



2022 Annotated App Store Guidelines



As lawmakers continue to consider measures that would restrict the ability of app platforms to manage their ecosystems, ACT | The App Association remains concerned that such limitations would massively reduce marketplace trust. For many small app developers within our membership, this threat is existential - without possessing a well-known brand presence themselves, they rely on a trusted ecosystem to seamlessly enter the market, reach millions of potential users, and grow their business. Though proponents of the so-called platform competition bills, including S. 2992, the American Innovation and Choice Online Act and S. 2710, the Open App Markets Act, repeatedly extol the pro-competitive virtues of reducing gatekeeper control over the platforms, they often overlook what platforms currently do to keep users safe and to create an ecosystem that users are actually comfortable transacting within. Without those protections and trust, the app marketplace is unlikely to remain a viable forum for smaller players to flourish.

With this document, we conduct a section-by-section investigation into one app platform's guidelines (the App Store Review Guidelines) to assess how exactly S. 2992 and S. 2710 are likely to erode currently existing consumer protections if they are passed into law. What this analysis --which is not exhaustive and is only the beginning of the inquiry into how the bills would impact app store management--reveals should concern anyone who proclaims to care about a safe app store experience for users. Our annotations (in blue) suggest that the legislation in question likely renders vast portions of the current guidelines—even uncontroversial protections against manipulative marketing practices, deceptive monetization of device features, misuse of children's data, and dozens of others—illegal outright or unenforceable without the platform initiating a costly legal defense in each instance. Even for the staunchest supporters of the bills, this analysis should provide good reason to question whether the legislation, as currently drafted, appropriately scopes prohibitions on plainly pro-consumer platform behavior. We hope these annotations add productive nuance to a discussion that too often exists in the lofty but vague realm of anti-Big Tech sentiment and consistently seems to ignore the common-sense mechanisms by which platforms ensure that bad actors stay out of the app store, maintaining a safe environment for developers who play by the rules.

Key Findings

On the following pages, we find that the platform antitrust bills would likely disrupt key consumer protections and quality control measures in each of the major sections of the App Store Review Guidelines, including Safety, Performance, Business, Design, and Legal.

Some of our critical findings include that:

-  The bills could prevent app stores from removing medical apps that provide inaccurate information. The bills would prevent limits on device hardware and software features, even if apps use them to make erroneous medical claims or diagnoses.
-  The bills could prevent app stores from removing apps that request excessive battery resources or risk damage to the device. The bills could prevent app stores from limiting access by apps to device features, even when that access compromises user safety by imposing excessive battery demands.
-  The bills could prevent app stores from removing apps that rip-off users with deceptive subscription terms and conditions. Under S. 2710, such techniques may be considered “legitimate business communications” and thus protected under the bill.
-  The bills could prevent app stores from removing apps that spam or copy-cat other apps. The bills bar app stores from enforcing any terms that may discriminate among similarly situated apps, even if those apps seek to game the system.
-  The bills could prevent app stores from removing apps that misrepresent their data sharing practices. The bills force app stores to rely on hard-to-prove legal defenses to justify pro-privacy platform decisions.

INTRODUCTION

The guiding principle of the App Store is simple—we want to provide a safe experience for users to get apps and a great opportunity for all developers to be successful. We do this by offering a highly curated App Store where every app is reviewed by experts and an editorial team helps users discover new apps every day. For everything else, there is always the open Internet. If the App Store model and guidelines are not best for your app or business idea that's okay, we provide Safari for a great web experience too.

On the following pages you will find our latest guidelines arranged into five clear sections: **Safety, Performance, Business, Design, and Legal.**

The App Store is always changing and improving to keep up with the needs of our customers and our products. Your apps should change and improve as well in order to stay on the App Store.

A few other points to keep in mind.

We have lots of kids downloading lots of apps. Parental controls work great to protect kids, but you have to do your part too. So know that we're keeping an eye out for the kids.

The App Store is a great way to reach hundreds of millions of people around the world. If you build an app that you just want to show to family and friends, the App Store isn't the best way to do that. Consider using Xcode to install your app on a device for free or use Ad Hoc distribution available to Apple Developer Program members. If you're just getting started, learn more about the Apple Developer Program.

We strongly support all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is great. We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.

If you attempt to cheat the system (for example, by trying to trick the review process, steal user data, copy another developer's work, manipulate ratings or App Store discovery) your apps will be removed from the store and you will be expelled from the Apple Developer Program.

WHAT WOULD CHANGE

S. 2710, Sec. 3(d) would interfere with the enforcement of more or less the entire guidelines on third-party apps because the provision would require Apple to provide "readily accessible means" for consumers to install third-party apps or app stores through means other than the App Store, thus creating a separate class of apps not subject to the guidelines.

S. 2992, Sec. 3(a)(4) also would interfere with the enforcement of substantially the entire set of guidelines on third-party apps because the provision would prohibit any material restriction on the capacity of a business user to access or interoperate with the platform, which may include imposing consequences like removal of an app for any violation of the guidelines, effectively mandating the acceptance of third-party software distributed outside the App Store and therefore not subject to the guidelines.

Similarly, Sec. 3(a)(1), (2), (3), (5), and (7) would interfere with the enforcement of the entire set of guidelines on third-party apps, because they reinforce the requirement for Apple to accept apps distributed through third-party means onto the platform by limiting restrictions that could be imposed on those apps.

SAFETY

Apps with user-generated content or services that end up being used primarily for pornographic content, Chatroulette-style experiences, objectification of real people (e.g. “hot-or-not” voting), making physical threats, or bullying do not belong on the App Store and may be removed without notice. If your app includes user-generated content from a webbased service, it may display incidental mature “NSFW” content, provided that the content is hidden by default and only displayed when the user turns it on via your website.

1. Safety

When people install an app from the App Store, they want to feel confident that it's safe to do so —that the app doesn't contain upsetting or offensive content, won't damage their device, and isn't likely to cause physical harm from its use. We've outlined the major pitfalls below, but if you're looking to shock and offend people, the App Store isn't the right place for your app

1.1 Objectionable Content

Apps should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy. Examples of such content include:

1.1.2

Realistic portrayals of people or animals being killed, maimed, tortured, or abused, or content that encourages violence. “Enemies” within the context of a game cannot solely target a specific race, culture, real government, corporation, or any other real entity.

1.1.3

Depictions that encourage illegal or reckless use of weapons and dangerous objects, or facilitate the purchase of firearms or ammunition.

1.1.4

Overtly sexual or pornographic material, defined by Webster's Dictionary as “explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings.” This includes “hookup” apps that may include pornography or be used to facilitate prostitution.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) would interfere with the enforcement of this entire section because the provision bars material restrictions on a business user's capacity to access the operating system and hardware and software features that are available to the platform's own offerings, and removing an app for violation of this guideline could be a material restriction on access to the operating system and hardware and software features.

WHAT WOULD CHANGE

S. 2710, Sec. 3(d) and 3(h) would interfere with the enforcement of this entire section because these provisions would require Apple to allow third-party apps not subject to the guidelines onto a device and would also bar Apple from restricting access by any app to the operating system and device features, and a trial attorney could easily claim that removal or rejection on the basis of any of these safety measures materially restricts an app's access to the platform.

1.2 User-Generated Content

Apps with user-generated content present particular challenges, ranging from intellectual property infringement to anonymous bullying. To prevent abuse, apps with user-generated content or social networking services must include: ●...

