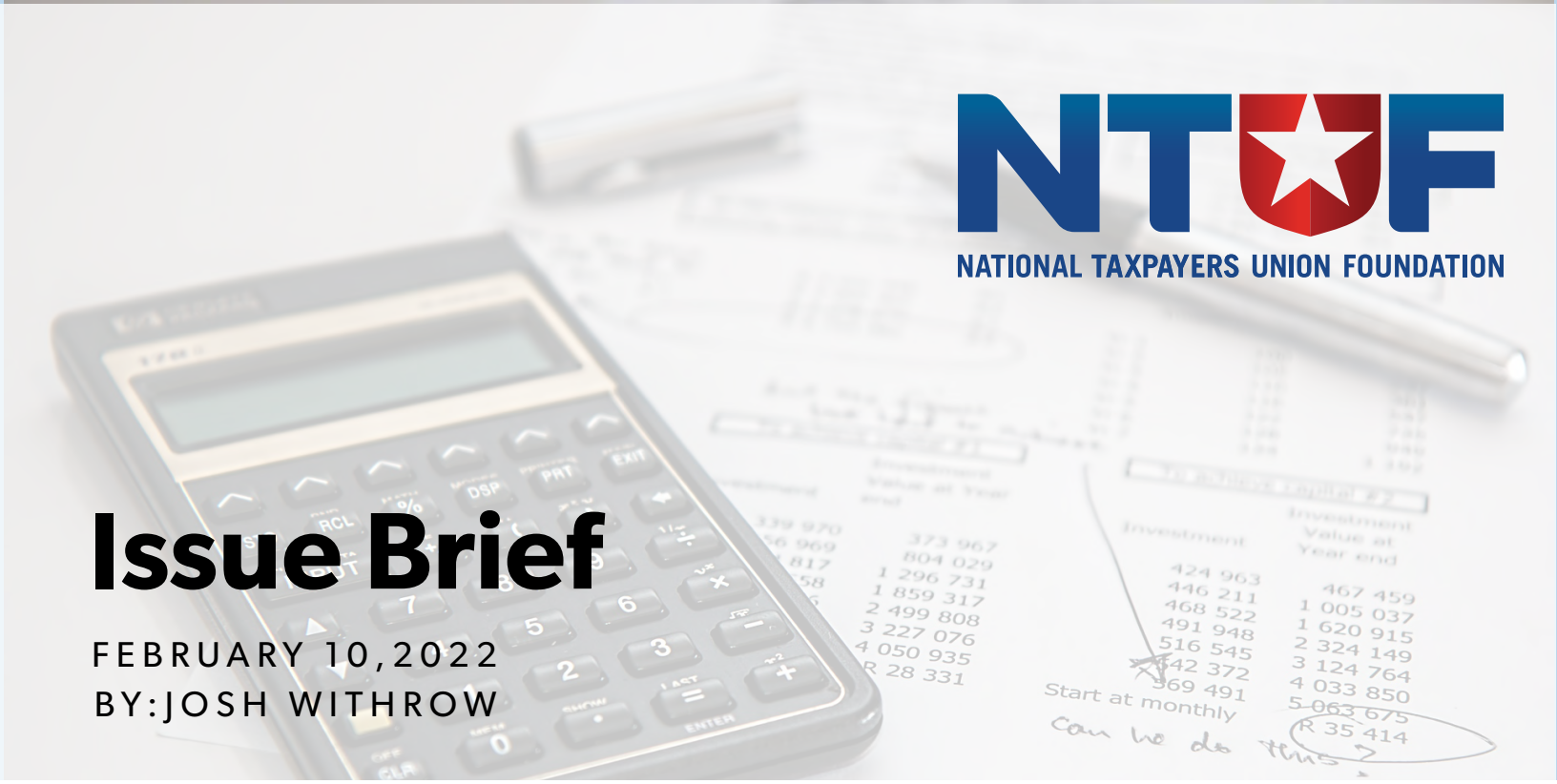

NATIONAL TAXPAYERS UNION FOUNDATION

Issue Brief

FEBRUARY 10, 2022

BY: JOSH WITHROW

Ham-Handed Interoperability Mandates for Big Tech Will Harm Consumers

One of the common themes among several of the bills moving through Congress that target "Big Tech" is the requirement that they make their products and platforms — especially the data generated by users of those platforms — more interoperable with, and more accessible to, their rivals. Interoperability as a concept has some value, and certainly might benefit competition in online markets in some respects. However, government-mandated interoperability would likely create a host of unintended consequences, especially if done overly broadly.

