitments by a bound party to offer a beneficiary terms that are at least as favorable as those that the bound party offers to the beneficiary's competitors (or to other third parties). They can promote competition, by ensuring that the beneficiary (and its own customers) can benefit from whatever favorable terms—such as low prices—the bound party is able to provide. But they can also penalize and deter discounting that may stimulate competition with the beneficiary, because they make discounting more expensive. When used by an app store with significant market or monopoly power, I fear that MFNs clauses may do more harm than good. And I also do not much worry about the ability of large digital platforms to bargain robustly to get favorable terms.

[97] https://www.congress.gov/117/bills/s2710/BILLS-117s2710rs.pdf (OAMA Feb. 2022 draft).

Accordingly, I support a ban on app price MFNs for app stores with significant market or monopoly power. I doubt such a ban will do much harm, and I think it could do some good.

Second, I also would support a limited ban on the competitive use of competitively sensitive nonpublic business information obtained by an app store owner directly from an app developer as a condition of operating the app store. For example, I would not allow an app store owner to make competitive use of app code, business plans, or other material that it may care to demand from an app developer as a prerequisite for being allowed on the app store.

To be clear: the limited ban that I support is much narrower than OAMA's current ban on use of data. I think app stores should be free to use all other data—including data about customer demand, searches, downloads, and so on—to compete against app developers, even in its own store. I also think app store owners should be free to buy data, and developers should be free to sell it to them. Restricting app stores from doing so would be a clear case of forcing a platform to do *less* for consumers and *more* for other businesses.

Third, I would also support transparency obligations to make sure that consumers know when paid advertising is affecting a search ranking or similar placement. A mandatory disclosure like "Ad" or "Advertising" would help consumers, and harm no-one.

But I do not support the rest of OAMA, and I fear that as currently framed it would do significant harm. Above all, I fear that forcing covered companies to host third-party app stores and third-party in-app payment systems would compromise security and quality in ways that would seriously harm consumers. Cybersecurity experts have highlighted the increased dangers of third-party app stores, and the importance of careful screening of apps. I also oppose non-discrimination obligations in app carriage for the same reasons that I oppose equivalent duties in AICOA. I think

Congress should not get into the business of punishing product improvements, nor deterring platforms from protecting users.

B. Some OAMA Provisions Could Stimulate Competition and Benefit Consumers

I support narrowed versions of three of OAMA's prohibitions: a ban on app pricing MFNs for app stores with significant market or monopoly power; a ban on competitive use of competitively sensitive nonpublic business information received directly by a covered company from an app developer in the course of operating an app store, for app stores with significant market or monopoly power; and an obligation to disclose paid advertising in search rankings or other placement.

1. Banning App Pricing MFNs Could Stimulate Interplatform Competition

Although Sections 3(a)(2) and 3(a)(3) of the current draft are found under the subtitle "Exclusivity and Tying," they are more accurately described as a prohibition against "most favored nation" (or MFN) obligations focused on app pricing.

In general, an MFN obligation commits one business (the bound party) to offer another business (the beneficiary) the best terms that the bound party is offering to any third party. An MFN assures the beneficiary that it is enjoying the most favorable terms that the bound party is able to offer. It may thus improve competition by reducing negotiation costs and spreading the benefits of favorable terms such as low prices.

But an MFN may also harm competition. In particular, it may be imposed by a business with market or monopoly power as a means of making sure that its trading partners cannot induce or sponsor competition by offering more favorable terms—such as low prices—to new entrants or

existing rivals. If a trading partner tried to use favorable terms to encourage rivalry with the monopolist, the MFN obligation would ensure that those favorable terms would have to be shared with the platform monopolist itself. This would, of course, eliminate the margin of favor that could induce entry or expansion, and make the effort self-defeating. The result: less competition.

Sections 3(a)(2) and 3(a)(3) can be understood as a ban on, among other things, the use of certain app pricing MFNs by app stores. In particular, Section 3(a)(2) prohibits a covered company from "requir[ing] as a term of distribution on an app store that pricing terms or conditions of sale be equal to or more favorable on its app store than the terms or conditions under another app store." (I think there is a typo here: I think the word "under" is supposed to read "on.") With that edit, I read this rule to effectively ban a covered company from requiring that apps be supplied for the cheapest available price as a condition of carriage on the app store. Implementing the ban in Section 3(a)(2) means that businesses will be able to offer special terms (*e.g.*, promotional pricing) to other channels without being kicked off the app store as a result.

I note that the meaning of the term "conditions of sale" is unclear: it seems to reach more broadly than pricing but does not appear to include all forms of most favored treatment: I would either clarify it or remove this provision.

Section 3(a)(3) prohibits a covered company from "tak[ing] punitive action or otherwise impos[ing] less favorable terms and conditions against a developer for using or offering different pricing terms or conditions of sale through another in-app payment system or on another app store." This rule effectively bans a covered company from giving better distribution to a developer that gives the platform better terms.

I think it is fairly clear that the use of certain kinds of MFN by dominant platforms can present some of the most troubling, and least beneficial, effects associated with MFNs. There is a real risk that platforms with significant market or monopoly power may use them to suppress discounting by lower-cost alternatives. And I do not much fear that such platforms will be unable to bargain firmly for favorable prices and terms on behalf of their customers. As such, I would be supportive of an appropriately tailored ban on app pricing MFNs by app stores with significant market or monopoly power.

On the other hand, I do think covered companies should be able to truthfully inform their consumers when an app is being offered on the best available terms, for example with a little badge, icon, or text that says "best pricing online!" or similar. This will inform consumers of truthful information that matters to competition.

But accepting both of those propositions means that a line will have to be drawn somewhere in the middle, because the spectrum between them is a bit messier than one might like. In particular, Congress may wish to reflect on at least (1) whether a covered company should be able to specially place or promote apps with best-pricing status (*e.g.*, by placing them more prominently in the app store on the basis that consumers are particularly interested in such apps, or by sending promotional emails to feature some apps that are being offered at "best pricing online" prices), and (2) whether a covered company should be able to induce best-pricing status by offering other kinds of value besides preferred placement and promotion (*e.g.*, lower distribution fees).

This is a close question. My own view is that it is probably not very sensible to *both* try to ban MFNs as a condition of carriage *and* allow a covered company to buy MFN status with preferred distribution or other favorable terms. It would simply be too easy for a covered company

to provide only minimal distribution, or non-feasible distribution, to all apps except those for which an MFN pricing commitment was made, and effectively reproduce the MFN. I also do not think the sky will fall in any relevant sense if app stores are prohibited from giving or withdrawing preferential status based on the prices at which apps are available elsewhere.

Ultimately, I think consumers will be better served by preserving the opportunity for discounting through other channels to support interplatform competition than they would be served by ensuring the possibility of favored promotion for best-priced apps.

That would suggest a reasonably simple rule: a covered company may not make any benefit or value—including preferred placement or distribution—conditional on most-favored pricing status, except that a covered company may accurately inform consumers when an app is being offered at the best available price.

I would limit this rule to app stores with significant market or monopoly power. Such a determination could be made administratively (subject to judicial review) and subject to review at regular intervals or upon the petition of the covered company.