A method for filtering objectionable material from being posted to the app A mechanism to report offensive content and timely responses to concerns The ability to block abusive users from the service Published contact information so users can easily reach you Apps with user-generated content or services that end up being used primarily for pornographic content, Chatroulette-style experiences, objectification of real people (e.g. “hot-or-not” voting), making physical threats, or bullying do not belong on the App Store and may be removed without notice. If your app includes user-generated content from a webbased service, it may display incidental mature “NSFW” content, provided that the content is hidden by default and only displayed when the user turns it on via your website.

1.2.1 Creator Content

Apps which feature content from a specific community of users called “creators” are a great opportunity if properly moderated. These apps present a singular, unified experience for customers to interact with various kinds of creator content. They offer tools and programs to help this community of non-developer creators to author, share, and monetize user-generated experiences. These experiences must not change the core features and functionality of the native app—rather, they add content to those structured experiences. ●...

These experiences are not native “apps” coded by developers—they are content within the app itself and are treated as user-generated content by App Review. Such creator content may include video, articles, audio, and even casual games. The App Store supports apps offering such user-generated content so long as they follow all Guidelines, including Guideline 1.2 for moderating user-generated content and Guideline 3.1.1 for payments and in-app purchases. Creator apps should share the age rating of the highest age-rated creator content available in the app, and communicate to users which content requires additional purchases.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) would interfere with the enforcement of this guideline because the provision bars material restrictions on a business user’s capacity to access the operating system and hardware and software features that are available to the platform’s own offerings, and removing an app for violation of this guideline could be a material restriction on access to the operating system and hardware and software features.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and (7) would also interfere with this provision because they could require the platform to allow creators to have access to the software, OS, and hardware features that a native app would have, and because the guideline may operate to restrict creators’ ability to collect data about a covered platform user directly through the OS.

S. 2710, Sec. 3(a) and (f) would interfere with the enforcement of this section because the provisions would require the platform to allow creators to potentially create things that function like native apps, while prohibiting the platform from requiring them to follow IAP rules.

1.3 Kids Category

The Kids Category is a great way for people to easily find apps that are designed for children.

If you want to participate in the Kids Category, you should focus on creating a great experience specifically for younger users. [These apps must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a parental gate.](#)

Keep in mind that once customers expect your app to follow the Kids Category requirements, it will need to continue to meet these guidelines in subsequent updates, even if you decide to deselect the category. Learn more about parental gates.

[You must comply with applicable privacy laws around the world relating to the collection of data from children online.](#) Be sure to review the Privacy section of these guidelines for more information. In addition, Kids Category apps may not send personally identifiable information or device information to third parties. Apps in the Kids Category should not include thirdparty analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit the IDFA or any identifiable information about children (such as name, date of birth, email address), their location, or their devices. This includes any device, network, or other information that could be used directly or combined with other information to identify users and their devices. Third-party contextual advertising may also be permitted in limited cases provided that the services have publicly documented practices and policies for Kids Category apps that include human review of ad creatives for age appropriateness.

1.4 Physical Harm

If your app behaves in a way that risks physical harm, we may reject it. For example:

1.4.1

[Medical apps that could provide inaccurate data or information, or that could be used for diagnosing or treating patients may be reviewed with greater scrutiny.](#)

Apps must clearly disclose data and methodology to support accuracy claims relating to health measurements, and if the level of accuracy or methodology cannot be validated, we will reject your app. For example, apps that claim to take x-rays, measure blood pressure, body temperature,

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(7) would interfere with the enforcement of this guideline because the provision bars material restrictions on a business user's access to data generated on the platform by an individual on the business user's service, even if the business user's data collection or processing conduct is illegal.

Apple could overcome the prohibition with an affirmative defense, which would apply only to the facts in the case at bar, and only if the platform meets narrow evidentiary requirements, if a lawsuit were filed to protect the app that was subject to removal.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and (7) would also interfere with this provision because they could require the platform to allow creators to have access to the software, OS, and hardware features that a native app would have, and because the provision may operate to restrict creators' ability to collect data about a covered platform user directly through the OS.

WHAT WOULD CHANGE

S. 2710, Sec. 3(f) would interfere with the enforcement of this guideline, because the provision would require Apple to give developers making fake medical apps full access to the system's sensors even if they use them to make false medical claims. Sec. 3(b) would also interfere with the enforcement of the guideline, because the provision would prohibit Apple from interfering with an app originally designed for a separate purpose, but communicated within the app after it had been approved to users that they could receive real medical help without the validation requirements in this guideline.

S. 2992, Sec. 3(a)(4) would interfere with Apple's enforcement of this guideline because rejecting a medical app due to inability to validate the accuracy or methodology of health measurements could easily be interpreted as a material restriction or impediment to the app's ability to access hardware or software features (the sensors in particular) versus Apple's own offerings.

blood glucose levels, or blood oxygen levels using only the sensors on the device are not permitted.

Apps should remind users to check with a doctor in addition to using the app and before making medical decisions. If your medical app has received regulatory clearance, please submit a link to that documentation with your app.

1.4.2

Drug dosage calculators must come from the drug manufacturer, a hospital, university, health insurance company, pharmacy or other approved entity, or receive approval by the FDA or one of its international counterparts. Given the potential harm to patients, we need to be sure that the app will be supported and updated over the long term.

1.4.3

Apps that encourage consumption of tobacco and vape products, illegal drugs, or excessive amounts of alcohol are not permitted on the App Store. Apps that encourage minors to consume any of these substances will be rejected. Facilitating the sale of controlled substances (except for licensed pharmacies and licensed or otherwise legal cannabis dispensaries), or tobacco is not allowed.

1.4.4

Apps may only display DUI checkpoints that are published by law enforcement agencies, and should never encourage drunk driving or other reckless behavior such as excessive speed.

1.4.5

Apps should not urge customers to participate in activities (like bets, challenges, etc.) or use their devices in a way that risks physical harm to themselves or others.

1.5 Developer Information

People need to know how to reach you with questions and support issues. Make sure your app and its Support URL include an easy way to contact you; this is particularly important for apps that may be used in the classroom. Failure to include accurate and up-to-date contact information not only frustrates customers, but may violate the law in some countries. Also ensure that Wallet passes include valid contact information from the issuer and are signed with a dedicated certificate assigned to the brand or trademark owner of the pass.

WHAT WOULD CHANGE

S. 2710, Sec. 4(b) would interfere with the enforcement of this guideline because the provision would prohibit Apple from imposing restrictions on communications of a developer “concerning legitimate business offers,” and a trial attorney could claim that restricting an app from calculating dosages or other drug facts would be a restriction on a communication concerning a legitimate business offer.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision would prohibit Apple from imposing restrictions on communications of a developer “concerning legitimate business offers,” and a trial attorney could claim that restricting an app from urging customers to participate in bets, challenges, etc., or use devices in a way that risks physical harm to themselves or others is a restriction on a communication concerning a legitimate business offer.

1.6 Data Security

[Apps should implement appropriate security measures to ensure proper handling of user information collected pursuant to the Apple Developer Program License Agreement and these Guidelines \(see Guideline 5.1 for more information\) and prevent its unauthorized use, disclosure, or access by third parties.](#)

1.7 Reporting Criminal Activity

Apps for reporting alleged criminal activity must involve local law enforcement, and can only be offered in countries where such involvement is active.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and Sec. 3(a)(7) would interfere with the enforcement of this guideline because the provisions would prohibit restrictions on access by certain apps to device and software features—as well as personal information—and requiring an app developer to ensure proper handling of user information and prevent its unauthorized use, disclosure, or access by third parties, would constitute such restrictions.

