ACT | The App Association

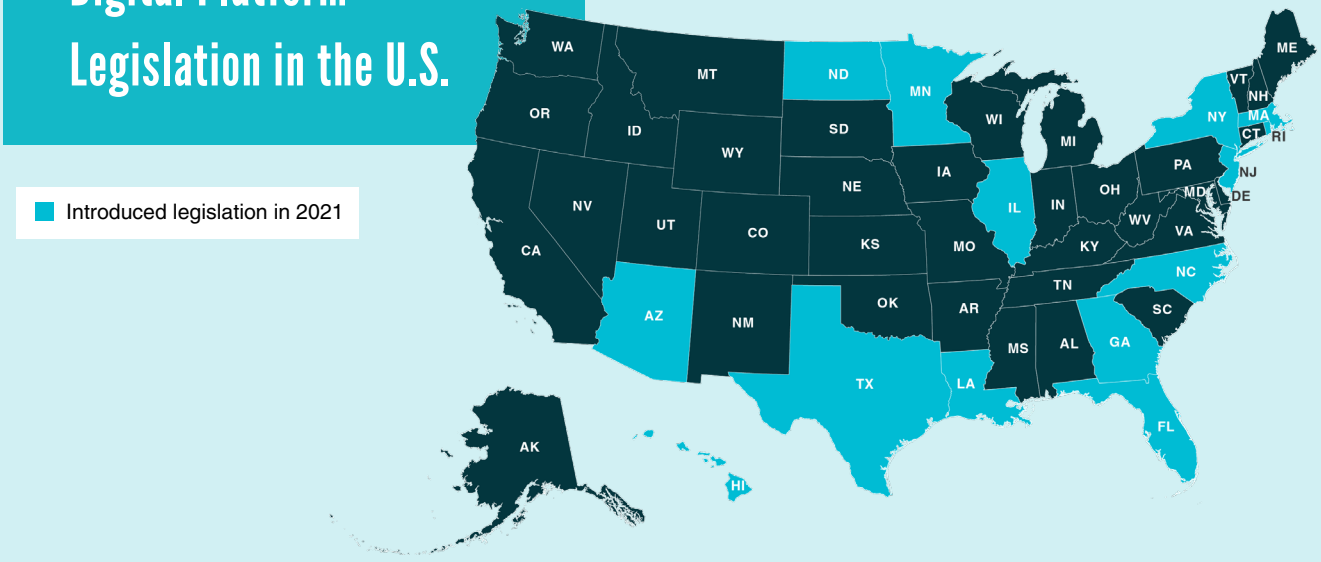
How Government Restrictions on Platform Privacy Measures Could Harm Small App Developers

JANUARY 2022

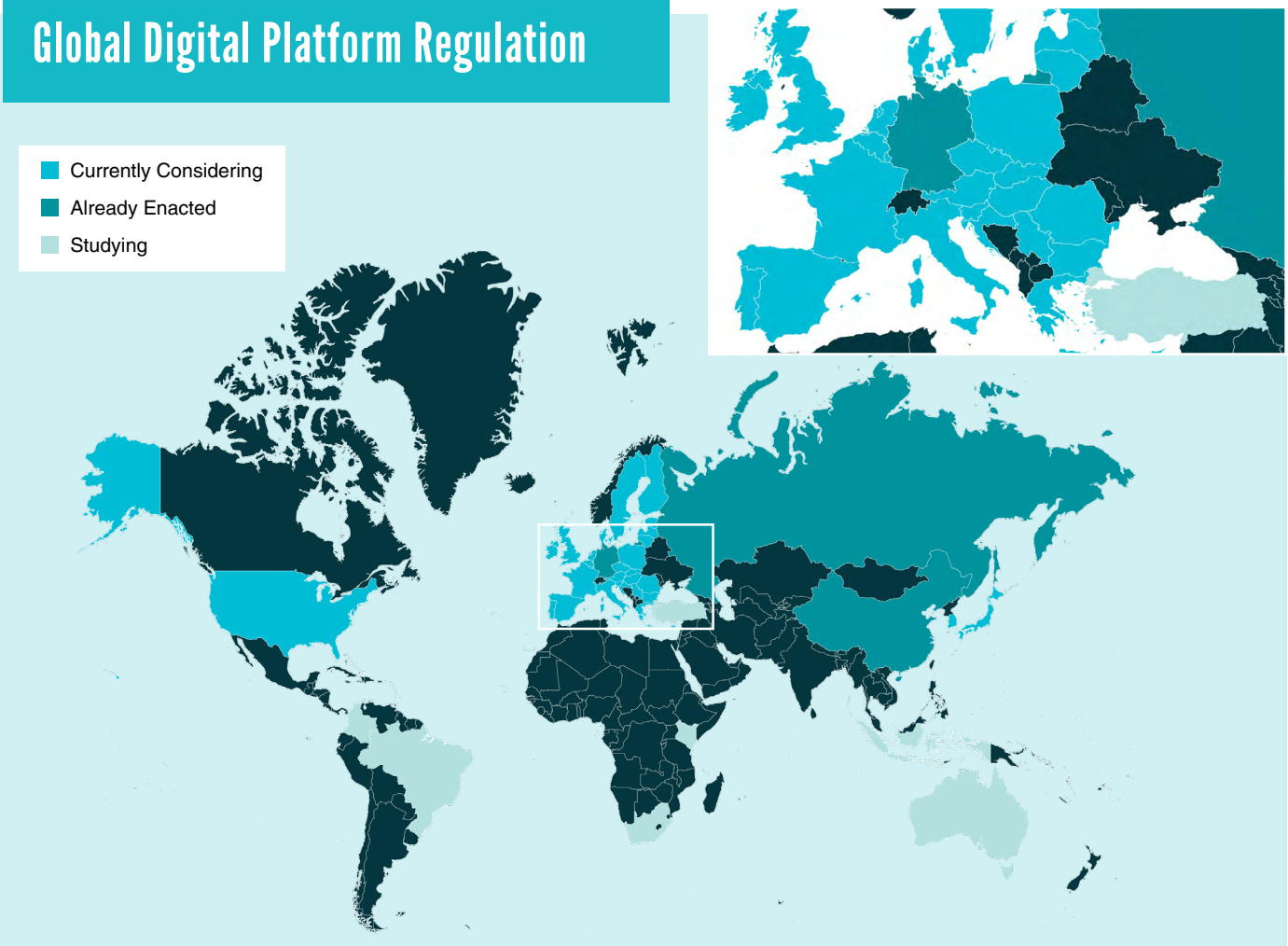
ACT | The App Association
1401 K Street NW Suite 501 Washington, DC 20005
202.331.2130 | ACTonline.org

@ACTonline /ACTonline.org

Digital Platform Legislation in the U.S.