Of the half dozen or so major antitrust reforms aimed specifically at Big Tech firms that have passed through House and Senate committees this year, three have interoperability mandates at their core: the ACCESS Act (H.R. 3849), the American Innovation and Choice Online Act (AICOA, S. 2992, and its similarly-named House variant, H.R. 3816), and the Open App Markets Act (OAMA, S. 2710). Each of these bills is targeted at "covered platforms," which are defined at a number of users and market cap size that, for the time being, would affect just a handful of companies — Google, Amazon, Facebook (now Meta), Apple and perhaps Microsoft (often collectively referred to as GAFAM).

Interoperability often arises somewhat organically as a result of industries finding it beneficial to seek optimal, common standards to build upon, like common screw sizes, computer ports, or software interfaces. The protocols upon which the internet is built, such as

Key Facts:

Interoperability within an industry is frequently desirable, but is not automatically beneficial, nor a cure for competition in digital markets.

Mandated interoperability, as proposed in current legislation targeting Big Tech, is likely to have major negative consequences for consumers.

One-sided mandates for Big Tech may endanger privacy and security, invite rent-seeking, and undermine U.S. leadership in tech.

TCP/IP and HTTPS, are a good example of the benefits of interoperable systems that have allowed millions of people on widely varied devices all to connect with one another.

The concern raised by proponents of interoperability mandates is that these largest online platforms have attained their immense wealth by figuring out how to monetize, and to some extent to "silo," their users' data away in order to prevent their smaller competitors from accessing it. Therefore, as the logic goes, enabling competitive digital markets requires forcing the doors open to the silos, or at least allowing competitors to tap into them too.

It's not at all clear, however, that forced interoperability is a panacea for the perceived lack of competition to these large firms which currently define the digital market.[1] But even if one accepts that the benefits of forced interoperability justify government intervention, the legislation currently before Congress is clumsily designed and certain to lead to a host of unintended consequences that would likely outweigh the benefits.

Data Integrity

In the case of the social media platforms affected by these bills (primarily Facebook/Instagram and YouTube), the interoperability being sought would theoretically be achieved primarily by requiring that large platforms provide the means to make the data they collect and store more easily transferable to an app, software, or platform developed by another company. For example, the ACCESS Act would require social media platforms to open up their application programming interfaces (APIs) so rival platforms can build tools to allow users to quickly transfer their profiles and posts to another competing platform. It also requires any competing (or "potentially" competing) businesses to be allowed access to other datasets generated by these large "covered platforms," such as from app stores.

The first and most obvious problem raised by interoperability mandates for social platforms has to do with data privacy and security. If the "covered platforms" are, for example, required to make users' data more easily transferable to rival platforms, a huge number of questions are raised about what constitutes ownership of that data. Is a photo posted by a friend that you are tagged in "yours" to transfer, and vice-versa? What about all the comments your friends made on your posts, which they might not want distributed on a new platform that is perhaps less private?

In the case of data security, is a covered platform still required to make its APIs available to companies which don't have adequate safeguards in place to protect that data? Who is liable if the third party accessing the data uses or shares it inappropriately? As tech law scholar Mikołaj Barczentewicz writes, "It does not require much imagination to see how, without adequate safeguards, mandating this kind of information exchange would inevitably result in something akin to the 2018 Cambridge Analytica data scandal."[2]

In the case of the ACCESS Act, all of these questions and more are left in vague terms for the Federal Trade Commission (FTC) to settle, down to the very legal definition of what constitutes "data."[3] In the case of the Open App Markets Act, companies are allowed to avoid the interoperability mandate only if they clear the high legal standard of "clear and convincing evidence" that their privacy or security concerns are legitimate.