2. A Limited Data Use Ban Could Promote Competition

Section 3(c) of the current draft bans a covered company from using "nonpublic business information derived from a third-party app for the purpose of competing with that app." In its current form, as I explain below, I think this provision, coupled with the definition of "nonpublic business information" in Section 2(6), is much too broad, and would prohibit the use of data that is lawfully in the hands of the app store to better serve consumers.

There are two kinds of practice that, in my view, should be protected by any bill. First, it is important that an app store be able to use for competitive purposes the information lawfully within its own hands as a result of that role, including information about consumer demand, searches, downloads, and purchases. Just like any store that both retails and manufactures, an important source of consumer benefit is the possibility that the retail information will inform better manufacturing. That is just as true for app stores as it is for other businesses. Second, it is also important to protect the ability of an app developer to sell—and an app store to buy and use—data that can be more effectively used or commercialized by the app store owner than the developer. Preventing that sale, as Doug Melamed has pointed out, would inflict harm to no good end.[98]

But I think it would be reasonable, and perhaps beneficial, to prevent app stores from making competitive use of nonpublic, competitively sensitive information—such as app code or future business plans—received directly from an app developer as a condition of operating the store. If app store operators with market or monopoly power imposed an obligation to provide such information to the app store and could then make competitive use of it against the apps, developers' incentives to invest in valuable feature improvements would be reduced and suppressed.

In principle—and subject to closer examination (as I am not an expert on the operation of app stores!)—I think the needle can be threaded well enough by limiting the restriction to a ban on competitive use of competitively sensitive nonpublic business information (1) received directly from the developer (2) as a condition of operating the app store business, and specifically protecting the app store's right to use *all other information and data* generated by the app store or

[98] A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

activity by anyone (customer or app developer) on or in the app store, as well as the right to enter into separate agreements for the purchase and sale of data.

In sum: I propose that a covered company should be able to make competitive use of all data, *except* competitively sensitive nonpublic business information turned over directly by the developer as a condition of access to an app store with significant market or monopoly power.[99]

3. A Requirement to Disclose Paid Advertising Through Ranking or Placement

Section 3(e) bans a covered company from engaging in certain forms of self-preferencing in app search. The provision specifically exempts "clearly disclosed advertising" in Section 3(e)(2)(B). In its current form, as I explain below, I think this provision is much too broad and will harm consumers (for reasons broadly equivalent to those discussed in the context of AICOA[100]).

But the exemption suggests a valuable rule. It would not be unreasonable to require that a covered company clearly disclose paid advertising that affects search ranking or involves preferred placement. When businesses pay for preferred app placement, consumers can easily be made aware of that fact—and disclosing advertising does not require upending algorithms or banning product improvements or procompetitive product distribution.

This could be accomplished by a specific and targeted provision requiring that any advertising for a business user involving preferred ranking, placement, or promotion be clearly disclosed, particularly by an app store with significant market or monopoly power. The FTC's

[99] I do appreciate that this could in principle create some opportunities for gamesmanship, by designing or operating stores in such a way as to gather additional competitively sensitive data "on" or "through" the platform rather than directly from the developer. I do not think there is a good solution to this problem that can be solved without doing more harm than good. And if forced to do so, I would probably be willing to sacrifice the benefits of the non-use rule in order to save the consumer benefits of the app store's ability to make competitive use of data.

[100] *See supra* § II.B–D.

Endorsement Guides may offer a useful framework: for example, one could imagine a provision that a covered company must "clearly and conspicuously disclose" the fact of paid promotion or preferencing.[101]

C. OAMA's Other Provisions Would Harm Consumers

I do not support the remainder of OAMA. I am particularly concerned by OAMA's forced access provisions, which I fear would threaten consumers and platforms.

1. Forcing Third Party IAPs Harms App Store Security and Viability

Section 3(a)(1) prohibits a covered company from "requir[ing] developers to use or enable an in-app payment system owned or controlled by the covered platform or any of its business partners as a condition of the distribution of an app on an app store or accessible on an operating system."

It is not quite clear what this means. Taken literally, it means that a covered company may not require that an app use the covered company's *own* IAP in order to be admitted to the app store or ecosystem, but it does not prevent a covered company from banning all other IAPs. In other words, an app store can say: "you choose—my IAP system, or no IAP system," and it will have complied with the provision. If that's the intended meaning, I don't object, but it's hard to believe that's really what anyone intends!

Nor is it really clear what "business partner" means. Suppose that an app store owner sets up an "approved IAP" program: IAP providers submit to careful checks and audits to make sure

[101] *See* FTC, Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255; *see also* FTC, The FTC's Endorsement Guides: What People Are Asking (updated Aug. 27, 2020), https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking.

that their IAP system is sufficiently safe and secure to be allowed on the platform. They may pay the app store for the right to be permitted in apps on the store (for this, too, is a form of distribution provided by the app store to the IAP system owner), or app developers may themselves pay for the right to use a third-party IAP. I cannot imagine why an app store should be prohibited from setting up a program of that kind.

In any event: I will assume that the intent is to re-draft the rule to require that an app store allow (some? all?) third-party IAP systems in apps sold on the store and used in the ecosystem.

Understood in this way, such a rule would generate two problems, both of which appear fairly serious. The first problem is a security one. Forcing app stores to allow third-party payment systems—or preventing or deterring them from imposing restrictions—puts consumers at risk by exposing their financial information to third parties on their platform. An app may knowingly or unknowingly choose to use an IAP that is low-quality, insecure, vulnerable to hostile or malicious actors, or simply run by those with little incentive or ability to serve consumers' interests, making it difficult for consumers to contest charges and obtain refunds.

Today, major app stores have every incentive to ensure that IAP systems are easy, secure, and safe, and that they handle requests for refunds or error corrections promptly and effectively. After all, when apps in an app store become unsafe for users, the app store becomes less appealing. Store owners also have the ability to keep consumers safe when they control the IAP. If an individual app turns out to be malicious or unsafe, a platform that controls the IAP can cut off its ability to extract funds, and can easily refund consumers.

But individual app developers do not have such an incentive. They can benefit—innocently or knowingly—from the high reputation of a platform or app store to win consumer confidence,

and expose consumers to harm after they have been downloaded and installed by an unsuspecting user. An individual app developer may choose a third-party IAP because it is cheap, because it is the first one the developer finds, or because it is part of a hostile or malicious plan.

The second problem is a commercial one. If app stores are forced to allow developers to operate their own IAP systems without a means of ensuring compensation for in-app purchases—that is, without becoming "business partners" with the IAP provider—then there is a serious threat that developers' business models will migrate overnight from charging for an app (an event on which the app store can take a commission) to charging for in-app purchases through developers' own IAPs (an event that is or may be invisible to the app store). For example, suppose that an app store charges 30% of the price of an app and all apps end up being priced at $9.99. If it then allows third party IAP systems without any means of monitoring and charging in-app payments, one would expect that overnight those apps will move to a $0.00 price point with a $9.99 in-app purchase required on first use. (Or something similar!) The result is a distortion in pricing incentives, with a sharp drop in platform revenue, and less security. App stores may in turn be forced to move to other pricing models, like flat fees, which will make many app business models entirely non-viable. (Of course: I am not suggesting that app stores should have a right to take a commission for purchases of things *other than the app itself*.)