Global Digital Platform Regulation



Source - United Nations Conference on Trade and Development, 'Competition law, policy and regulation in the digital era', July 2021.

Executive Summary

- Some of the new platform competition proposals considered by Congress and in the states would require app platforms to make compromises when it comes to the privacy and security of their ecosystems in the name of competition. Many of these proposals would undermine overall trust in app stores, as well as in our member companies. Legislators and regulators need to take account of how such proposals stand to disrupt the secure app ecosystem and negatively affect the same small business competitors they seek to empower.
- Small app developers benefit mightily from the investments of the large app platforms on privacy and security features, such as Apple's App Tracking Transparency, privacy labeling, just-in-time notifications, encryption, and more, some of which could be eliminated or curtailed by the competition proposals. Congress should avoid forbidding these tools while key congressional committees investigate fresh waves of digital privacy harms, and as consumers increasingly rely on platform privacy features to protect themselves and their children from those abuses.
- Blanket non-discrimination mandates and line of business restrictions that prevent the vetting and removing of apps that violate app store guidelines—or that require platforms to allow sideloading of software to circumvent the app platform review process altogether—harms App Association members who play by the rules. These mandates would also undermine user trust in apps writ large, resulting in a scenario where consumers are most likely to download apps made by established companies with brand name recognition only—in other words, big companies with a long history on the app platforms or the market more broadly.
- Open interoperability mandates would mandate "access by design" instead of "privacy by design," opening the floodgates to data access by both legitimate and questionable firms. Considering Congress has yet to pass a baseline comprehensive privacy law, we do not believe the appropriate protections to support such a regime are yet in place.

Introduction

The conversation surrounding internet privacy, especially as it relates to major technology platforms in the United States, has evolved substantially in the three years following the Cambridge Analytica data-sharing scandal that demonstrated just how easily, and quickly, massive societal disruptions can follow from poor data governance. Calls for a comprehensive privacy law are now standard practice among both Democrats and Republicans in Congress, albeit as both sides bemoan the slow progress towards compromise.[1] At the state level, two legislatures managed to enact their own comprehensive laws this year (Virginia and Colorado, joining California), with more than half of all states considering proposals in 2021.[2] Privacy nutrition labels are suddenly in vogue after years of research isolated to academia, while large platforms increasingly compete on privacy-enhancing technologies that shut off key spigots that fill the surveillance advertising marketplace with intimate user data.[3]

In fact, in many ways, the conversation around large technology platforms has grown beyond privacy, moving into concerns around those platforms' size and possible market dominance. Earlier this year, the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law (House Judiciary Antitrust Subcommittee) concluded a massive, multi-year investigation into several internet platforms, culminating in the introduction of a package of six bills intended to rectify the perceived wrongs identified in the report.[4] Meanwhile, legislators at the state level are showing increasing interest in the topic, with the introduction of handful of bills in several states that tackle various aspects of internet platform regulation, ranging from restrictions on app store marketplaces to constraints on certain social media content moderation practices to general reforms to state antitrust statutes. Legislators and regulators in jurisdictions around the world are also stepping in, including in the U.K., EU, India, China and elsewhere, with new proposals intended to increase competition in markets led, and sometimes dominated, by large tech platforms.

While the motivation and particulars of such proposals vary widely, a key component of many are blanket non-discrimination[5] and line of business restrictions[6] that affect platforms' ability to police their ecosystems. Other proposals require greater data portability, interoperability, and access for the third-party companies that both rely on the large platforms to reach customers in the greater marketplace, and which, in some cases, directly compete with those same platforms.[7] That is, platform antitrust proposals often delve into the realm of privacy, introducing a new front in the battle over the treatment of consumer data.

Recent platform antitrust proposals are of key interest to ACT | The App Association (App Association) member companies, many of which currently enjoy the benefits of platform-level privacy protections offered through software distribution platforms, such as app stores. App Association member companies set out to create the software that brings smart devices to life. They also make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

App Association member companies maintain, in many ways, complicated relationships with the largest app stores, Apple's App Store and Google Play, in particular. On the one hand, App Association member companies believe the platforms can do better in many areas to accommodate the small software developer

segment of the market. Small app developers expend enormous amounts of time and effort honing their products, so it is understandably frustrating when those efforts culminate in an app store rejection, but especially frustrating when the reasons for those rejections aren't clearly communicated. Our members frequently cite the need for more transparency and better communication of developer guidelines as one of the top areas where the app stores could improve their developer relations. Recently, the App Association compiled a document where we lay out these and other priority asks from the small app developer community to the platforms.[8]

At the same time, small app developers benefit mightily from the investments of the large app stores (which, importantly, also interconnect with those companies' underlying operating systems) in myriad ways, especially on privacy and security. Unlike the large platforms themselves or big-name app competitors, App Association members do not enjoy the insulations of brand-awareness, large PR departments, or hordes of lawyers to mitigate the fallout of privacy faux pas or security breaches when they occur.[9] Our members are, by definition, smaller companies that often operate on shoestring budgets, with employees that double- or triple-up on different core roles at their business throughout the day. That means that our members must put extraordinary care into maintaining user trust and ensuring that breaches do not occur in the first place. Innovations like Secure Enclave in iOS, end-to-end encryption, and just-in-time notifications all represent massive investments in privacy and security-enhancing technology that our members leverage to protect users without expending the extraordinary amounts of time and capital it would take to develop such tools themselves.