PERFORMANCE

2.1 App Completeness

Submissions to App Review, including apps you make available for pre-order, should be final versions with all necessary metadata and fully functional URLs included; placeholder text, empty websites, and other temporary content should be scrubbed before submission. Make sure your app has been tested on-device for bugs and stability before you submit it, and include demo account info (and turn on your back-end service!) if your app includes a log-in. [If you offer in-app purchases in your app, make sure they are complete, up-to-date, and visible to the reviewer, or that you explain why not in your review notes.](#) Please don't treat App Review as a software testing service. We will reject incomplete app bundles and binaries that crash or exhibit obvious technical problems.

2.2 BETA Testing

Demos, betas, and trial versions of your app don't belong on the App Store –use TestFlight instead. Any app submitted for beta distribution via TestFlight should be intended for public distribution and should comply with the App Review Guidelines. Note, however, that apps using TestFlight cannot be distributed to testers in exchange for compensation of any kind, including as a reward for crowd-sourced funding. Significant updates to your beta build should be submitted to TestFlight App Review before being distributed to your testers. To learn more, visit the TestFlight Beta Testing page.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision would prohibit Apple's interference with developer communications concerning "a legitimate business offer," and a requirement to explain in-app purchases could constitute such a restriction on business offers.

2.3 Accurate Metadata

Customers should know what they're getting when they download or buy your app, so make sure all your app metadata, including [privacy information](#), your app description, screenshots, and previews accurately reflect the app's core experience and remember to keep them upto-date with new versions.

2.3.1

Don't include any hidden, dormant, or undocumented features in your app; your app's functionality should be clear to end users and App Review. All new features, functionality, and product changes must be described with specificity in the Notes for Review section of App Store Connect (generic descriptions will be rejected) and accessible for review. Similarly, marketing your app in a misleading way, such as by promoting content or services that it does not actually offer (e.g. iOS-based virus and malware scanners) or [promoting a false price, whether within or outside of the App Store, is grounds for removal of your app from the App Store and termination of your developer account](#). Egregious or repeated behavior is grounds for removal from the Apple Developer Program. We work hard to make the App Store a trustworthy ecosystem and expect our app developers to follow suit; if you're dishonest, we don't want to do business with you.

2.3.2

If your app includes in-app purchases, make sure your app description, screenshots, and previews clearly indicate whether any featured items, levels, subscriptions, etc. require additional purchases. [If you decide to promote in-app purchases on the App Store, ensure that the in-app purchase Display Name, Screenshot and Description are appropriate for a public audience, that you follow the guidance found in Promoting Your In-App Purchases, and that your app properly handles the SKPaymentTransactionObserver method so that customers can seamlessly complete the purchase when your app launches.](#)

2.3.3

Screenshots should show the app in use, and not merely the title art, login page, or splash screen. They may also include text and image overlays (e.g. to demonstrate input mechanisms, such as an animated touch point or Apple Pencil) and show extended functionality on device, such as Touch Bar.S

.....

WHAT WOULD CHANGE

S.2992, Sec. 3(a)(2) would make it difficult for Apple to enforce this guideline because the platform making a determination that an app is not accurately representing its privacy practices and removing it based on that determination could be interpreted as a limitation on the ability of a rival app to compete.

.....

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(3) could interfere with Apple's enforcement of this guideline because the provision would bar Apple from taking punitive action against a developer for offering "different pricing terms" on another app store.

Sec. 3(b) could also interfere with the guideline's enforcement because that provision bars Apple from imposing restrictions on developers' communications with the users of their app through the app or directly.

.....

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(3) could interfere with Apple's enforcement of this guideline because the provision would bar Apple from taking punitive action when a developer offers "different pricing terms" or "conditions of sale" through a third-party in-app payment system.

2.3.4

Previews are a great way for customers to see what your app looks like and what it does. To ensure people understand what they'll be getting with your app, [previews may only use video screen captures of the app itself.](#) Stickers and iMessage extensions may show the user experience in the Messages app. You can add narration and video or textual overlays to help explain anything that isn't clear from the video alone.

2.3.5

[Select the most appropriate category for your app, and check out the App Store Category Definitions if you need help. If you're way off base, we may change the category.](#)

2.3.6

Answer the age rating questions in App Store Connect honestly so that your app aligns properly with parental controls. If your app is mis-rated, customers might be surprised by what they get, or it could trigger an inquiry from government regulators. If your app includes media that requires the display of content ratings or warnings (e.g. films, music, games, etc.), you are responsible for complying with local requirements in each territory where your app is available.

2.3.7

[Choose a unique app name, assign keywords that accurately describe your app, and don't try to pack any of your metadata with trademarked terms, popular app names, pricing information, or other irrelevant phrases just to game the system.](#) App names must be limited to 30 characters. Metadata such as app names, subtitles, screenshots, and previews should not include prices, terms, or descriptions that are not specific to the metadata type. App subtitles are a great way to provide additional context for your app; they must follow our standard metadata rules and should not include inappropriate content, reference other apps, or make unverifiable product claims. Apple may modify inappropriate keywords at any time or take other appropriate steps to prevent abuse.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with Apple's enforcement of this guideline because it would bar Apple from imposing restrictions on developers' communications with users of their apps concerning "legitimate business offers" (the guideline would limit how any business offers may appear in previews).

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2) would interfere with Apple's enforcement of this guideline because Apple's unilateral decision, even if the developer was "way off base," to re-categorize an app could be interpreted as a limitation on the ability for that app to compete on the platform (e.g., if Apple re-categorizes it as a Kids app).

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) could interfere with this guideline because the provision bars restrictions on a developer's communications concerning "legitimate business offers."

2.3.8

Metadata should be appropriate for all audiences, so make sure your app and in-app purchase icons, screenshots, and previews adhere to a 4+ age rating even if your app is rated higher. For example, if your app is a game that includes violence, select images that don't depict a gruesome death or a gun pointed at a specific character. Use of terms like "For Kids" and "For Children" in app metadata is reserved for the Kids Category.

Remember to ensure your metadata, including app name and icons (small, large, Apple Watch app, alternate icons, etc.), are similar to avoid creating confusion.

2.3.9

You are responsible for securing the rights to use all materials in your app icons, screenshots, and previews, and you should display fictional account information instead of data from a real person.

2.3.10

[Make sure your app is focused on the iOS, iPadOS, macOS, tvOS or watchOS experience, and don't include names, icons, or imagery of other mobile platforms in your app or metadata, unless there is specific, approved interactive functionality. Make sure your app metadata is focused on the app itself and its experience. Don't include irrelevant information.](#)

•••

WHAT WOULD CHANGE

S. 2710, Sec. (3)(b) would interfere with the platform's enforcement of this guideline because the provision would bar restrictions on a developer's communications with users regarding a legitimate business offer.

2.3.11

Apps you submit for pre-order on the App Store must be complete and deliverable as submitted. Ensure that the app you ultimately release is not materially different from what you advertise while the app is in a pre-order state. If you make material changes to the app (e.g. change business models), you should restart your pre-order sales.

2.3.12

Apps must clearly describe new features and product changes in their "What's New" text. Simple bug fixes, security updates, and performance improvements may rely on a generic description, but more significant changes must be listed in the notes.

•••••

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(3) would interfere with the platform's enforcement of this guideline because certain in-app events may fall within an event type provided in App Store Connect and others may not, which a developer could argue materially harms competition among similarly situated business users.