My point is a modest one: forcing or incentivizing app stores to say "yes" to IAP providers when they would otherwise say "no" is bad for security, even while it has other benefits. And if the consequence is to allow developers to move app pricing to an invisible space, that outcome seems bad for commercial viability and likely to result in less efficient arrangements all round.

2. Forcing Off-Platform Steering Threatens App Store Viability

Section 3(b) of the current draft prohibits a covered company—anyone operating an app store or app distribution system platform with 50 million users or more in the United States—from "impos[ing] restrictions on communications of developers with the users of an app of the developer through the app or direct outreach to a use concerning legitimate business offers, such as pricing terms and product or service offerings." It allows a covered company to give a user the opportunity to consent before "collection and sharing of the data of the user by an app."

I am sympathetic to the project of this provision, and my feelings are somewhat mixed. Such a rule could have real benefits, and my first instinct was to include this in the set of rules that I would support. But on reflection I think the costs and harms would probably overwhelm the benefits. As such, I do not support the rule.

Benefits first. There is obviously plenty to be said for a rule of this kind, at least as applied to app stores with market or monopoly power. It ensures that app developers have the opportunity to provide customers with accurate information about off-platform opportunities (including promotions and differentiated offerings through other channels, such as discounted prices of which a consumer may not have been aware). It thus could promote competition with the platform itself.

But a rule of this kind presents two different risks.

The first risk seems to be an existential commercial one. There is a clear threat that app developers will use the app store to generate customer leads and will then move those customers off-platform for all paid activity, including the purchase of the app itself. This, in turn, could threaten the profitability of the app store itself, and push app stores to less efficient charging mechanisms like flat fees. (If an app store charges a flat $3 for distribution, plenty of valuable apps

would become impossible to profitably sell on the store.) From this perspective, the communication restriction can be understood as an effort to protect against developer conduct that would otherwise erode or even destroy the business case for the app store in the first place.

To make this concrete: a developer with a fully free right to communicate with users could just charge a low or zero price for the app itself and move the payment for the app off-platform ("Thanks for downloading our app for free on the Apple App Store. To use our app, you must activate it by going to [website].com, entering a code and paying $5.99."). The result would be that an app store received *zero* revenue despite conferring massive value on the app developer. That does not seem a sustainable circumstance.

The second risk is a threat to quality: specifically, the risk that the platform experience could easily be turned into a spammy and unwelcome one. Imagine if the developer of every app you had ever downloaded had the right to get your contact details from the relevant app store, and the automatic and permanent ability to contact you through emails, text messages, popup notifications, phone calls, and other forms of communication. The result would almost certainly be a barrage of marketing misery on your device: and among other things this could seriously erode the value of the app store and ecosystem. It may be instructive to imagine what would happen if all the manufacturers of products you bought at the supermarket could freely contact you in perpetuity because you bought their product. It is not clear that that would be a better world for consumers—*regardless of whether there was a one-time consent at the time of purchase*. Not every developer will respect an "unsubscribe" click, or will do so promptly.

So on balance I do not support this provision, although I will continue to try to think of a narrower version that would not threaten app store profitability or the quality of the experience.

3. The Data Non-Use Obligation Threatens Desirable Conduct

Section 3(c) bans a covered platform from using "nonpublic business information derived from a third-party app for the purpose of competing with that app."

In its current form, I think this is much too broad, and likely to be anti-consumer in its operation. In principle, as I noted above, I would not object to a prohibition on app stores making competing use of competitively sensitive nonpublic business information obtained directly from the developer as a condition of participation in the app store, rather than from the operation of the platform. If an app store owner demanded such information as a price of admission—such as the code used to perform desirable functions—incentives for apps to invest in desirable features would be stifled. But it does not seem wise to try to *ban* app stores from asking for such data, as it may well be necessary for legitimate purposes (such as security or quality audits). As such, the best solution seems to be a ban on competitive use of competitively sensitive nonpublic business information *received directly from the developer* as a condition of operating the app store.

But the current draft goes much too far. Pursuant to Section 2(6), "nonpublic business information" includes virtually all information gained in the course of operating the app store itself. Specifically, it includes: "nonpublic data that is . . . derived from a developer or an app or app store owned or controlled by a developer, including interactions between users and the app or app store of the developer; and . . . collected by a covered company in the course of operating an app store or providing an operating system."

There are two problems with this definition. First, because a covered company is itself a developer (by reason of the definition of "developer" in Section 2(4)), it appears to include

virtually all the data a covered company obtains. (This seems to be a drafting error rather than a substantive issue.)

Second, almost everything that happens on an app store is in some sense actually or arguably "derived from" the apps in the store! So this would could prohibit an app store owner from using information that consumers are, for example, interested in video-sharing apps, or that they are searching for games with a dog theme, or that they tend to be drawn to apps with a yellow icon, and responding accordingly to meet demand. It would also prevent app stores from buying—and developers from selling—valuable data that could best be commercialized by the app store owner.

Accordingly, I propose app stores should be allowed to use information gathered from the operation of the app store—including information about user and business user activity on and in the app store—for competitive purposes, and they should be allowed to buy data for competitive use from developers. Only competitively sensitive nonpublic business information received directly from the developer as a condition of participation in the app store would be protected. (On one reading of the text, this is precisely what Section 3(c) aims to capture, in which case this is just a suggestion as to drafting rather than a substantive disagreement!)

All of this assumes, of course, that it is possible in practice to live with the line of separation that I have articulated. If it is not, and if no reasonably close equivalent was available, I would probably abandon the effort to police the line and would allow full competitive use.

In addition, the broad definition of "nonpublic business information" in Section 2(6), which cuts much too broadly by including information generated by the store's own business rather than obtained directly from an app developer, should be abandoned.

4. Forcing Access for Apps and App Stores Threatens Users

Section 3(d) requires a covered company that controls both app store *and* an operating system on which that app store runs to allow users to: "choose third-party apps or app stores as defaults for [appropriate] categories"; "install third-party apps or app stores through means other than its app store"; and "hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners."

As a threshold matter, this provision is not clearly drafted: it is not clear whether the drafter intends that a covered company can satisfy its obligation by allowing *some* third-party options, at its own election, or must allow *all* such options.

But serious harm seems likely. First, and most importantly: an obligation to allow third-party app stores would force open the gates of each operating system to the world. Operating system owners could no longer control the flow of applications and code into their own ecosystems. They would no longer be in a position to ensure the quality, compatibility, or freedom from malicious code of the apps that flow into their operating-system ecosystems, or to make sure that developers are reputable and free from hostile influence or control. This would expose consumers to serious threats: threats to quality, user privacy, financial privacy, the security of their devices (including access to cameras, microphones, and GPS location), the integrity of the operating system, and so on.

There is an overwhelming consensus among cybersecurity experts that third-party app stores, and unscreened apps, present greater danger for users and systems, serving as entry points for malware and hostile actors to obtain access to users and their data.