Furthermore, the incredible user trust in the underlying app ecosystems, nurtured over years and currently flourishing within the app stores, is a major boon to the ability of our members to market and grow their products and services. Because users are much more confident in the safety of downloading an app from within the app store compared to downloading software on the open web, our members can quickly get into the hands of millions of users, a reality that did not exist prior to app stores.[10]

Unfortunately, some of the measures considered by in Congress and in the states ask app platforms to make compromises when it comes to the privacy and security of their ecosystems in the name of competition. Many of these would undermine overall trust in app stores, and, as a result, in many of our member companies. That is a tradeoff that we don't believe need exist and represents a point with which many App Association members take issue. As legislators and regulators scramble to introduce antitrust proposals directed to the largest tech platforms, it is vital that they take account of how such proposals stand to disrupt the secure app ecosystem and negatively affect the very competitors they seek to empower.

How Platform Non-discrimination Measures and Line of Business Restrictions Can Decrease Trust in App Association Member Companies

A key feature of many recent antitrust proposals are blanket non-discrimination mandates and line of business restrictions. Proponents argue that such restrictions are necessary to mitigate the ability of large tech platforms to pick winners and losers among the many companies and products that operate on top of their services, especially in cases where the platform company offers a competing product.

Unfortunately, as written, bills like the **American Choice and Innovation Online Act (ACIA - H.R. 3816)/ American Innovation and Choice Online Act (S. 2992)** create an unnecessary privacy vs. competition trade-off, ultimately devaluing privacy and disturbing the trusted app ecosystem our members benefit from in the name of promoting competition. The House version of ACIA would prevent app stores from "excluding" apps on the basis of integral privacy and safety checks conducted when those apps seek to enter the app store or perform updates, because such exclusions would constitute unfair discrimination against competing businesses.[11] Forbidden exclusionary conduct under the bill includes vetting and removing apps that violate app store guidelines; for example an app that fails to post a privacy policy within the app, or an app intended primarily for children that allows third-party advertising.[12] While the bill gestures towards the valid privacy and security justifications app stores may use to exclude certain apps, it makes it all but impossible to actually rely upon those justifications.[13]

Meanwhile, the Senate version of ACIA (S. 2992) attempts to limit the damage the House version would wreak, though without great effect. For instance, S. 2992 attempts to rescope prohibited conduct to include any conduct that would "unfairly preference the covered platform operator's own products, services, or lines of business over those of another business user . . . in a manner that would materially harm competition *on the platform*" (emphasis added) as opposed to *any* similarly situated "business user", as in the House bill. While seemingly more flexible, this construct remains problematic for App Association members like Betsy Furler of For All Abilities, who utilizes platform accessibility features built into Apple's operating system, such as Guided Access and VoiceOver, to build her own solutions for individuals with accessibility needs. Certainly, a software platform offering its own Guided Access feature as part of its bundle of developer services provides a clear advantage

The American Choice and Innovation Online Act (H.R. 3816)

Introduced by Antitrust Subcommittee Chairman Cicilline (D-RI) and Representative Lance Gooden (R-TX), ACIA prohibits conduct that "advantages the covered platform operator's own products, services, or lines of business" over those of another competitor or excludes or disadvantages those of a competitor relative to the platforms. The bill also prohibits a platform company from engaging in any conduct that "discriminates among similarly situated business users" on the platform.

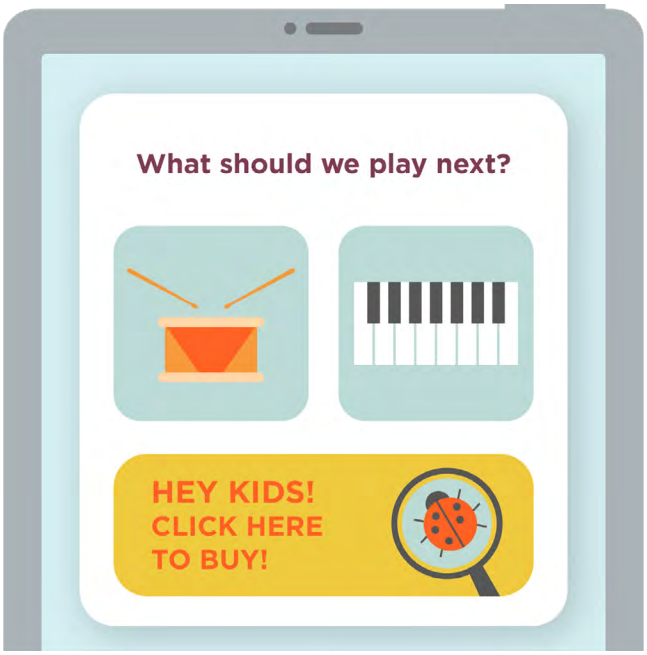
Effect on Small App Developers

The bill may eliminate the ability for platforms to remove questionable or unscrupulous apps, such as those that use fake reviews to get a leg-up over competitors. It may also prohibit the pre-installation of platform-owned apps that our members currently utilize to enhance their own products or outlaw the platform's role in restricting app maker access to customer data, a key safety mechanism that enhances trust in apps generally.

to the platform's own offering over a potential competitor offering such a feature on a standalone basis for developers. Doing so might even "harm competition on the covered platform" in the eyes of other would-be entrants who might be threatened by its success and adoption. The bill's arbitrary narrowing of the relevant market to "on the covered platform"—moving from the current common understanding of a market as products and services that consumers treat as substitutes—could eliminate any useful platform offering for developers simply because the platform provided it. In other words, S. 2992 would likely discourage platforms from providing tools like Guided Access that could meet the definition of prohibited conduct under S. 2992, robbing a developer with good intentions, like Betsy, of a powerful tool.