2.3.13

[In-app events are timely events that happen within your app. To feature your event on the App Store, it must fall within an event type provided in App Store Connect. All event metadata must be accurate and pertain to the event itself, rather than the app more generally. Events must happen at the times and dates you select in App Store Connect, including across multiple storefronts.](#)

[You may monetize your event so long as you follow the rules set forth in Section 3 on Business.](#)

And your event deep link must direct users to the proper destination within your app. Read In-App Events for detailed guidance on acceptable event metadata and event deep links.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) would interfere with enforcement of this guideline because the provision would bar bundling the platform's own in-app payment system with distribution on the platform.

2.4 Hardware Compatibility

2.4.1

To ensure people get the most out of your app, iPhone apps should run on iPad whenever possible. We encourage you to consider building universal apps so customers can use them on all of their devices. Learn more about Universal apps.

2.4.2

Design your app to use power efficiently and be used in a way that does not risk damage to the device.

Apps should not rapidly drain battery, generate excessive heat, or put unnecessary strain on device resources. For example, apps should not encourage placing the device under a mattress or pillow while charging or perform excessive write cycles to the solid state drive. Apps, including any third-party advertisements displayed within them, may not run unrelated background processes, such as cryptocurrency mining.

2.4.3

People should be able to use your Apple TV app without the need for hardware inputs beyond the Siri remote or third-party game controllers, but feel free to provide enhanced functionality when other peripherals are connected. If you require a game controller, make sure you clearly explain that in your metadata so customers know they need additional equipment to play.

2.4.4

Apps should never suggest or require a restart of the device or modifications to system settings unrelated to the core functionality of the app. For example, don't encourage users to turn off Wi-Fi, disable security features, etc.

2.4.5

Apps distributed via the Mac App Store have some additional requirements to keep in mind:

(i) They must be appropriately sandboxed, and follow macOS File System Documentation. They should also only use the appropriate macOS APIs for modifying user data stored by other apps (e.g. bookmarks, Address Book, or Calendar entries).

(ii) They must be packaged and submitted using technologies provided in Xcode; no third-party installers allowed. They must also be self-contained, single app installation bundles and cannot install code or resources in shared locations.

(iii) They may not auto-launch or have other code run automatically at startup or login without consent nor spawn processes that continue to run without consent after a user has quit the app. They should not automatically add icons to the Dock or leave shortcuts on the user desktop.

●....

WHAT WOULD CHANGE

S. 2710, Sec. 3(f) would interfere with the enforcement of this guideline because the provision requires Apple to provide open access to device features, including demands on battery life, to the extent an aggrieved developer could show that similar apps offered by the platform have better access to battery life resources.

S. 2992, Sec. 3(a)(4) would interfere with the enforcement of this guideline because the provision would bar Apple from materially restricting access by a developer to device features, including demands on battery life.

●....

WHAT WOULD CHANGE

S. 2710, Sec. 3(f) would interfere with the enforcement of this guideline because the provision would require Apple to provide access to software and hardware features on equivalent terms as the platform's similar apps and an aggrieved developer may be able to find a platform-provided app with greater access.

Sec. 3(b) would interfere with the enforcement of this guideline because the provision prohibits restrictions on communications with a user concerning a legitimate business offer (in the context of the bill's requirement to allow sideloading, a trial attorney could easily). Interpret encouragement to disable security features as a necessary complement to a legitimate business offer).

(iv) They may not download or install standalone apps, kexts, additional code, or resources to add functionality or significantly change the app from what we see during the review process.

(v) They may not request escalation to root privileges or use setuid attributes.

(vi) They may not present a license screen at launch, require license keys, or implement their own copy protection.

(vii) They must use the Mac App Store to distribute updates; other update mechanisms are not allowed.

(viii) Apps should run on the currently shipping OS and may not use deprecated or optionally installed technologies (e.g. Java) (ix) Apps must contain all language and localization support in a single app bundle.

2.5 Software Requirements

2.5.1

Apps may only use public APIs and must run on the currently shipping OS. Learn more about public APIs. Keep your apps up-to-date and make sure you phase out any deprecated features, frameworks or technologies that will no longer be supported in future versions of an OS. Apps should use APIs and frameworks for their intended purposes and indicate that integration in their app description. For example, the HomeKit framework should provide home automation services; and HealthKit should be used for health and fitness purposes and integrate with the Health app.

2.5.2

Apps should be self-contained in their bundles, and may not read or write data outside the designated container area, nor may they download, install, or execute code which introduces or changes features or functionality of the app, including other apps.

Educational apps designed to teach, develop, or allow students to test executable code.

2.5.3

Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the operating system and/or hardware features, including Push Notifications and Game Center, will be rejected. Egregious violations and repeat behavior will result in removal from the Apple Developer Program.

WHAT WOULD CHANGE

S. 2710, Sec. 3(d)(2) could interfere with the enforcement of this guideline because the provision would require Apple to provide readily accessible means for users of its operating system to install third-party apps or app stores through means other than its app store and this guideline restricts developers' ability to install apps outside the app store.

WHAT WOULD CHANGE

S. 2992 3(a)(4) would interfere with the enforcement of this guideline because the provision would prohibit Apple from materially restricting a business user's access to software features and removing an app for introducing viruses or other code that "disrupts" normal operation of the operating system or hardware features would constitute such a restriction.

Apple could overcome this prohibition on a case-by-case basis via an affirmative defense, but the guideline would be otherwise unenforceable.

2.5.4

Multitasking apps may only use background services for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc. If your app uses location background mode, include a reminder that doing so may dramatically decrease battery life.

2.5.5

Apps must be fully functional on IPv6-only networks.

2.5.6

Apps that browse the web must use the appropriate WebKit framework and WebKit Javascript.

2.5.7

Video streaming content over a cellular network longer than 10 minutes must use HTTP Live Streaming and include a baseline 192 kbps HTTP Live stream.

2.5.8

Apps that create alternate desktop/home screen environments or simulate multi-app widget experiences will be rejected.

2.5.9

[Apps that alter or disable the functions of standard switches, such as the Volume Up/Down and Ring/Silent switches, or other native user interface elements or behaviors will be rejected.](#) For example, apps should not block links out to other apps or other features that users would expect to work a certain way. Learn more about proper handling of links.

2.5.10

Apps should not be submitted with empty ad banners or test advertisements.



WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) could interfere with Apple's enforcement of this guideline because the provision prohibits material restrictions on a business user's access to hardware or software features, which may include altering functions of standard switches like volume, ring, and other native user interface elements.

2.5.11 SiriKit and Shortcuts:

(i) Apps integrating SiriKit and Shortcuts should only sign up for intents they can handle without the support of an additional app and that users would expect from the stated functionality. For example, if your app is a meal planning app, you should not incorporate an intent to start a workout, even if the app shares integration with a fitness app.

(ii) Ensure that the vocabulary and phrases in your plist pertains to your app and the Siri functionality of the intents the app has registered for. [Aliases must relate directly to your app or company name and should not be generic terms or include third-party app names or services.](#) ●.....

(iii) Resolve the Siri request or Shortcut in the most direct way possible and do not insert ads or other marketing between the request and its fulfillment. Only request a disambiguation when required to complete the task (e.g. asking the user to specify a particular type of workout).

2.5.12

Apps using CallKit or including an SMS Fraud Extension should only block phone numbers that are confirmed spam. Apps that include call-, SMS-, and MMS- blocking functionality or spam identification must clearly identify these features in their marketing text and explain the criteria for their blocked and spam lists. You may not use the data accessed via these tools for any purpose not directly related to operating or improving your app or extension (e.g. you may not use, share, or sell it for tracking purposes, creating user profiles, etc.).

2.5.13

Apps using facial recognition for account authentication must use LocalAuthentication (and not ARKit or other facial recognition technology) where possible, and must use an alternate authentication method for users under 13 years old.