The **U.S. Cybersecurity and Infrastructure Security Agency** in the Department of Homeland Security says: "Reduce the risk of downloading [potentially harmful apps] by *limiting your download sources to official app stores*, such as your device's manufacturer or operating system app store. *Do not download from unknown sources*[.]"[102]

The **Federal Bureau of Investigation** "recommends only obtaining smartphone [banking] apps from *trusted sources like official app stores or directly from bank websites*."[103]

The U.S. **National Security Agency**'s Mobile Device Best Practices document states: "Install . . . only [applications] from *official application stores*."[104]

The **Federal Trade Commission** says: "Use official app stores. To reduce the risk of installing potentially harmful apps, download apps *only from official app stores*, such as your device's manufacturer or operating system app store."[105]

The **General Services Administration** says: "Allowing mobile apps to be loaded from an unknown source presents *one of the greatest risks* to GSA's environment when using mobile devices."[106]

The UK's **National Cyber Security Center**'s Threat Report on Application Stores states that "even official app stores (such as Apple's App Store and Google's Play Store) with vetting processes to detect malicious functionality in apps have been impacted by malware. Furthermore,

[102] https://www.cisa.gov/news-events/news/privacy-and-mobile-device-apps (emphasis added).

[103] https://www.ic3.gov/Media/Y2020/PSA200610 (emphasis added).

[104] https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF (emphasis added).

[105] https://consumer.ftc.gov/articles/how-protect-your-privacy-apps (emphasis added).

[106] https://www.gsa.gov/cdnstatic/Securing_Mobile_Devices_and_Applications_%5BCIO_IT_Security_12-67_Rev_4%5D_01-26-2018.pdf, 17.

the current well-known *third party app stores* (that is, stores which are not provided by the manufacturer or the operating system provider) appear to have *less robust vetting processes, and so represent a greater risk*."[107] It warns: "While there's [fewer] people using the most common third party app stores (compared with official app stores), a lack of robust vetting processes means that their users are *especially vulnerable to threat actors* uploading malware[.]"[108]

McAfee's 2023 Consumer Mobile Threat Report states: "*Stick to the verified stores[.]* While any app store is susceptible to hosting malicious applications, official platforms like Google Play and the Apple App Store have rigorous processes in place to both examine apps before they are released and to identify and remove malicious apps that are discovered after release. *Third-party app stores do not necessarily observe these processes, and some are even designed to intentionally distribute malware to mobile users.*"[109] And: "[I]t's essential that you download applications from official app stores like Google Play or the Apple Store."[110]

Nokia's 2021 Threat Intelligence Report contains abundant analysis of the dangers and risks. It urges: "[t]he easiest and most obvious form of prevention is to *download apps only from official app stores*."[111] And "*[b]ecause of the risks of third-party apps, endpoint security teams have always advised users to download apps exclusively from official channels such as Google*

[107] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 7 (emphasis added).

[108] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 11 (emphasis added).

[109] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 8 (emphasis added).

[110] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 24.

[111] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).

Play and the Apple App Store. But this advice is often not enough as malware writers continue to come up with new ways to get rogue apps into these official stores undetected."[112]

The 2021 Nokia report notes that the closed model of Apple's iOS has been instrumental to its security: "While Google has taken an open approach to app development and distribution, Apple has always maintained a proprietary approach, allowing downloads only through the official App Store. *As a result, Apple products have generally been considered the most secure mobile computing platform.*"[113] "Among smartphones, Android devices remain *the most targeted* by malware *due to the open environment and availability of third-party app stores.*"[114] Indeed: "Android devices make up 50.31% of all infected devices," with iOS far behind.[115]

Nokia's 2020 report urges the same point: Users should "[i]nstall *only applications that are from trusted app stores (*Google Play, Apple, Microsoft)."[116] And it repeatedly emphasizes the difference between official and third-party app stores: "Over the last few years, a significant improvement has been seen in the security of official mobile app stores. However, *third-party app stores are still rife with Trojanized applications.*"[117] "The security of official app stores, such as Google Play Store, has increased continuously. However, *the fact that Android applications can be downloaded from just about anywhere still represents a huge problem, as users are free to*

[112] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).
[113] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).
[114] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).
[115] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).
[116] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 6 (emphasis added).
[117] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 7 (emphasis added).

download apps from third-party app stores, where many of the applications, while functional, are Trojanized. iPhone applications . . . are for the most part limited to one source, the Apple Store."[118]

This is quite a consensus. The risks are bad enough for every user. But unsophisticated or vulnerable users—including children, seniors, and those unfamiliar with particular devices—will almost certainly not be in much of a position to protect themselves, and their infected devices will in turn present risks to others. Third-party app stores are a notorious vector for infection of devices—and devices in turn are a vector for infection of Americans' home networks. Indeed, as the 2020 Nokia report notes, "an increased number of Android malware infections has been detected in residential [*i.e.*, home] networks."[119]

There cannot be any serious room for doubt. Forcing more third-party app stores into our digital ecosystem will put consumers at greater risk.

The same is true of rules that force more third-party *apps* into app stores. It is also widely appreciated that hostile and malicious apps commonly disguise themselves as benign apps, even sneaking onto official app stores.[120] The 2021 Nokia report notes that "[s]ome types of malware are well known for masquerading as legitimate applications," and that Android malware often relies upon "[m]imicry of popular apps including health and fitness, photography, utility, personalization, and communication apps."[121] And McAfee's 2023 report explains: "[M]any malicious apps actually deliver some legitimate functionality. Just because the free photo editor or social media tracker you downloaded works, doesn't mean that it's not hiding something.

[118] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 8 (emphasis added).

[119] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 12.

[120] *See supra* note 27 and accompanying text.

[121] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 19.

Criminals often use encryption to hide their malicious code from reviewers, or they build in a delay, so the bad stuff doesn't show up until it has passed the tests. Another trick is to check the device's location and only behave badly in certain countries. Others download additional code to themselves after installation, keeping reviewers from ever seeing the malicious bits. Finally, sometimes criminals manage to infect legitimate apps by putting their code in a third-party code library that gets automatically included in the next software update."[122]

In other words: deterring app stores from restricting and supervising the flow of apps into the store will put consumers at greater risk.

Second, a general obligation to allow users to use a third-party app for *every* function on an OS—regardless of how central that function is to the OS itself—does not seem remotely plausible. Must a covered company allow a third-party file browser? A third party command line interface? A third party settings app? And so on. This provision appears to require that an operating system open itself up to third-party functions of every kind. This may not be Congress's intention.

Third, allowing consumers to delete critical apps and app stores, rather than just select others as defaults, exposes consumers to the risk that unsophisticated users—or those misled by malicious actors—will be able to degrade the functionality of their own device. It is not clear that this would be overall beneficial.

My concerns here mirror those I expressed in connection with AICOA: this amounts to a ban on closed systems, and a sharp challenge to system security, and I think that would be a mistaken and dangerous step. In particular, platforms should not face penalties for saying "no" to

[122] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 6.

third-party app stores, when such stores constitute a critical vector of threats to American consumers and families—nor for erring on the side of safety when it comes to suspicious apps.