The platform's ability to vet and, in some cases, exclude apps that do not take user privacy seriously is key to preserving the overall trust in the app store. The vast majority of mobile device users cite trust as the number one factor when deciding to grant an app access to their personal data, and users already commonly restrict access and delete apps they believe pose a privacy risk.[14] 89 percent of users have at some point denied features, such as microphone or location access, to an app they did not trust, while 63 percent of users have deleted an app outright due to privacy concerns.[15] Instead of hamstringing future privacy and security monitoring, Congress should push app stores to *strengthen* their screening process so they can meet the strong consumer demand for a trustworthy ecosystem.

App Association members also support app store commitments to vet for privacy and security because it preserves a fair playing field between them and competing apps that may not wish to play by the rules. Without a healthy reviewal process to ensure compliance, it becomes much easier for bad actors to ignore important safeguards to serve illegitimate aims.



Imagine two simple music production apps directed toward children. Nominally, the music production apps could be construed to compete with Apple's Logic line of software and apps, thus triggering non-discrimination restrictions under both the House and Senate versions of ACIA. Imagine that one app complies with the Child Online Privacy Protection Act (COPPA), which requires the app to receive verifiable parental consent (VPC) for collection of any data about kids and prevents the app from selling children's data to third parties for the purpose of advertising without first obtaining VPC. Meanwhile, another app flouts the rules and begins monetizing the app through advertisements. The app that monetizes via advertising gains a whole new stream of revenue it could use to further advantage itself over the competitor.

While COPPA prohibits this activity, ACIA effectively shields the app from the platform imposing any consequences on it, like removing the app for violating the platform's terms of service. That's because both versions of ACIA, along with several of the other bills mentioned in this paper, include a difficult to achieve affirmative defense for the platform to justify its removal decision. In the House version, the platform must show that if it removes the app, doing so "would not result in harm to the competitive process by restricting or impeding legitimate activity by business users", while in the Senate version the standard becomes "has not resulted in and would not result in *material* harm" (emphasis added). In both versions the platform must show that the action "was narrowly tailored, could not be achieved through a less discriminatory means, was non-pretextual, and was necessary" to "prevent a violation of, or comply with, Federal or State law . . . or protect user privacy or non-public data."[16] The platform company would further have to make this showing by "clear and convincing evidence" in the House version or "the preponderance of evidence" in the Senate version.

In other words, the platform company is presumed liable under ACIA (albeit with slightly more flexibility in the Senate version) for removing the bad actor app because removal would run afoul of ACIA's prohibition on both advantaging Apple's own offerings (Logic vs. the children's music production app) *and* its prohibition on "discriminating" between similarly situated business users, *unless* it can meet the high evidentiary bar described above. Even in clear cut situations like an app openly flouting COPPA, it seems unlikely that a platform company would want to assume the substantial risk of additional liability in order to remove the app. While in this example ACIA improves the bad-actor's position vis-à-vis Apple (insofar as it actually seeks to compete against Apple in the first place) many other important prerogatives, including user privacy and competition among smaller market players, are tossed aside in the process.

While the consequences described above are serious and concerning on their own, equally concerning are the long-term effects that an unmanaged software marketplace would have on the smallest app makers. Specifically, if platform companies are prohibited from making management decisions because they are prohibited for being discriminatory, the burden for vetting the privacy practices of apps falls to consumers. If consumers are unable to rely on platform companies to perform a gatekeeping function that involves the prevention and removal of apps that disrespect privacy expectations, they either must do their own, in-depth investigations of app makers or else rely on some other proxy to weed out bad actors, such as reputation. In the long run, consumers are most likely to download only apps made by established companies with brand name recognition—in other words, only big companies with a long history on the app stores. Most App Association members are younger companies with only limited brand name recognition in their respective markets. Therefore, they rely much more on the privacy-based vetting and gatekeeping functions of platform companies and prohibitions on those gatekeeping functions impact them disproportionately vis-à-vis larger competitors.

Some non-discrimination measures currently under consideration in Congress and in numerous states would also require platforms to allow the "sideloading" of apps (and app stores) either via a general prohibition on the disadvantaging or excluding of third-parties or via a more specific provision saying a platform may not "restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features."[17]

Competition and Antitrust Law Enforcement Reform Act (CALERA) (S. 225)

Introduced by Senator Amy Klobuchar (D-MN), the bill, among numerous other changes to competition laws and enforcement paradigms, would expanding existing antitrust laws to forbid "exclusionary conduct that presents an appreciable risk of harming competition."

Effect on Small App Developers

Similar to the ACIA (H.R. 3816), the bill may eliminate the ability for platforms to vet their own ecosystems in order to remove questionable or unscrupulous apps. For example, CALERA's definition of "exclusionary conduct" includes conduct that "materially disadvantages 1 or more actual or potential competitors." If any *potentially* competing app maker can show that a platform company deciding to remove its app disadvantages the app maker while presenting any "appreciable risk" of harming competition, it has a plausible antitrust case. The threat of an antitrust case under this standard, which would give a single competitor a great deal of leverage in these situations, could easily dissuade a platform company from removing bad actor apps that threaten consumer privacy.

Sideloading brings the issue of privacy and security vetting to another level. Today, the vast majority of app downloads come through official app store channels, meaning that most of the apps that virtually all everyday users interact with have gone through each app store's rigorous vetting process. In Apple's case, for example, App Store review resulted in nearly one million removals of new apps and rejections to updates of existing apps last year.[18] Though certainly not all of these apps or updates were crafted with malicious intentions, the stats clearly indicate the important privacy and security function of review performed at the platform level. Most importantly, as a result of these vigorous processes, users are able to browse the official app stores with the confidence that any app they choose to download is free of harmful malware. On the other hand, the situation is far less rosy for those who choose to download through unofficial third-party app stores, as is currently possible through the Android operating system. In fact, researchers recently found that 99.9 percent of mobile malware was hosted on third-party app stores.[19]

Sideloading

"Sideloading" is the process of downloading and installing mobile apps onto a device via unauthorized third-party app stores or straight from the web. Sideloaded apps more frequently contain malware than apps downloaded through official app stores.