Ultimately, the solution to many of these problems would be for Congress to pass a federal data privacy and security framework that would clear up questions about what kinds of user-generated data can and cannot be shared without user consent and who is responsible if it is misused or compromised. It would be irresponsible to enact any broad interoperability mandate without such a framework in place. In the meantime, these private companies have already been taking huge steps on their own to facilitate data portability between users on different platforms.[4]

[1] Sam Bowman, "Mandatory Interoperability Is Not a 'Super Tool' for Platform Competition," Truth on the Market blog, Nov. 29, 2021. https://truthonthemarket.com/2021/11/29/mandatory-interoperability-is-not-a-super-tool-for-platform-competition/
[2] Mikolaj Barczentewicz, "Privacy and Security Risks of Interoperability and Sideloading Mandates," Truth on the Market blog, Jan. 26, 2022. https://truthonthemarket.com/2022/01/26/privacy-and-security-risks-of-interoperability-and-sideloading-mandates/
[3] Josh Withrow, "The Flawed ACCESS Act Creates More Problems than It Solves," NTU Foundation, June 22, 2021. https://www.ntu.org/foundation/detail/the-flawed-access-act-creates-more-problems-than-it-solves
[4] See the Data Transfer Project, accessed Jan. 27, 2022. https://datatransferproject.dev/

Product Safety and Security

Many of the controls that app stores exercise over developer access to their services help keep security vulnerabilities and malicious apps to a minimum, a benefit which is threatened by these overly broad interoperability mandates. For example, AICOA's interoperability requirement would force any rival app to have full access and interoperability with basically anything that Google or Apple's own products can access on their software or devices. For them to be able to deny access on the basis of security or users' data privacy, the platform operators are held to an incredibly high standard, in effect encouraging them to err on the side of access over security.[5]

The OAMA particularly focuses on mandating that app stores not bar third-party apps from using competing payment systems (both the Apple and Google Play stores require in-app payments to run through them), and that users be allowed to "sideload" apps and app stores (which, of the targeted platforms, only Apple does not allow).[6] Forcing all apps that take payments to funnel through the platform's in-house payment system is the key revenue source for the platform owners, but it is also a security and convenience benefit for its customers. Knowing that their payments are secure and that transaction disputes will be handled by the app store owners themselves is another way that consumers know they can trust what they download.

Trust in the app stores — and trust that the apps will work with the phone's operating system and not compromise the user's phone or data — is also a key to the success of new apps by smaller developers.[7] This is one reason that many smaller app developers have been resistant to these interoperability requirements — reduced trust in the overall app store ecosystem is likely to lead consumers to be more hesitant to try newer apps over more established ones.[8]

Both Google and Apple screen the apps that are allowed into their app stores for malware, spyware, and poor design that might lead to security vulnerabilities, but it remains true that Android users are more exposed to malware than iPhone users (though that gap is shrinking).[9] Apple has staked much of its brand on seamless integration and secure products, and one of the tradeoffs is that users have less control over how they can modify their devices. The question is why the government needs to foreclose the option of making this tradeoff, when consumers have competing products to choose from.

Cui Bono?

Unfortunately, the nature of a government mandate that allows competitors to demand interoperability with the covered platforms inevitably creates a golden opportunity for rent-seeking rivals, particularly when the targeted companies are saddled with having to affirmatively prove that they are not acting anti-competitively. It's not a coincidence that many of the biggest supporters of all of these bills are some of GAFAM's next biggest rivals, who stand to benefit greatly from being able to force a level of interoperability that they are not obliged to provide to others in turn.[10]

The same rent-seeking impulses that will motivate domestic rivals will also apply to foreign rivals. Especially in the context of these bills that specifically target the largest four or five U.S. tech giants, an interoperability mandate provides an easy way for foreign competitors to siphon data from the covered platforms while not having to reciprocate in any way. Even some of the Senators who voted AICOA out of committee in January