5. A Ban on "Unreasonable" App Self-Preferencing Will Harm Consumers

Section 3(e) prohibits a covered company from "provid[ing] unequal treatment of apps in an app store through unreasonably preferencing or ranking the apps of the covered company or any of its business partners over those of other apps in organic search results." In turn, "unreasonably preferencing" is defined in Section 3(e)(2) to *include* ranking apps based on ownership by the covered company or its business partners (*i.e.*, preferring the covered company's own apps) and to *exclude* "clearly disclosed advertising." I think this is much too broad as drafted, and I expect that consumer harm would result.

First, the provision could—and I think likely would—be read to include an obligation not just to *rank* third-party apps, but to *carry* third-party apps in the first place. After all, distributing one's own apps while entirely refusing to distribute those of some, or all, third parties, is certainly a form of "preferencing." But a must-carry obligation for apps would be harmful for all the reasons that AICOA's various forced access obligations would be harmful. In short, it would expose consumers to significant increased risks, including risks to quality, privacy, security, and so on, by deterring app store owners from saying "no" in close cases. Here, as in the context of AICOA, it may be helpful to have "Russian Hacker Maps" in mind: likely rebranded "USA Trusty Maps" and owned by an intermediate holding company. By deterring app stores from saying no in a case like this one, Congress would expose consumers to an increased risk that Russian Hacker Maps would get onto Americans' phones and other devices.

Second, the provision seems to stop an app store owner from *correctly and desirably* factoring in the known benefits of its own ownership and control of individual apps. The fact that the app store owner also owns and supplies an app—and therefore is uniquely able to guarantee its quality, security, compatibility, and future behavior—is often relevant to assessing whether a consumer will want the app. Indeed, many consumers actively prefer known brands like Google, Apple, and Microsoft, and rationally value the reputation for quality and trustworthiness that these brands have obtained. Likewise, the fact that the app store owner can guarantee the quality, security, compatibility, or future behavior (including software patches and updates) of its own apps *is also* relevant to assessing whether those apps will be desirable for consumers. Ruling this out as a consideration makes no sense.

Recall that, as with self-preferencing more generally, manipulation of search results will not be in the interests of a covered platform in many cases. An app store that promotes worse own-brand apps ahead of better third-party apps will tend to drive *both* consumers and app developers to other app stores, because consumers will be less satisfied, and developers will earn less

Third, this provision will generate tremendous uncertainty and extended litigation. The concept of "unreasonable" self-preferencing remains essentially undefined, other than the two specifically treated examples. I see no alternative to endless uncertainty and abundant litigation over the extent to which self-preferencing might be "unreasonable." This process seems likely to add a ton of cost into app development and app store operation, for uncertain benefit.

6. An Equal-Access Obligation for Apps Will Harm Consumers

Section 3(f) requires a covered company to "provide access to operating system interfaces, development information, and hardware and software features to developers on a timely basis and

on terms that are equivalent or functionally equivalent to the terms for access by similar apps or functions provided by the covered company or to its business partners."

This amounts to a forced-access obligation for all third party apps to the operating system, hardware features (like cameras, microphones, and GPS locators), and software features (which could include just about anything, including software features that reflect user data or implicate privacy and security). This seems extremely unwise, for all the reasons identified in the context of AICOA's similar provisions.

It invites the two central criticisms that I make of AICOA above, and which I will therefore repeat only briefly. First, it will discourage operating system owners that also operate an app store from introducing product improvements or feature innovations for their own apps that they would be unable or unwilling to share with the whole universe of third-party app developers (including developers that may offer low quality, malicious, or unstable apps).[123]

Second, it will also deter operating system owners that also operate an app store from refusing access to apps that appear dangerous to users (or simply objectionable), but where the operating system owner is not sure that it could, or wants to, go through the hassle of proving the defense.[124] Thus, on a very important margin, it will incentivize operating system owners to protect their users less than they otherwise would. That seems dangerous and undesirable.

7. The User Security Defense is Too Narrow

Section 4(a)(1) creates an affirmative defense for conduct that is "necessary to achieve user privacy, security, or digital safety," undertaken "to prevent spam or fraud," "necessary to prevent

[123] *See supra* § II.C.1.

[124] *See supra* § II.C.2.

unlawful infringement of preexisting intellectual property," or "taken to prevent a violation of, or comply with, Federal or State law." And Section 7(b) sets the conditions for the application of the defense. It provides that, to benefit from the defense in Section 7(a), a covered company must establish by a preponderance of the evidence that it is applied consistently to apps of the covered company and other apps (*i.e.*, that the measure in question is not applied in such a way as to favor the company's own apps); is not "used as a pretext to exclude, or impose unnecessary or discriminatory terms on, third party apps, in-app payment systems, or app stores"; and is "narrowly tailored and could not be achieved through a less discriminatory and technically possible means."

Of course, it is much better to have such a provision than not to do so. But in its current form this defense is not sufficient to protect consumers for several reasons.

First, the defense omits several grounds on which an app store should probably be able to deny carriage or equal treatment. For example, it does not appear to protect a covered company that declines to give equal treatment to an app characterized by:

- objectionable content (*e.g.*, sexually explicit content, including in products, services, or apps aimed at or marketed to children; promotion of terrorism; promotion of violence or criminality);
- inaccurate, false, or outdated information;
- poor quality service;
- a threat of consumer confusion;
- a threat to the security or integrity of the platform itself (if security means "user" security, as the context and Section subtitle suggest);

- a threat to the security of other app developers (rather than users) (if security means "user" security, as the context and Section subtitle suggest);
- a threat that equal treatment would result in data, access, or interoperability being provided to the government of a foreign adversary (unless the relevant entity is specifically blacklisted or watchlisted by the federal government pursuant to Section 7(6));
- unusual technological, commercial, or other difficulties or costs of integration; or
- lack of information regarding a possible concern (*e.g.*, the ultimate ownership and control of an app, or the way in which an app will use data).

Second, it imposes an unduly restrictive "less discriminatory alternative" test. Rather than asking whether a particular practice was reasonably tailored to one of the enumerated legitimate purposes, it asks whether the measure was narrowly tailored such that it "*could not be achieved* through *less discriminatory* and *technically possible* means." (Emphasis added.) This seems to be a very onerous condition that threatens to make the defenses little or no use in many real cases. If there is *any* "technically possible" alternative that the app store "could" use—regardless of whether a rational app store would in fact use it as an alternative to the challenged practice, or even whether it would be reasonable to do so—then the defense fails and the platform is on the hook.

Third, it creates, but does not define, a "pretext" exception. If the conditions for an appropriate denial of service or carriage are present, it should not matter what the subjective thoughts of the covered company's employees might have been. To put it concretely: users should not be exposed to Russian Hacker Maps simply because, in denying it access under circumstances that create a reasonable threat to platform security or user privacy, the relevant employee had had

some subjective occurrent thoughts about competition. Like practices in like circumstances should not be treated differently because of different subjective thoughts.