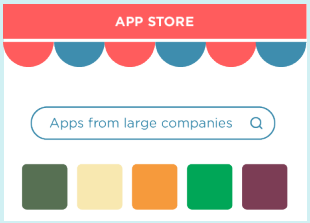
Unfortunately, mandated sideloading would obviate the screening process altogether, resulting in a less secure app store experience for all users. Unlike blanket non-discrimination language that prevents platforms from performing "exclusionary" privacy and security checks only when those products compete with a platform's own offering, a sideloading mandate allows any app to bypass a screening process if downloaded through the third party. As a result, fraudsters and anyone seeking to install malware on a consumer's device would have a direct pipeline, free from platform oversight, to do so. As more low-quality or outright fraudulent apps penetrate the ecosystem, users are likely to abandon apps altogether, or at least reduce their consumption of apps to the bare essentials, ironically benefiting the larger entities that compete over core device use-cases, like music libraries or photo apps. Decreasing user trust in the overall marketplace for apps harms our members through no fault of their own.

Vicious Cycle of App Spoofers

User **sideloads a spoofed app** that copies an App Association member app

Spoofed app downloads **malware** onto user device

User discovers malware and **loses trust** in similar apps or other, dissimilar apps without an established reputation, deleting them from their device



User adopts a policy of **only downloading apps made by large companies** with established reputations

It is important to note that the risks of sideloading are far from hypothetical or simply relegated to nerdy academic studies on the topic. Leading figures in the defense, cybersecurity, and consumer security space have long warned of the risks of downloading apps from unofficial app stores and advise their own employees and customers from doing so.[20] Moreover, researchers in adjacent markets increasingly recognize the need for trusted gatekeepers, such as in for internet of things (IoT) software. One study cited the lack of a centralized, trusted platform for the dissemination of IoT apps as a key reason that the market for smart devices is now "one of the most lucrative markets for hackers" and will continue to be so until the trust issue is solved.[21]

Another way platform skeptics intend to address conflict of interest questions is through line of business restrictions that would categorically prohibit a platform operator from owning any other business that runs alongside its own platform. For instance, a social media platform would be unable to also own a messaging application that runs on the platform. While perhaps reasonable in

Open App Markets Act (S.2710)

Introduced by Senators Richard Blumenthal (D-CT), Marsha Blackburn (R-TN), and Amy Klobuchar (D-MN), the bill would require app stores to allow users to download apps from third-party app stores, bar app stores from using non-public information about apps to compete with them, and require that operating systems provide equal access to software and hardware features to all apps.

Effect on Small App Developers

Similar to the American Choice and Innovation Online Act (H.R. 3816), S. 2710 would outlaw the platform's role in restricting access to an app maker's customer's data, a key privacy and safety mechanism that enhances trust in apps generally. The bill would also require sideloading, a feature that reduces trust in app ecosystems.

some contexts, such line of business restrictions are especially problematic in the application marketplace due to the important interconnectivity between the app stores and the underlying operating systems and devices on which they run.

While the intent of such proposals is meant to prevent app stores and other platforms from holding important user data hostage from direct competitors and other interested third parties, there are valid privacy and security reasons that app platforms and their parent companies carefully manage the flow of data between the different levels of the device. Bills like the **Ending Platform Monopolies Act (H.R. 3825)** would make it impossible for app platforms to manage data as it travels between the device, operating system, and apps downloaded from the app store. Forcing a broken link between any of these three businesses destroys the privacy benefits consumers and app makers derive from the integrated bundle of services. For example, if an app platform is unable to closely interoperate with the operating system, the platform will be unable to complete important checks that prevent apps from collecting more data than they promise or ensure that the app does not disable important security features embedded deep into the operating system. Breaking up the companies and then overlaying a set of interoperability requirements (see next section) is a poor substitute to an integrated set of services like this that occurs naturally in the market. In attempting to recreate the privacy and efficiency benefits of this integration, such a regime comes with the added friction of a government-designed market structure as opposed to one that is disciplined instead by competition from other companies in the market. In particular, creating gaps in the flow of data in this ecosystem unavoidably opens up new privacy and security risks that do not appear to be justified by other considerations.

Moreover, several of the most promising advances in privacy over the last few years were born out of the important interplay between operating systems, app stores, and devices.[22] For example, Apple's App Tracking Transparency (ATT) tool creates a simple solution to the opt-in/opt-out binary that has so far evaded easy resolution in the policy world, massively improving user privacy outcomes along the way.[23] ATT provides an easy and efficient way for users to opt-out of unwanted tracking that follows them outside of the app onto websites or even other third-party apps. ATT's seamless operationalization is only possible because of the synergy between the app store, which conducts the review to determine the extent of the app's data usage, and the operating system, which then sends out the push notification that appears on the user's device.

Ending Platform Monopolies Act (H.R. 3825)

Introduced by Representatives Pramila Jayapal (D-WA) and Lance Gooden (R-TX), the bill authorizes the Federal Trade Commission (FTC) and the Department of Justice to take action when a covered platform operator runs a line of business other than the covered platform that gives it an unfair advantage vis-à-vis competitors or creates a conflict of interest.

Effect on Small App Developers

The bill could prohibit the simultaneous control of the device, the operating system, and the app store. Because this dismantling would break up the bundle of services (such as privacy-enhancing technologies) and make them more expensive for developers to source, the bill would raise barriers to entry for App Association members and future companies like them.

Usage statistics for ATT bear out that users seeking to protect the sensitive data they share with apps have wholly embraced this development. In the first three weeks following the release of iOS 14.5, which first introduced the ATT tool, only around 6 percent of U.S. users chose to allow tracking among users who chose to either allow or deny tracking.[24] As ATT continues to make inroads with consumers, the parent companies of other app platforms are experimenting with their own tools to reduce the surveillance of users across the web.[25]

Privacy labels are another recent advancement applauded by many within the privacy world but thrown into question by line of business restrictions. As the sophistication of apps and the marketplace for insights and data generated through those apps continues to grow, app platforms have begun to introduce easy to understand privacy "nutrition" labels that share key information about to whom and for what reason user data is shared or sold. The new tool benefits all, as it gives honest app developers an easier way to show off their privacy bona fides, while also negating the need for users to dig through dense privacy policies to uncover simple facts about a company's policies.