---

[5] AICOA's requirement is that any exception to interoperability be "narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary" to prevent various specific harms. For more on why this is an impossibly high legal standard, see: Berin Szoka and Ari Cohn, Letter to Senate Judiciary Committee, Re: Markup of S. 2710, The Open App Markets Act (February 3, 2022). Published online by TechFreedom, accessed Feb. 6, 2022. https://techfreedom.org/wp-content/uploads/2022/02/Letter-re-S.2710-Affirmative-Defenses-2.2.22.pdf

[6] "Sideloading" refers to the practice of downloading and installing apps from outside the default app stores provided by the makers of the device's operating system.

[7] "How Government Restrictions on Platform Privacy Measures Could Harm Small App Developers," ACT, the App Association, Jan. 2022. https://actonline.org/wp-content/uploads/Antitrust-and-Privacy-Whitepaper-01062022.pdf

[8] Developers Alliance Staff, "What Does U.S. Senate Bill 2992 Mean for Software Developers and the App Economy?" The Developers' Alliance, accessed 3 Feb., 2022. https://www.developersalliance.org/news/what-does-us-senate-bill-s2992-mean-for-software-developers-and-the-app-economy

[9] Randal C. Picker, "Security Competition and App Stores," *Concurrentialiste: Journal of Antitrust Law*, Aug. 23, 2021. https://leconcurrentialiste.com/picker-app-stores/

[10] Thomas A. Lambert, "What's Behind the War on Big Tech?" *Regulation*, Fall 2021. https://www.cato.org/regulation/fall-2021/whats-behind-war-big-tech#

acknowledged that they held concerns about the bill's interoperability requirements and the potential cybersecurity and data privacy threats it might create for the covered platforms.[11]

There would be indirect consequences as well, as the U.S. companies which are subject to the interoperability requirements would be hampered in their ability to keep up with innovation compared to their competitors, foreign and domestic. Contrary to the narrative that the GAFAM firms are "monopolies" whose dominance is stifling innovation, the need to keep ahead of their competition has driven them to be among the world's largest private investors in cutting edge tech R&D.[12] Revenue that is lost to compliance with these new interoperability mandates and to fending off the new antitrust complaints and litigation will all take away from what these firms can use to research new products and technologies.

Conclusion

To the extent that generic interoperability mandates targeted at these selected Big Tech companies "level the playing field," for competitors, they do so with little regard for outcomes for consumers. In specific cases where a lack of interoperability can be found to be truly anticompetitive in a way that harms consumer welfare, that can be litigated via existing antitrust law. Instead, the sweeping interoperability requirements that are under consideration in Congress today, though, threaten to break many of the products and services that led consumers to make these U.S. companies the largest and most successful in the world.

The key question that should inform competition policy is whether there are legitimate reasons that companies might choose to restrict interoperability, and in this case there are many.[13] Among others, these include data security and privacy, standardization of user experience, and curation of a given audience and environment on the platform. The benefits of these choices often cannot be measured in terms of competition or even in prices, but in consumer satisfaction, which raises serious questions about whether it is appropriate for government regulators to preempt market choices in these environments.

About the Author

Josh Withrow is the Director of Technology Policy for National Taxpayers Union Foundation.

[11] "Senators Sound the Alarm on the Privacy, Security, and Global Competitiveness Problems in Sen. Klobuchar's Antitrust Bill," CCIA's Springboard blog, accessed Feb. 4, 2022. https://springboardccia.com/2022/01/25/senators-sound-the-alarm-on-the-privacy-security-and-global-competitiveness-problems-in-sen-klobuchars-anti-tech-bill/
[12] Christo Petrov, "Top R&D Spenders," SpendMeNot.com, updated Oct. 15, 2021. https://spendmenot.com/blog/top-rd-spenders/
[13] Bowman, ibid.

NATIONAL TAXPAYERS UNION FOUNDATION

2022 National Taxpayers Union Foundation
122 C Street NW, Suite 650, Washington, DC 20001
ntuf@ntu.org