2.5.14

Apps must request explicit user consent and provide a clear visual and/or audible indication when recording, logging, or otherwise making a record of user activity. This includes any use of the device camera, microphone, screen recordings, or other user inputs.

2.5.15

[Apps that enable users to view and select files should include items from the Files app and the user's iCloud documents.](#) ●.....

2.5.16

App Clips, widgets, extensions, and notifications should be related to the content and functionality of your app. Additionally, all App Clip features and functionality must be included in the main app binary. App Clips cannot contain advertising.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision bars restrictions on communications concerning "legitimate business offers," which an aggrieved developer could interpret to include using a third-party app name or services as an alias in Shortcuts or SiriKit.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1) would interfere with this guideline because the provision bars preferring Apple's own services over those of another business user, which may include requiring the Files app and iCloud to appear in prompts to select files.

BUSINESS

.....

There are many ways to monetize your app on the App Store. If your business model isn't obvious, make sure to explain in its metadata and App Review notes. If we can't understand how your app works or your in-app purchases aren't immediately obvious, it will delay your review and may trigger a rejection. And while pricing is up to you, [we won't distribute apps and in-app purchase items that are clear rip-offs. We'll reject expensive apps that try to cheat users with irrationally high prices.](#)

.....

If we find that you have attempted to manipulate reviews, inflate your chart rankings with paid, incentivized, filtered, or fake feedback, or engage with third-party services to do so on your behalf, we will take steps to preserve the integrity of the App Store, which may include expelling you from the Apple Developer Program.

3.1 Payments

3.1.1 In-App Purchase:

[If you want to unlock features or functionality within your app, \(by way of example: subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version\), you must use in-app purchase. Apps may not use their own mechanisms to unlock content or functionality, such as license keys, augmented reality markers, QR codes, etc. Apps and their metadata may not include buttons, external links, or other calls to action that direct customers to purchasing mechanisms other than in-app purchase.](#) Apps may use in-app purchase currencies to enable customers to "tip" the developer or digital content providers in the app.

.....

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision bars restrictions on communications concerning legitimate business offers, and an aggrieved developer could argue that a price Apple determines to be "clear rip-offs" is nonetheless a "legitimate business offer."

S.2992, Sec. 3(a)(3) would interfere with the enforcement of this guideline as well because the provisions would bar discrimination in the application of guideline among similarly situated business users and a trial attorney could interpret the decision to remove or reject an app on this basis as discriminatory.

Sec. 3(a)(4) would also interfere with the enforcement of this guideline because the provision would prohibit material restrictions on the capacity of a business user to access software features that are available to offerings of the platform that would compete with the business user and trial attorney could use this as a hook to challenge a decision to reject based on an app's high price.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) would interfere with the enforcement of this guideline because the provision prohibits Apple from requiring developers to use its own in-app payment system.

S. 2992, Sec. 3(a)(5) could interfere with this guideline because it prohibits conditioning access to the covered platform on the purchase or use of other services that are "not part of or intrinsic to" the covered platform and payment processing may be interpreted as "not part of or intrinsic to" the platform.

Digital gift cards, certificates, vouchers, and coupons which can be redeemed for digital goods or services can only be sold in your app using in-app purchase. Physical gift cards that are sold within an app and then mailed to customers may use payment methods other than in-app purchase.

Non-subscription apps may offer a free time-based trial period before presenting a full unlock option by setting up a Non-Consumable IAP item at Price Tier 0 that follows the naming convention: "XX-day Trial."

Prior to the start of the trial, your app must clearly identify its duration, the content or services that will no longer be accessible when the trial ends, and any downstream charges the user would need to pay for full functionality.

Learn more about managing content access and the duration of the trial period using Receipts and Device Check.

3.1.2 Subscriptions:

Apps may offer auto-renewing in-app purchase subscriptions, regardless of category on the App Store. When incorporating auto-renewable subscriptions into your app, be sure to follow the guidelines below.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision prohibits restrictions on developer communications concerning legitimate business offers, and a trial attorney could interpret disclosure requirements regarding free trials as a restriction on communications concerning legitimate business offers.

...
...

Apps may use in-app purchase currencies to enable customers to “tip” the developer or digital content providers in the app.

Any credits or in-game currencies purchased via in-app purchase may not expire, and you should make sure you have a restore mechanism for any restorable in-app purchases.

Apps may enable gifting of items that are eligible for in-app purchase to others. Such gifts may only be refunded to the original purchaser and may not be exchanged.

Apps distributed via the Mac App Store may host plug-ins or extensions that are enabled with mechanisms other than the App Store.

Apps offering “loot boxes” or other mechanisms that provide randomized virtual items for purchase must disclose the odds of receiving each type of item to customers prior to purchase.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) would interfere with the enforcement of this guideline because the provision prohibits Apple from requiring developers to use its own in-app payment system.

S. 2992, Sec. 3(a)(5) could interfere with this guideline because it prohibits conditioning access to the covered platform on the purchase or use of other services that are “not part of or intrinsic to” the platform.

WHAT WOULD CHANGE

S. 2710, Sec. 3(1) would interfere with the enforcement of this guideline because the provision prohibits requiring developers to use the platform’s own payment system, limiting the platform’s ability to impose restrictions on payment processing, including a prohibition on the exchange of gifted items.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision would prohibit Apple from restricting communications of developers concerning “legitimate business offers” and a trial attorney could interpret a requirement to disclose the odds of receiving certain items in a loot box as restricting its communication concerning a legitimate business offer.

3.1.2(a) Permissible uses: If you offer an auto-renewing subscription, you must provide ongoing value to the customer, and the subscription period must last at least seven days and be available across all of the user's devices. While the following list is not exhaustive, examples of appropriate subscriptions include: new game levels; episodic content; multiplayer support; apps that offer consistent, substantive updates; access to large collections of, or continually updated, media content; software as a service ("SAAS"); and cloud support.

In addition:

- Subscriptions may be offered alongside à la carte offerings (e.g. you may offer a subscription to an entire library of films as well the purchase or rental of a single movie).
- You may offer a single subscription that is shared across your own apps and services.
- Games offered in a streaming game service subscription may offer a single subscription that is shared across third-party apps and services; however, they must be downloaded directly from the App Store, must be designed to avoid duplicate payment by a subscriber, and should not disadvantage non-subscriber customers.
- Subscriptions must work on all of the user's devices where the app is available. Learn more about sharing a subscription across your apps.
- Apps must not force users to rate the app, review the app, download other apps, or other similar actions in order to access functionality, content, or use of the app.
- As with all apps, those offering subscriptions should allow a user to get what they've paid for without performing additional tasks, such as posting on social media, uploading contacts, checking in to the app a certain number of times, etc.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline because the provision prohibits restrictions on developer communications concerning legitimate business offers and a subscription period for in-app purchases that auto-renew after less than seven days may qualify as a legitimate communication.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

- Subscriptions may include consumable credits, gems, in-game currencies, etc., and you may offer subscriptions that include access to discounted consumable goods (e.g. a platinum membership that exposes gem-packs for a reduced price).
- If you are changing your existing app to a subscription-based business model, you should not take away the primary functionality existing users have already paid for. For example, let customers who have already purchased a "full game unlock" continue to access the full game after you introduce a subscription model for new customers.
- Auto-renewing subscription apps may offer a free trial period to customers by providing the relevant information set forth in App Store Connect. Learn more about Subscription Free Trials.
- Apps that attempt to scam users will be removed from the App Store. This includes apps that attempt to trick users into purchasing a subscription under false pretenses to engage in bait-and-switch and scam practices; these will be removed from the App Store and you may be removed from the Apple Developer Program.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

- Cellular carrier apps may include auto-renewing music and video subscriptions in predefined bundles with cellular data plans, with prior approval by Apple. Other autorenewing subscriptions may also be included in pre-defined bundles with cellular dataplans, with prior approval by Apple, if the cellular carrier apps support in-app purchase for new users and the carrier provides a mechanism for customers to revert to in-app purchase upon termination of the customer's bundled service. Such subscriptions cannot include access to or discounts on consumable items.