Notably, the push to create more accessible privacy labeling and provide clearer information for users in the mobile space is part of a larger effort that spans related fields, such as that for IoT device security, a clear indicator that the marketplace is increasingly receptive to such interventions.[26] Despite this momentum, these consumer-friendly tools may run afoul of proposed legislation, since information about which sensitive device features apps can access and the ability for the platform to verify self-reported privacy label information only exists because of the strong relationship between app, device, and operating system.

How Interoperability Mandates Can Harm Small App Developers

The policy solutions discussed thus far mostly seek to resolve questions of platform power through the closing of doors; that is, by reducing the ability of platforms to travel through different passageways to connect all their services under the same roof. The other major prong represented in recent antitrust proposals seeks to solve through the opening of windows; that is, by increasing the number entities from the outside with access to the building.[27] Proponents argue that by increasing access, new market entrants will emerge to challenge incumbent businesses, especially those that ward off competitors through the advantage of network effects (most notably, large social media companies).[28] Others say that a broader market for consumer data will incent smaller firms to innovate novel use-cases for data that larger firms may have overlooked.[29] "Open window" mandates offered by antitrust backers typically take two forms: data portability and data interoperability.

Data portability is a concept that will already be familiar to many through its inclusion in existing comprehensive privacy laws in Europe (the General Data Protection Regulation [GDPR]) and in some individual states, including California (California Consumer Privacy Act [CCPA]). Typically, data portability mandates require that businesses, upon request, provide a consumer's data in a commonly used and machine-readable format and that users have the right to request a business to transfer the data to another business, if technically feasible.

New bills, such as the **Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 (H.R. 3849)**, would codify at the federal level data portability rights similar to those required through GDPR and CCPA and already put into place by many businesses. The App Association supports the inclusion of data portability language like that included in GDPR and CCPA as a component of a federal privacy bill that sets a uniform standard for data protection and access across the states.

A federal privacy bill becomes even more vital when considering the more problematic interoperability prong. Even some of the biggest proponents of interoperability mandates recognize the existence of a federal privacy bill as an essential pre-requisite to the opening windows across the board.[30] Consider the framework offered by the ACCESS Act of 2021. The bill requires covered platforms to maintain a set of transparent, third party accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with *any* competing business or any *potentially* competing business. The only constraints to the otherwise unlimited access that the bill contemplates is when the business fails to "reasonably secure" the data it receives or introduces a "security risk" (terms left ambiguous under the legislation), or when it fails meet FTC-developed standards (new rulemaking authorized under the bill) to interoperate.[31]

ACCESS Act of 2021 (H.R. 3849)

Introduced by Representatives Mary Gay Scanlon (D-PA) and Burgess Owens (R-UT), the bill gives the FTC new authority and enforcement tools to establish new rules for interoperability and data portability.

Effect on Small App Developers

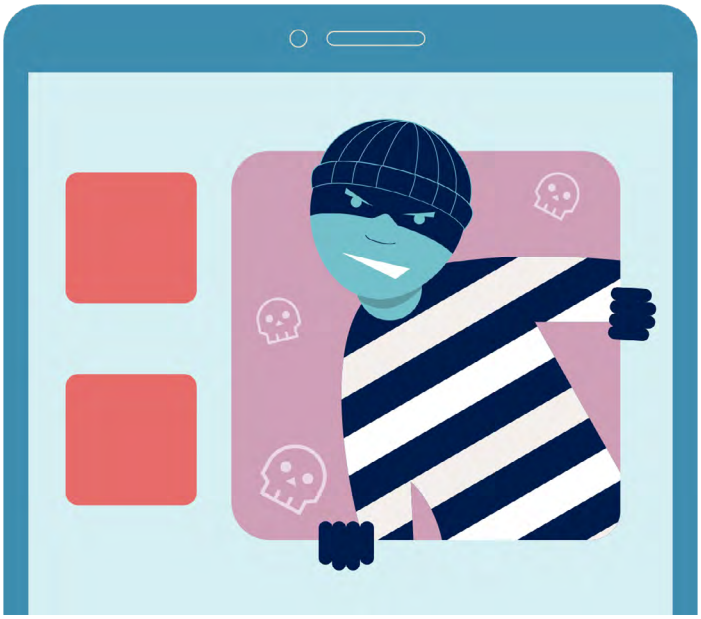
The data interoperability mandates could create a cornucopia of privacy risks as greater amounts of data leave the secure ecosystem of the app platforms, potentially undermining user trust in apps.

Of course, without a federal privacy law on the books, it would fall to the chronically underfunded and understaffed FTC to police the marketplace against these security risks or non-compliance with standards. Both are incredibly complex and technical tasks that the agency has never overseen in any comparable market to date. As we've pointed out in other areas where FTC has sole oversight, such as that for the Children's Online Privacy Protection Act (COPPA), enforcement can be unacceptably lax or scattershot, with bad actors brazenly evading the rules through loopholes that allow them to accrue huge advantages over those that play by the rules.[32] It's unlikely that the outcomes would be much better in the larger, much more technically complex market for user mobile data accessed through open APIs.

The ACIA also includes similar language that would prevent covered platforms from restricting or impeding third parties from accessing *any* data generated on the platform through its activities or those of its users, such as through "contractual or technical restrictions that prevent the portability of such data by the business user to other systems or applications."[33] In practice, this prohibition end-runs around app store guidelines that require apps to notify users of their collection or transmission of data, including sensitive data; presumes the illegality of platform-level notifications or warnings about an app accessing sensitive data; and runs afoul of privacy frameworks in other jurisdictions, such as GDPR.