Accordingly, it would be much better and simpler to provide that a measure that was in fact reasonably related to a legitimate justification would be protected conduct regardless of whatever subjective thoughts anyone had had about anything.

Of course, this provision is the critical measure that allows app stores to protect consumers. Making it too narrow will risk serious harm. And, to the extent that this affirmative defense is eroded or narrowed, app stores will face stronger incentives to just allow risky apps and actors onto the platform—and onto consumers' devices and into their homes.

8. OAMA Should Be Limited to Government Enforcement

Section 5(a)(1) provides for federal and state government enforcement. If Congress enacts a version of OAMA, I support limiting enforcement to federal and state government enforcement. (I note that the FTC enforcement provision presents the question of whether the FTC may enforce OAMA through rulemaking. Congress may wish to address this question explicitly.)

But Section 5(b) allows developers to sue covered companies for violations of OAMA, including for treble damages and attorney fees, plus prejudgment interest at the election of the court, plus injunctive relief under regular conditions.

I do not recommend empowering developers to bring or threaten treble-damages litigation under OAMA—and certainly not at first. In the hands of the federal government, an appropriately tailored version of OAMA could be enforced and applied in a manner consistent with the public interest. In the hands of all conceivable app developers—and potential *classes* of app developers

under Federal Rule of Civil Procedure 23—OAMA would be a weapon for threatening app stores with endless and expensive litigation. This would turbocharge concerns that app stores will face incentives to let close cases through the door, with the result that consumers will be exposed to more bad-quality, high-risk, or otherwise undesirable apps.

9. The National Security Exception is Too Narrow

Section 7(6) explains that nothing in OAMA should be construed to "require a covered company to interoperate or share data with persons or business users that" either "are on any list maintained by the Federal Government by which entities are identified as limited or prohibited from engaging in economic transactions as part of United States sanctions or export control regimes," or "have been identified by the Federal Government as national security, intelligence, or law enforcement risks."

I take this provision to be an effort to ensure that OAMA does not end up requiring covered app stores to carry, supply, promote, interoperate with, or otherwise support apps that pose a national security or other law enforcement threat.

But the problem is that the grounds are far too narrow. In order to benefit from this exception, a covered platform must be *knowingly dealing with an entity that has been specifically blacklisted or watchlisted by the federal government*! This is a desperately high bar that will apply to a vanishingly small number of cases.

The entities of ultimate concern here include a fairly broad array of hostile foreign governments and quasi-state actors, as well as hostile, criminal, and malicious private actors. Of equal concern are entities that may be owned, controlled, influenced by, or vulnerable to, such actors. Critically: *such ownership, control, influence, or vulnerability will not always be clear.* If

a covered company must justify any denial following lengthy and expensive litigation discharge a burden of proof, then it is less likely to deny access in the first place.

To do real work, I think this provision would need to immunize action taken by a covered platform if was reasonably related to a legitimate justification, such as protection against threats to users, businesses, the app store, or the platform. This includes malicious and hostile actors of all kinds as well as those owned, controlled, influenced by, or vulnerable to, such actors. Any action reasonably related to protection against such risks should probably be permitted. The point would be to avoid deterring covered companies from taking protective measures.

IV. A ROADMAP FOR PROMOTING COMPETITION

I understand that there is bipartisan commitment to supporting antitrust enforcement. In case it is useful to the Subcommittee, in this Part I briefly outline a four-part roadmap to doing so while avoiding the risks and concerns associated with AICOA or OAMA.[125]

A. Fully Fund Federal Enforcement

The best way to protect competition in digital markets is to ensure that digital monopolists must compete on the merits, and that unlawful transactions and practices are promptly detected and prohibited. This means, above all else, fully funding antitrust enforcement. In fact, the *most* urgent need in antitrust enforcement today—more urgent than substantive law reform, and much easier to design—is a serious infusion of resources to the agencies. The FTC Bureau of Competition and DOJ Antitrust Division have been heavily outgunned for a long time by the scale of the challenges they face.

[125] This Part draws on and incorporates material from my February 2022 testimony before the Subcommittee.

The FTC's website demonstrates the soaring workload of the agencies and the desperate imbalance between work and resources. In fiscal year 1979, there were 814 HSR filings,[126] while in fiscal year 2021 there were 3,520 HSR filings: more than four times as many.[127] But the staffing of the agency has not just failed to keep pace: shockingly, it has *declined*. In fiscal year 1979, the agency's FTE utilization was 1,746, while by fiscal year 2021, it had fallen to 1,123: a loss of more than 35%.[128] Similarly, in September 2022 testimony before this Subcommittee, AAG Jonathan Kanter indicated that "the Antitrust Division ended [fiscal year 2021] with 352 fewer employees than in 1979."[129]

In addition to the urgent need for staff, the agencies need money for experts, without whom antitrust cases against sophisticated businesses often cannot be won. For example, a recent successful hospital merger litigation—of the kind that may appear, from afar, relatively straightforward when compared to novel cases in tech markets—involved no fewer than *seven* testifying experts, with the defendants retaining five to the FTC's two.[130] (The FTC won in the trial court and prevailed on appeal.[131]) If this is the expert need for a hospital merger—a type of case in which the FTC has decades of world-leading experience and expertise—it is easy to see how enforcement targeted at novel practices in novel markets, including tech markets affecting news, urgently need serious financial backing.

---

[126] FTC, *Third Annual Report to Congress Pursuant to Section 201 of the Hart-Scott-Rodino Antitrust Improvements Act of 1976*, https://www.ftc.gov/system/files/documents/reports/3rd-report-fy-1979/3annrpt1979.pdf/, 4.

[127] FTC & U.S. Dept. of Justice, *Hart-Scott-Rodino Annual Report Fiscal Year 2021*, https://www.ftc.gov/system/files/ftc_gov/pdf/p110014fy2021hsrannualreport.pdf, 2.

[128] https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

[129] U.S. Department of Justice, Press Release, Assistant Attorney General Jonathan Kanter of the Antitrust Division Testifies Before the Senate Judiciary Committee Hearing on Competition Policy, Antitrust, and Consumer Rights (Sept. 20, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-testifies-senate-judiciary.

[130] *FTC v. Hackensack Meridian Health, Inc.*, Case No. 20-18140, 2021 WL 4145062, at *1–2 (D.N.J. filed Aug. 4, 2021).

[131] FTC v. Hackensack Meridian Health, Inc., 30 F.4th 160, 164 (3d Cir. 2022).

The recent funding increase for DOJ and the FTC is a terrific development and a great start. The FTC's budget for fiscal year 2023 contemplates a staffing increase to 1,440 FTE and $490 million: an increase of 300 FTE and $139 million over fiscal year 2022. This is a step forward for free and competitive markets!