3.1.2(b) Upgrades and Downgrades:

Users should have a seamless upgrade/downgrade experience and should not be able to inadvertently subscribe to multiple variations of the same thing. Review best practices on managing your subscription upgrade and downgrade options.

3.1.2(c) Subscription Information:

Before asking a customer to subscribe, you should clearly describe what the user will get for the price. How many issues per month? How much cloud storage? What kind of access to your service? Ensure you clearly communicate the requirements described in Schedule 2 of the Apple Developer Program License Agreement, found in Agreements, Tax, and Banking.

3.1.3 Other Purchase Methods:

The following apps may use purchase methods other than in-app purchase.

3.1.3(a) "Reader" Apps: Apps may allow a user to access previously purchased content or content subscriptions (specifically: magazines, newspapers, books, audio, music, and Reader apps may offer account creation for free tiers, and account management functionality for existing customers.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4)-(5) may come into play here if developers can argue that the restrictions on bundles are reducing access to the platform.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with Apple's ability to enforce this consumer protection. This guideline could be interpreted as infringing on a legitimate business communication.

3.1.3(b) Multiplatform Services: Apps that operate across multiple platforms may allow users to access content, subscriptions, or features they have acquired in your app on other platforms or your web site, including consumable items in multi-platform games, provided those items are also available as in-app purchases within the app.

3.1.3(c) Enterprise Services: If your app is only sold directly by you to organizations or groups for their employees or students (for example professional databases and classroom management tools), you may allow enterprise users to access previously-purchased content or subscriptions. Consumer, single user, or family sales must use in-app purchase.

3.1.3(d) Person-to-Person Services: If your app enables the purchase of real-time person-to-person services between two individuals (for example tutoring students, medical consultations, real estate tours, or fitness training), you may use purchase methods other than in-app purchase to collect those payments. One-to-few and one-to-many real-time services must use in-app purchase.

3.1.3(e) Goods and Services Outside of the App: If your app enables people to purchase physical goods or services that will be consumed outside of the app, you must use purchase methods other than in-app purchase to collect those payments, such as Apple Pay or traditional credit card entry.

3.1.3(f) Free Stand-alone Apps: Free apps acting as a stand-alone companion to a paid web based tool (eg. VOIP, Cloud Storage, Email Services, Web Hosting) do not need to use in-app purchase, provided there is no purchasing inside the app, or calls to action for purchase outside of the app.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) would interfere with the enforcement of this guideline because the provision would bar Apple from requiring game developers to maintain an option to purchase consumables through Apple's own payment processing system.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) would interfere with the enforcement of this guideline because the provision would bar Apple from requiring consumers, single users, or family sales to use Apple's own payment processing system.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1) and Sec. 3(a)(3) - these two sections put together would seem to eliminate Apple's ability to enforce this guideline, since Apple would not be able to "take punitive action or otherwise impose less favorable terms and conditions" when a developer offers different "conditions of sale" through another in-app payment processor.

3.1.4 Hardware-Specific Content:

In limited circumstances, such as when features are dependent upon specific hardware to function, the app may unlock that functionality without using in-app purchase (e.g. an astronomy app that adds features when synced with a telescope). [App features that work in combination with an approved physical product \(such as a toy\) on an optional basis may unlock functionality without using in-app purchase, provided that an in-app purchase option is available as well.](#) You may not, however, require users to purchase unrelated products or engage in advertising or marketing activities to unlock app functionality.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

3.1.5 Cryptocurrencies:

- (i) [Wallets: Apps may facilitate virtual currency storage, provided they are offered by developers enrolled as an organization.](#)
- (ii) [Mining: Apps may not mine for cryptocurrencies unless the processing is performed off device \(e.g. cloud-based mining\).](#)
- (iii) [Exchanges: Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered by the exchange itself.](#)
- (iv) Initial Coin Offerings: Apps facilitating Initial Coin Offerings ("ICOs"), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law.
- (v) [Cryptocurrency apps may not offer currency for completing tasks, such as downloading other apps, encouraging other users to download, posting to social networks, etc.](#)

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce these consumer protections.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(d) would interfere with Apple's ability to enforce this consumer protection.

3.1.6 Apple Pay:

Apps using Apple Pay must provide all material purchase information to the user prior to sale of any good or service and must use Apple Pay branding and user interface elements correctly, as described in the Apple Pay Marketing Guidelines and Human Interface Guidelines. Apps using Apple Pay to offer recurring payments must, at a minimum, disclose the following information:

- The length of the renewal term and the fact that it will continue until canceled
- What will be provided during each period
- The actual charges that will be billed to the customer
- How to cancel

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(b) and (d) would interfere with Apple's ability to enforce this consumer protection.

3.1.7 Advertising:

Display advertising should be limited to your main app binary, and should not be included in extensions, App Clips, widgets, notifications, keyboards, watchOS apps, etc. Ads displayed in an app must be appropriate for the app's age rating, allow the user to see all information used to target them for that ad (without requiring the user to leave the app), and may not engage in targeted or behavioral advertising based on sensitive user data such as health/medical data (e.g. from the HealthKit APIs), school and classroom data (e.g. from ClassKit), or from kids (e.g. from apps in the Kids Category), etc. Interstitial ads or ads that interrupt or block the user experience must clearly indicate that they are an ad, must not manipulate or trick users into tapping into them, and must provide easily accessible and visible close/skip buttons large enough for people to easily dismiss the ad.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and S. 2710, Sec. 3(b) and (d) would interfere with Apple's ability to enforce this consumer protection.

3.2 Other Business Model Issues

The lists below are not exhaustive, and your submission may trigger a change or update to our policies, but here are some additional dos and don'ts to keep in mind:

3.2.1 Acceptable

- (i) Displaying your own apps for purchase or promotion within your app, provided the app is not merely a catalog of your apps.
- (ii) Displaying or recommending a collection of third-party apps that are designed for a specific approved need (e.g. health management, aviation, accessibility). Your app should provide robust editorial content so that it doesn't seem like a mere storefront.
- (iii) Disabling access to specific approved rental content (e.g. films, television programs, music, books) after the rental period has expired; all other items and services may not expire.
- (iv) Wallet passes can be used to make or receive payments, transmit offers, or offer identification (such as movie tickets, coupons, and VIP credentials). Other uses may result in the rejection of the app and the revocation of Wallet credentials.
- (v) Insurance apps must be free, in legal compliance in the regions distributed, and cannot use in-app purchase.
- (vi) Approved nonprofits may fundraise directly within their own apps or third-party apps, provided those fundraising campaigns adhere to all App Review Guidelines and offer Apple Pay support. These apps must disclose how the funds will be used, abide by all required local and federal laws, and ensure appropriate tax receipts are available to donors. Additional information shall be provided to App Review upon request. Nonprofit platforms that connect donors to other nonprofits must ensure that every nonprofit listed in the app has also gone through the nonprofit approval process. Learn more about becoming an approved nonprofit.
- (vii) Apps may enable individual users to give a monetary gift to another individual without using in-app purchase, provided that (a) the gift is a completely optional choice by the giver, and (b) 100% of the funds go to the receiver of the gift. However, a gift that is connected to or associated at any point in time with receiving digital content or services must use in-app purchase.
- (viii) Apps used for financial trading, investing, or money management should be submitted by the financial institution performing such services.