The lack of comprehensive privacy rules in the United States also means that consumers would have no rights to correct, delete, or prevent further sales of their data even as untold numbers of new players gain access. According to Pew Research, 79 percent of Americans are already worried about data collection and usage by private companies.[34] Now imagine mandating that any third party gain access to the most sensitive data generated on one's device without giving consumers the ability to correct or delete their data when they discover an inaccuracy. As more privacy invasions and data breaches originate from these new players in the ecosystem, studies show that smaller players will face an especially difficult time surviving if their systems become compromised.[35] Once again, the risks of creating a marketplace potentially rife with fraud and abuse only stands to harm App Association members who rely on the trust generated by the existing app ecosystem.

Finally, it's also worth considering what types of new players we're talking about under a completely open interoperability mandate. The ACCESS Act fails to prevent all sorts of questionable firms from obtaining access through open APIs, such as those currently under FTC investigation or with open enforcement actions, known fraudsters, or potentially even businesses beholden to hostile state actors, from accessing consumer data, so long as they reasonably secure the data they receive. The nightmare scenario under this regime is easy to imagine, as we already went through it with the Cambridge Analytica scandal, except now, Facebook would have even less ability to shut down the



offending service, once discovered. Poorly vetted third parties that latch onto APIs can use that data for all sorts of nefarious purposes, including election meddling, discriminatory advertising, or other highly targeted profiling meant to manipulate individuals based on personal characteristics.

While the bill allows a covered platform to set privacy and security standards for access by competing businesses "to the extent reasonably necessary to address a threat to the covered platform or user data," it is unclear how this allowance sits alongside non-discrimination language considered in other bills that prohibits privacy or security actions that have an exclusionary affect unless the platform can offer an affirmative defense in court.[36]

Case Study: Interoperability Mandates in Health Care

Federal law imposes an interoperability and portability regime on healthcare "covered entities" and "business associates" under the Health Insurance Portability and Accountability Act (HIPAA).

These requirements are important interventions to ensure that the electronic health records (EHR) companies share usable information about patients' health with patients and the companies they select.

The record is replete with instances where EHR companies have blocked access to a patient's own data and that they engage in this blocking activity to preserve their advantage over other competitors in the ecosystem. Therefore, the information blocking rules requiring EHRs to provide access to healthcare data via APIs is necessary and must be vigorously enforced.

With respect to software platforms, analogous conditions are not present. The House Judiciary Antitrust Subcommittee's report did not build a record on this point, and we are not aware of widespread conduct by app stores or operating systems preventing consumers from accessing their own data to share with other companies.

Conclusion

We've come a long way since Cambridge Analytica. As consumers express increased desire for secure and private interactions within the apps and services they use on mobile platforms, both apps and platforms continue to innovate new ways to meet those goals. At the same time, there is still plenty to do to build trust and ensure that the nation set a strong standard for privacy, beginning with enacting a national comprehensive law with robust consumer rights.

As the larger conversation around internet platforms grows to encompass both privacy and antitrust, lawmakers must take care not to ignore the importance of nurturing the former in the name of the latter. Afterall, a more competitive marketplace is not guaranteed to solve the informational barrier that consumers face in making privacy choices in today's digital economy, especially if we outlaw emerging technologies that ease the process for consumers to make informed choices. However, as in any "market for lemons" equilibrium where the consumer is informationally outgunned by a more powerful player, the opposite may be true; firms may be forced to compete more on privacy once clearer information about data practices is made available to consumers and they are better able to vote with their feet. App Association members want to live in a world where they are rewarded for their good data stewardship and protected from reputational harm when some bad actor threatens the ecosystem with less than stellar stewardship. We'll continue fighting for this world, and, with any luck, those at the center of the current platform debate will join us too.

Endnotes

1. See, e.g., U.S. Senate Committee on Commerce, Science, and Transportation, "Committee Leaders Urge President to Prioritize Data Privacy Legislation" (July 16, 2021), available at https://www.commerce.senate.gov/2021/7/committee-leaders-urge-president-to-prioritize-data-privacy-legislation

2. Sarah Rippy, "US State Privacy Legislation Tracker", IAPP (July 28, 2021), available at https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

3. Bresee et al., A 'Nutrition Label' for Privacy", Proceedings of the 5th symposium on usable privacy and security, SOUPS '09 (2009), available at https://dl.acm.org/doi/abs/10.1145/1572532.1572538; Ian Carlos Campbell, "Apple will require apps to add privacy 'nutrition labels' starting December 8th", The Verge (November 5, 2020), available at https://www.theverge.com/2020/11/5/21551926/apple-privacy-developers-nutrition-labels-app-store-ios-14; Suzanne Frey, "New safety section in Google Play will give transparency into how apps use data" Android Developers Blog (May 6, 2021), available at https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html; Dieter Bohn, ""Privacy and Ads in Chrome Are About to Become FloCing Complicated", The Verge (March 30, 2021), available at https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing ("If Google sticks to its roadmap, by this time next year Chrome will no longer allow websites to use third-party cookies, which are cookies that come from outside their own domains. The change theoretically makes it vastly more difficult for advertisers to track your activities on the web and then serve you targeted ads. Safari and Firefox have already blocked those cookies, but when it comes to market share, Chrome is currently the leader and so its switchover is the big one.")

4. Office of Congressman David Cicilline, "House Lawmakers Release Anti-Monopoly Agenda for 'A Stronger Online Economy: Opportunity, Innovation, Choice'" (June 11, 2021), available at https://cicilline.house.gov/press-release/house-lawmakers-release-anti-monopoly-agenda-stronger-online-economy-opportunity

5. See American Choice and Innovation Online Act, H.R. 3816, 117th Cong. (2021)

6. See Ending Platform Monopolies Act, H.R. 3825, 117th Cong. (2021)

7. See ACCESS Act of 2021, H.R. 3849, 117th Cong. (2021)

8. "Competition Policy Priorities", ACT | The App Association, available at https://actonline.org/wp-content/uploads/competition-policy-priorities.pdf

9. Huseyin Cavusoglu, Birendra Mishra & Srinivasan Raghunathan, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, International Journal of Electronic Commerce 9, no. 1 (2004), available at https://www.jstor.org/stable/27751132 ("The result confirmed that smaller firms lose more than larger firms in case of a security breach.")