But it is, unfortunately, just a start. Even with the increase, FTC expected staffing will stand in 2023 at just 82.5% of fiscal year 1979 staffing[132]—and, again, recall that HSR filings are now at more than *four times* their 1979 levels! And of course the work itself is harder and more expensive than it was in 1979: today, courts are more demanding of antitrust plaintiffs; fact discovery is more burdensome and expensive than it was in 1979, including because of the vast explosion in the creation and retention of documents and data; and expensive experts are a strict necessity for antitrust litigation.[133] As the FTC's most recent budget justification notes:

> It is commonplace for defendants in FTC litigations to outspend the Commission by a significant amount on expert support, which often results in FTC experts having to conduct more extensive—and thus more costly—rebuttal analyses. In recent years, the Commission's substantial litigation docket has generated *projected expert spending that far exceeds our available budgeted resources, sometimes by as much as [five] times,* potentially threatening the Commission's ability to challenge meritorious cases.[134]

There is plenty of bang available for the taxpayer's buck here. Fully funding federal enforcement would allow the agencies to cover their docket, including, for example:

---

[132] FTC, Fiscal Year 2023 Congressional Budget Justification, https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf, cover letter & 8.

[133] For a recent view from the litigation finance world, *see, e.g.*, Jason Levine, *The role of litigation finance in antitrust lawsuits* (Mar. 30, 2022), https://omnibridgeway.com/insights/blog/blog-posts/blog-details/global/2022/03/29/the-role-of-litigation-finance-in-antitrust-lawsuits ("The complexity and long duration of antitrust cases also make them inordinately expensive to litigate. . . . The prohibitive costs stem not only from the need for top-of-the-market counsel and expert witnesses, but also from the expense of motions practice and discovery that is comprehensive and hard-fought. Defendants frequently produce millions of documents, and the parties take dozens of depositions, even in single-plaintiff antitrust cases. This is particularly true when opt-out cases are consolidated with class actions for pretrial proceedings, as in multidistrict matters, and discovery is intermingled.").

[134] FTC, Fiscal Year 2023 Congressional Budget Justification, https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf, 13,

- **A fuller docket of healthcare provider transactions.** Hospital and physician-practice transactions, including serial roll-up acquisitions, acquisitions of dialysis clinics, that affect both urban and rural communities and threaten Americans' access to healthcare. The FTC's elite record in hospital merger challenges—one loss since the program was rebooted roughly twenty years ago—leaves it well positioned to extend its protection over transactions outside major metropolitan areas into under-served parts of the country, including rural markets for healthcare services. This is crucial work. For example, the recent work of Thomas Wollmann highlights the dangers of "stealth consolidation"—that is, non-reportable deals—in dialysis markets across the country.[135]
- **Anticompetitive conduct in healthcare markets.** The FTC's recent action against "Pharma Bro" Martin Shkreli demonstrates the dangers of monopolizing and otherwise anticompetitive practices in healthcare markets that affect American patients and families. That case involved practices that raised the price of a critical treatment for toxoplasmosis—a parasitic infection that presents a deadly threat to immunosuppressed and immunocompromised individuals, including HIV patients and transplant recipients—by a remarkable *4,000%*, while blocking the entry of rivals that would have been able to supply American families and bring prices down. The FTC filed suit in 2020 and won at trial in 2021, resulting in a resounding FTC victory and a full remedy that included disgorgement of illegally obtained

[135] *See* Thomas Wollmann, *How to Get Away With Merger, Stealth Consolidation and its Effects on U.S. Healthcare*, NBER Working Paper 27274 (rev. July 2021), https://faculty.chicagobooth.edu/~/media/faculty/Thomas-Wollmann/Research/how_to_get_away_nber_w27274_v2.pdf.

profits and a lifetime industry ban for Shkreli.[136] This victory was obtained by the same litigating unit at the FTC that achieved the pathbreaking *Actavis* victory that exposed "pay for delay" agreements between branded incumbents and generic entrants to full antitrust scrutiny.[137] Full funding would enable this vital work to cover more markets, analyze more practices, and ultimately protect more consumers, patients, and families.

- **Transactions affecting local markets, particularly in rural and under-served locations in states where state Attorneys-General are not equipped to protect competition.** Practices and transactions affecting rural and under-served communities across the United States, including transactions that threaten competition among supermarkets, other grocery and food suppliers, gas stations, and retail banks. A merger to monopoly in a local market is still an illegal merger to monopoly! But too often such transactions are too small to justify the attention of federal enforcers with scarce resources, or over-stretched State AGs. More funding would enable the federal enforcers to show the flag in local markets and rural or under-served communities, and make it clear that there are no "small market" exceptions to the Sherman Act.
- **Transactions or practices in complex markets, such as digital and platform markets.** The agencies have been criticized in recent years for failure to challenge certain transactions in digital markets, such as Facebook's acquisition of Instagram. But the reality is that digital antitrust cases are hard to prepare, hard to litigate, and

[136] FTC v. Shkreli, 581 F. Supp. 3d 579 (S.D.N.Y. 2022).

[137] FTC v. Actavis, Inc., 570 U.S. 136 (2013).

> hard to win. Traditional metrics like market shares and nominal prices may be controversial or entirely absent; the competitive effects of particular practices may be harder to prove with confidence; and the design and application of remedies may raise tremendous complexities. And any responsible antitrust agency will (and should!) consider, when deciding how to allocate enforcement resources like staff and dollars, the risk of litigation, and the opportunity costs of the case that the agency would not be able to bring as a result. As a result, effective digital antitrust means making sure that more traditional dockets—with clearer harms in simpler markets—are covered too. When the agencies can cover the clearest and strongest cases, the case for devoting resources to more complex matters becomes stronger.

B. Support State Enforcement

State Attorneys-General play a critical role in the nation's antitrust enforcement system, but—with a handful of exceptions—seldom have the expertise, staffing, or experience to litigate a significant antitrust case alone. Accordingly, Congress may wish to consider reinforcing the antitrust enforcement capacity of the State Attorneys-General, with a contribution of funding grants and/or technical assistance. State AGs are often the first line of defense for consumers as well as critical partners to federal enforcers, but—while many offices are leading and effective voices in antitrust enforcement—others lack sufficient funding and expertise to maintain a robust antitrust enforcement program. Federal support could help to change this.

C. Modernize Antitrust Doctrine

I support the careful revision of our core antitrust statutes to ensure that markets remain free and competitive, and to clarify Congress's intention that acts and practices that harm

competition—and thus harm consumers and workers—are unlawful. The bills introduced by Ranking Member Lee and Chair Klobuchar represent valuable achievements and helpful contributions to this conversation.[138]

Although a full description of possible revisions and improvements is beyond the scope of this testimony, some specific recommendations include the following:

- **Section 1 Sherman Act.** The 2018 decision of the Supreme Court in *Ohio v. American Express* imposed a burden on plaintiffs to not only prove evidence of competitive harm, such as a price increase, but also to affirmatively disprove claimed offsetting benefits. In doing so it unsettled an understanding, built on decades of previous precedent, that after a plaintiff has successfully proved harm, like a price increase, the burden passes to a defendant to prove offsetting benefits. This should be corrected. The *AmEx* Court also unsettled antitrust's basic rule that a market should be defined by reference to demand-side substitutability, and the result was to procure the immediate failure of at least one DOJ enforcement action in a manner that was universally condemned (and was saved only by the action of the UK's Competition and Markets Agency). This also should be corrected.
- **Section 2 Sherman Act.** The law of Section 2 has become notoriously vague and hostile to plaintiffs: including government plaintiffs with robust economic evidence in hand. While it should be hard for a plaintiff to win a monopolization case—antitrust should not be a bailout for unsuccessful competitors—it should not be