3.2.2 Unacceptable

- (i) Creating an interface for displaying third-party apps, extensions, or plug-ins similar to the App Store or as a general-interest collection.
- (ii) Monetizing built-in capabilities provided by the hardware or operating system, such as Push Notifications, the camera, or the gyroscope; or Apple services, such as Apple Music access or iCloud storage.
- (iii) Artificially increasing the number of impressions or click-throughs of ads, as well as apps that are designed predominantly for the display of ads.
- (iv) Unless you are an approved nonprofit or otherwise permitted under Section 3.2.1
- (vi) above, collecting funds within the app for charities and fundraisers. Apps that seek to raise money for such causes must be free on the App Store and may only collect funds outside of the app, such as via Safari or SMS. ●.....
- (v) Arbitrarily restricting who may use the app, such as by location or carrier.
- (vi) Apps should allow a user to get what they've paid for without performing additional tasks, such as posting on social media, uploading contacts, checking in to the app a certain number of times, etc.

Apps should not require users to rate the app, review the app, watch videos, download other apps, tap on advertisements, enable tracking, or take other similar actions in order to access functionality, content, use the app, or receive monetary or other compensation, including but not limited to gift cards and codes.

- (vii) Artificially manipulating a user's visibility, status, or rank on other services unless permitted by that service's Terms and Conditions.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2), (3), and (4) and S. 2710, Sec. 3(b), (d), and (f) would interfere with Apple's ability to enforce this consumer protection.

(vii) Artificially manipulating a user's visibility, status, or rank on other services unless permitted by that service's Terms and Conditions.

(viii) Apps that facilitate binary options trading are not permitted on the App Store. Consider a web app instead. Apps that facilitate trading in contracts for difference ("CFDs") or other derivatives (e.g. FOREX) must be properly licensed in all jurisdictions where the service is available.

(ix) Apps offering personal loans must clearly and conspicuously disclose all loan terms, including but not limited to equivalent maximum Annual Percentage Rate (APR) and payment due date. Apps may not charge a maximum APR higher than 36%, including costs and fees, and may not require repayment in full in 60 days or less.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2), (3), and (4) and S. 2710, Sec. 3(b), (d), and (f) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2) and (3) and S. 2710, Sec. 3(b) and (d) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2710, Sec. 3 (b) would come into play, so long as developers can argue that their communications with app users were "legitimate."

DESIGN

.....

Apple customers place a high value on products that are simple, refined, innovative, and easy to use, and that's what we want to see on the App Store. Coming up with a great design is up to you, but the following are minimum standards for approval to the App Store. And remember that even after your app has been approved, you should update your app to ensure it remains functional and engaging to new and existing customers. Apps that stop working or offer a degraded experience may be removed from the App Store at any time.

4.1 Copycats

●

Come up with your own ideas. We know you have them, so make yours come to life. Don't simply copy the latest popular app on the App Store, or make some minor changes to another app's name or UI and pass it off as your own. In addition to risking an intellectual property infringement claim, it makes the App Store harder to navigate and just isn't fair to your fellow developers.

4.2 Minimum Functionality

Your app should include features, content, and UI that elevate it beyond a repackaged website. If your app is not particularly useful, unique, or "app-like," it doesn't belong on the App Store. If your App doesn't provide some sort of lasting entertainment value or adequate utility, it may not be accepted. Apps that are simply a song or movie should be submitted to the iTunes Store. Apps that are simply a book or game guide should be submitted to the Apple Books Store.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2), (3), and (4) and S. 2710, Sec. 3(b), (d), and (f) would interfere with Apple's ability to enforce this consumer protection.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1) – (4) and S. 2710, Sec. 3(d) and (f) would interfere with the enforcement of this consumer protection.

4.2.1

Apps using ARKit should provide rich and integrated augmented reality experiences; merely dropping a model into an AR view or replaying animation is not enough.

4.2.2

Other than catalogs, apps shouldn't primarily be marketing materials, advertisements, web clippings, content aggregators, or a collection of links.

4.2.3

(i) Your app should work on its own without requiring installation of another app to function.

(ii) Make sure you include sufficient content in the binary for the app to function at launch

(iii) If your app needs to download additional resources in order to function on initial launch, disclose the size of the download and prompt users before doing so.

4.2.4

Apple Watch apps that appear to be a watch face are confusing, because people will expect them to work with device features such as swipes, notifications, and third-party complications. Creative ways of expressing time as an app interface is great (say, a tide clock for surfers), but if your app comes too close to resembling a watch face, we will reject it.

4.2.5

Apps that are primarily iCloud and iCloud Drive file managers need to include additional app functionality to be approved.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) would interfere with the enforcement of this guideline, because the provision would prohibit Apple from restricting developer communications concerning a "legitimate business offer" and a trial attorney could claim that marketing materials, advertisements, and collections of links are legitimate business offers, even if an app has no other purpose.

WHAT WOULD CHANGE

S. 2710, Sec. 3(d)(2) provides that app developers should be allowed to install apps through means other than the app store, which could ostensibly include a multi-app download process executed through a third-party app store.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1) could come into play if developers argue that a prohibition on confusing watch faces is self-preferential toward the native Apple Watch design.

WHAT WOULD CHANGE

S. 2710, Sec. 3(f)/ S.2992, Sec. 3(a)(4) may come into play because they require platforms to provide the same hardware and software features to developers that they provide to their own products.

S. 2992, Sec. 3(a)(1) could come into play if developers argue that this prohibition favors Apple's own file managing apps.

4.2.6

Apps created from a commercialized template or app generation service will be rejected unless they are submitted directly by the provider of the app's content. These services should not submit apps on behalf of their clients and should offer tools that let their clients create customized, innovative apps that provide unique customer experiences.

Another acceptable option for template providers is to create a single binary to host all client content in an aggregated or "picker" model, for example as a restaurant finder app with separate customized entries or pages for each client restaurant, or as an event app with separate entries for each client event.

4.2.7

Remote Desktop Clients: If your remote desktop app acts as a mirror of specific software or services rather than a generic mirror of the host device, it must comply with the following:

- (a) The app must only connect to a user-owned host device that is a personal computer or dedicated game console owned by the user, and both the host device and client must be connected on a local and LAN-based network.
- (b) Any software or services appearing in the client are fully executed on the host device, rendered on the screen of the host device, and may not use APIs or platform features beyond what is required to stream the Remote Desktop.
- (c) All account creation and management must be initiated from the host device.
- (d) The UI appearing on the client does not resemble an iOS or App Store view, does not provide a store-like interface, or include the ability to browse, select, or purchase software not already owned or licensed by the user. For the sake of clarity, transactions taking place within mirrored software do not need to use in-app purchase, provided the transactions are processed on the host device.
- (e) Thin clients for cloud-based apps are not appropriate for the App Store.

4.3 Spam

Don't create multiple Bundle IDs of the same app. If your app has different versions for specific locations, sports teams, universities, etc., consider submitting a single app and provide the variations using in-app purchase. [Also avoid piling on to a category that is already saturated; the App Store has enough fart, burp, flashlight, fortune telling, dating, drinking games, and Kama Sutra apps, etc. already.](#) We will reject these apps unless they provide a unique, high-quality experience. Spamming the store may lead to your removal from the Apple Developer Program.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1-4) would interfere with Apple's enforcement of this guideline because a determination that the market for a certain type of app is saturated could be argued to be discriminatory.