10. Joel Thayer and Morgan Reed, "The Impact of Platforms on Software Distribution: What Makes an Ecosystem Work?", ACT | The App Association, available at https://actonline.org/wp-content/uploads/The-Dynamic-App-Economy3.pdf

11. See American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(a)(1) (2021)

12. See App Store Review Guideline 1.3 (Kids); Guideline, 5.1.1 (Data Collection and Storage), available at https://developer.apple.com/app-store/review/guidelines/

13. See American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(c)(B)(ii) (2021)

14. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019," (2019), available at https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf

15. Id. at 6

16. See American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(c) (2021)

17. See e.g. American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2(b)(i) (2021); Competition and Antitrust Law Enforcement Reform Act of 2021, S. 225, 117th Cong. § 26A (2)(b)(i) (2021); Open App Markets Act, S. 2710, 117th Cong. § 3(d)(ii) (2021)

18. Apple, "Building a Trusted Ecosystem for Millions of Apps", p. 12 (June 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf

19. Symantec, "ISTR Internet Security Threat Report, Volume 23," p. 52 (March 2018), available at https://nsarchive.gwu.edu/document/17671-symantec-istr-internet-security-threat-report

20. See Griffin, Robert Jr., "Study on Mobile Device Security," U.S. Department of Homeland Security (April 2017), available at https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf ("Additionally, users should avoid [and enterprises should prohibit on their devices] sideloading of apps and the use of unauthorized app stores."); ENISA, "Vulnerabilities - Separating Reality from Hype," European Union Agency for Cybersecurity (August 24, 2016) available at https://www.enisa.europa.eu/publications/info-notes/vulnerabilities-separating-reality-from-hype ("Use the official application marketplace only. Users should … not [download applications] from third-party sources, to minimise the risk of installing a malicious application. Users should not sideload applications if they do not originate from a legitimate and authentic source."); Joe Gervais, "The Risks of Third-Party App Stores", Norton (July 18, 2018), available at https://us.norton.com/internetsecurity-mobile-the-risks-of-third-party-app-stores.html ("You might be tempted to download apps in the third-party stores, but you can't be sure about them.")

21. Abdullahi Arabo, Ian Brown & Fadi El-Mousa, Privacy in the Age of Mobility and Smart Devices in Smart Homes, Fourth IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT), 2012 (September 4, 2012), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2173360

22. See Cam Kerry, "One year after Schrems II, the world is still waiting for U.S. privacy legislation", Brookings TECHTANK (August 16, 2021), available at https://www.brookings.edu/blog/techtank/2021/08/16/one-year-after-schrems-ii-the-world-is-still-waiting-for-u-s-privacy-legislation/ ("In the absence of comprehensive privacy legislation, though, Apple and Google's efforts to control app stores and the flow of data on their systems are having the greatest impact on improving privacy protection in the app and adtech ecosystems. While promoting competition in the app market could produce indirect consumer benefits, reducing Apple and Google's ability to impose some level of privacy standards on mobile apps could enable more privacy abuses in the app ecosystem.")

23. Anthony Ha, "Apple's App Tracking Transparency feature has arrived — here's what you need to know", TechCrunch (April 26, 2021), available at https://techcrunch.com/2021/04/26/apples-app-tracking-transparency-feature-has-arrived-heres-what-you-need-to-know/

24. Estelle Laziuk, "iOS 14.5 Opt-in Rate - Daily Updates Since Launch", Flurry (May 25, 2021), available at https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/

25. See, e.g., Dieter Bohn, "Privacy and Ads in Chrome Are About to Become FloCing Complicated", The Verge (March 30, 2021), available at https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing

26. See, e.g., Agarwal et al., Ask the Experts: What Should Be on an IoT Privacy and Security Label?, 2020 IEEE Symposium on Security and Privacy (SP) (2020), available at https://www.computer.org/csdl/proceedings-article/sp/2020/349700a771/1j2LfTRYbNC

27. See ACCESS Act of 2021, H.R. 3849, 117th Cong. (2021)

28. See, e.g., Bennett Cyphers and Cory Doctorow, "Privacy Without Monopoly: Data Protection and Interoperability", EFF (February 12, 2021), available at https://www.eff.org/wp/interoperability-and-privacy

29. See, e.g., Andy Thurai, "How APIs Fuel Innovation", Wired (2013), available at https://www.wired.com/insights/2013/12/how-apis-fuel-innovation/

30. See Bennett Cyphers and Cory Doctorow, "Privacy Without Monopoly: Data Protection and Interoperability", EFF (February 12, 2021), available at https://www.eff.org/wp/interoperability-and-privacy ("More than anything, the dangers of data-sharing that we have addressed here underline the need for better privacy law.")

31. See ACCESS Act of 2021, H.R. 3849, 117th Cong. § 4(b-c) (2021)

32. Matt Schwartz, "COPPA, VPC, and the New Normal for Kids Online" ACT | The App Association (August 10, 2020), available at https://actonline.org/2020/08/10/coppa-vpc-and-the-new-normal-for-kids-online/

33. See American Choice and Innovation Online Act, H.R. 3816, 117th Cong. § 2 (b)(4) (2021)

34. Pew Research Center, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" (November 15, 2019), available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

35. See, e.g., Huseyin Cavusoglu, Birendra Mishra & Srinivasan Raghunathan, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, International Journal of Electronic Commerce 9, no. 1 (2004), available at https://www.jstor.org/stable/27751132 ("The result confirmed that smaller firms lose more than larger firms in case of a security breach."); National Cyber Security Alliance, America's Small Businesses Must Take Online Security More Seriously (Oct. 2012), available at www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic. ("60 percent of small and mid-sized businesses that are hacked go out of business within six months.")

36. See ACCESS Act of 2021, H.R. 3849, 117th Cong. § 4(d) (2021); American Choice and Innovation Online Act, H.R. 3816, 117th § 2(c) Cong. (2021)