[138] Competition and Antitrust Law Enforcement Reform Act, S.R. 225, 117th Cong. (2021); Tougher Enforcement Against Monopolists Act, S.R. 2039, 117th Cong. (2021).

virtually impossible. The erosion of monopolization law invites abuses, leaves businesses and consumers uncertain of their rights, discourages agencies from enforcing the law, undermines the credibility of the antitrust project, and fuels calls for more radical interventions that may not serve consumers. At a minimum, Congress should clarify: the legal rules applicable to claimed justifications (in particular, that as under Section 1 the existence and sufficiency of a justification under Section 2 is a matter for a defendant to prove, not for a plaintiff to disprove); the absence of any "bad purpose" requirement, given antitrust's exclusive concern with actual and likely economic effects; and—if possible—the definition of monopolization's conduct element and its relationship to lawful competition.[139]

- **Section 7 Clayton Act.** Section 7 was intended as a shield against transactions that threatened competition. It was not intended to require a plaintiff to prove to a high level of certainty, or to quantify, the specific competitive effects that would flow from a challenged merger or acquisition. Indeed, Congress specifically amended the language of the provision during legislative deliberation: striking out a requirement that the effect of a transaction "will be" substantially to lessen competition and replacing it with a requirement that the effect "may be" of this kind—*specifically* in order to provide stronger protection against dangerous deals. But the courts have lost track of Congress's intention here: forcefully restating it would help to sharpen antitrust on an important margin.

[139] For my own view, *see* Daniel Francis, *Making Sense of Monopolization*, 84 Antitrust L.J. 779 (2022).

- **Hart-Scott-Rodino Act.** The HSR Act is the foundation for merger review in the United States. It currently grants the agencies a default initial period of 30 days to review and analyze a transaction.[140] If a deal raises sufficient concerns, the agency may issue a "Second Request" for further detailed information. Once the merging parties substantially comply with that request, the agency is back on another 30-day clock. The problem is that this often leaves too short a time to review the vast amount of information included in a Second Request, to engage fully with other market participants like customers and competitors, and to analyze claimed efficiencies and possible remedies. But all of these are necessary for accurate enforcement: that is, to challenge illegal deals and to stay out of the way of those that are not illegal.

  In practice, the agencies bargain with merging parties for additional time, trading away the opportunity to receive documents or information on particular issues or from particular custodians in order to get enough time to make a sensible decision. But this is not a happy circumstance. Kneejerk timelines force agencies into premature litigate-or-leave decisions that do not promote sound enforcement, free and competitive markets, or the interests of businesses—including merging parties as well as their competitors and trading partners. Granting significant additional time after substantial compliance with a second request—changing the 30 days to, say, 90 or even 120 days—would ensure that agencies are not stuck without the time they need for a real investigation. It would also affect only a tiny fraction of

[140] *See* 15 U.S.C. § 18a.

deals, corresponding to the most competitively troubling transactions. indeed, just 1.9% of merger filings attracted a Second Request in fiscal year 2021, with the number usually hovering somewhere around 3%.[141] And, of course, only the largest deals are HSR-reportable in the first place.

I would probably pair this change with a direction to the agencies to resume the practice of Early Termination of the HSR waiting period for deals that obviously raise no competitive concerns.[142] There is no good reason to force companies to wait a month to close their deal *after* the agencies have determined that they will not investigate further: that seem to be a pure tax on mergers and should end.

D. Targeted Platform Regulation

Although I have been generally opposed to the measures under discussion, I would support careful, market-specific regulatory intervention in specific markets where competitive concerns supported such measures. These would be targeted to specific markets and to market or monopoly power tests, not bigness criteria or to specific companies. This could include:

- **Transparency and disclosure obligations in ad tech markets.** A common concern in advertising markets is that the operation of many tools and auctions is opaque to market participants, creating opportunities for manipulation, abuse, and lost competition. I would not oppose market-specific transparency and disclosure obligations (particularly for

[141] FTC & U.S. Dept. of Justice, Hart-Scott-Rodino Annual Report Fiscal Year 2021, https://www.ftc.gov/system/files/ftc_gov/pdf/p110014fy2021hsrannualreport.pdf.

[142] FTC, Press Release, FTC, DOJ Temporarily Suspend Discretionary Practice of Early Termination (Feb. 4, 2021).

entities with significant market or monopoly power) that helped publishers, advertisers, and others in the ad tech chain make informed choices among alternatives.

- **Consumer transparency obligations, especially related to advertising.** The core of some concerns about practices like search ranking manipulation is that consumers may falsely believe that they are being given a "neutral" search ranking. To the extent that this is true, and particularly for businesses with significant market or monopoly power, I would support a mandatory disclosure (*e.g.*, "Advertising") when a search ranking is in whole or part the result of paid advertising, to help consumers make informed choices. I would also not oppose a short, ordinary-language mandatory disclosure in appropriate cases to make clear that search rankings may reflect commercial interests (*e.g.*, "Search rankings may reflect a wide variety of factors, including our business interests.").
- **Market-specific ban on MFNs.** As I indicate above in my comments on OAMA, I am not opposed to a ban on the use of most-favored-nation ("MFN") clauses by entities with significant market or monopoly power *in specific markets* in which there are grounds to think that the harms of such commitments may outweigh any benefits.
- **Market-specific interoperability or portability requirements.** I am also not opposed to the introduction of certain interoperability or portability requirements *in specific markets* in which there are grounds to think that such measures would generate real benefits without unduly harming competition or users.[143] Targeting specific markets ensures that the

[143] The costs and benefits of interoperability requirements are the subject of a rich literature. In brief, they can allow smaller competitors and entrants to grow despite the presence of large incumbents; but they can also stifle incentives to invest (because benefits are shared more fully with rivals), may reduce security, and deter innovations and improvements that are incompatible with the interoperability requirements. *See, e.g.*, Herbert Hovenkamp, *Antitrust Interoperability Remedies*, Colum. L. Rev. Forum 1 (2023); Fiona Scott Morton & Michael Kades, *Interoperability as a Competition Remedy for Digital Networks*, https://ssrn.com/abstract=3808372; Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf.

measure is feasible and in the interests of consumers; it also ensures that legislators and any involved agencies can plausibly formulate sensible principles and think seriously about concerns (*e.g.*, that an interoperability standard may hold up innovation or change, or soften competition rather than sharpening it). Any such requirements must provide really robust protection for security, quality, and privacy: probably in the form of a blanket rule that measures reasonably related to the protection of users, business users, or the platform are lawful.

V. CONCLUSION

In sum, although I do not support AICOA and OAMA because I fear they would do more harm than good, I would warmly welcome robust action to support vigorous antitrust enforcement, the modernization of our antitrust laws, and some targeted platform regulations. I would also be supportive of a narrower version of OAMA.

I am grateful for the opportunity to testify before the Subcommittee. I would of course be happy to assist Congress further at any time.