4.4 Extensions

Apps hosting or containing extensions must comply with the App Extension Programming Guide or the Safari App Extensions Guide and should include some functionality, such as help screens and settings interfaces where possible. [You should clearly and accurately disclose what extensions are made available in the app's marketing text and the extensions may not include marketing, advertising, or in-app purchases.](#)

4.4.1

[Keyboard extensions have some additional rules.](#)

They must:

- Provide keyboard input functionality (e.g. typed characters);
- Follow Sticker guidelines if the keyboard includes images or emoji;
- Provide a method for progressing to the next keyboard;
- Remain functional without full network access and without requiring full access;
- Collect user activity only to enhance the functionality of the user's keyboard extension on the iOS device.

They must not:

- Launch other apps besides Settings; or
- Repurpose keyboard buttons for other behaviors (e.g. holding down the "return" key to launch the camera).

4.4.2

Safari extensions must run on the current version of Safari on macOS. [They may not interfere with System or Safari UI elements and must never include malicious or misleading content or code.](#) Violating this rule will lead to removal from the Apple Developer Program. Safari extensions should not claim access to more websites than strictly necessary to function.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(3) likely prevents punitive action based on the existence of in-app purchases if the developer uses a third-party payment processor.

S. 2710, Sec. 3(b) prevents the disruption of "legitimate business communications".

WHAT WOULD CHANGE

S. 2710, Sec. 3(f) and S. 2992, Sec. 3(a)(4) would interfere with the enforcement of these guidelines because those provisions would prohibit restrictions on access to software features, and it could be argued that any of these guardrails on the characteristics of keyboard extensions constitute such restrictions.

S. 2992, Sec. 3(a)(7) would also interfere with Apple's enforcement of this guideline because the provision would bar Apple from restricting an app's access to user activity.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2) - a prohibition on extensions blocking UI elements could be argued to be discriminatory, especially insofar as the UI elements in question are not central to the functioning of the browser.

Apple may need to rely on the affirmative defense to overcome S. 2992, Sec. 3(a)(4) here.

4.4.3 Stickers

Stickers are a great way to make Messages more dynamic and fun, letting people express themselves in clever, funny, meaningful ways. Whether your app contains a sticker extension or you're creating free-standing sticker packs, its content shouldn't offend users, create a negative experience, or violate the law.

(i) In general, if it wouldn't be suitable for the App Store, it doesn't belong in a sticker.

(ii) Consider regional sensitivities, and do not make your sticker pack available in a country where it could be poorly received or violate local law.

(iii) If we don't understand what your stickers mean, include a clear explanation in your review notes to avoid any delays in the review process.

(iv) Ensure your stickers have relevance beyond your friends and family; they should not be specific to personal events, groups, or relationships.

(v) You must have all the necessary copyright, trademark, publicity rights, and permissions for the content in your stickers, and shouldn't submit anything unless you're authorized to do so. Keep in mind that you must be able to provide verifiable documentation upon request. Apps with sticker content you don't have rights to use will be removed from the App Store and repeat offenders will be removed from the Apple Developer Program. If you believe your content has been infringed by another provider, submit a claim here.

4.5 Apple Sites and Services

4.5.1

Apps may use approved Apple RSS feeds such as the iTunes Store RSS feed, but may not scrape any information from Apple sites (e.g. apple.com, the iTunes Store, App Store, App Store Connect, developer portal, etc.) or create rankings using this information.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1) – (4) would interfere with the enforcement of this guideline because Apple's interpretation of what constitutes "suitable for the App Store" could be challenged as discriminatory.

4.5.2 Apple Music

(i) MusicKit on iOS lets users play Apple Music and their local music library natively from your apps and games. When a user provides permission to their Apple Music account, your app can create playlists, add songs to their library, and play any of the millions of songs in the Apple Music catalog. Users must initiate the playback of an Apple Music stream and be able to navigate using standard media controls such as "play," "pause," and "skip." Moreover, your app may not require payment or indirectly monetize access to the Apple Music service (e.g. in-app purchase, advertising, requesting user info, etc.). Do not download, upload, or enable sharing of music files sourced from the MusicKit APIs, except as explicitly permitted in MusicKit documentation.

(ii) Using the MusicKit APIs is not a replacement for securing the licenses you might need for a deeper or more complex music integration. For example, if you want your app to play a specific song at a particular moment, or to create audio or video files that can be shared to social media, you'll need to contact rights-holders directly to get their permission (e.g. synchronization or adaptation rights) and assets. Cover art and other metadata may only be used in connection with music playback or playlists (including App Store screenshots displaying your app's functionality), and should not be used in any marketing or advertising without getting specific authorization from rights-holders. Make sure to follow the Apple Music Identity Guidelines when integrating Apple Music services in your app.

(iii) Apps that access Apple Music user data, such as playlists and favorites, must clearly disclose this access in the purpose string. Any data collected may not be shared with third parties for any purpose other than supporting or improving the app experience. This data may not be used to identify users or devices, or to target advertising.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b) and 3(f), and S. 2992, Sec. 3(a)(2) and (4) would interfere with the enforcement of this quality measure.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2), (3), and (4), and S. 2710, Sec. 3(d) and (f) would interfere with the enforcement of this consumer protection.

4.5.3

Do not use Apple Services to spam, phish, or send unsolicited messages to customers, including Game Center, Push Notifications, etc. Do not attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, aliases, or other information obtained through Game Center, or you will be removed from the Apple Developer Program.

4.5.4

Push Notifications must not be required for the app to function, and should not be used to send sensitive personal or confidential information. [Push Notifications should not be used for promotions or direct marketing purposes unless customers have explicitly opted in to receive them via consent language displayed in your app's UI, and you provide a method in your app for a user to opt out from receiving such messages.](#) Abuse of these services may result in revocation of your privileges.

WHAT WOULD CHANGE

S. 2710, Sec. 3(b). Platform is allowed to offer users ability to consent, but can they mandate it?

4.5.5

Only use Game Center Player IDs in a manner approved by the Game Center terms and do not display them in the app or to any third party. 4.5.6 Apps may use Unicode characters that render as Apple emoji in their app and app metadata. Apple emoji may not be used on other platforms or embedded directly in your app binary.

4.6 Alternate App Icons

Apps may display customized icons, for example, to reflect a sports team preference, provided that each change is initiated by the user and the app includes settings to revert to the original icon. All icon variants must relate to the content of the app and changes should be consistent across all system assets, so that the icons displayed in Settings, Notifications, etc. match the new springboard icon. This feature may not be used for dynamic, automatic, or serial changes, such as to reflect up-to-date weather information, calendar notifications, etc.

4.7 HTML5 Games, Bots, etc

Apps may contain or run code that is not embedded in the binary (e.g. HTML5-based games, bots, etc.), as long as code distribution isn't the main purpose of the app, the code is not offered in a store or store-like interface, and provided that the software adheres to the additional rules that follow in 4.7.1 and 4.7.2. These additional rules are important to preserve the experience that App Store customers expect, and to help ensure user safety.

4.7.1

Software offered under this rule must:

be free or purchased using in-app purchase;
only use capabilities available in a standard
WebKit view (e.g. it must open and run natively in Safari
without modifications or additional software);
and use WebKit and JavaScript Core to run third-party software
and should not attempt to extend or expose native platform APIs
to third-party software; be offered by developers that have joined
the Apple Developer Program and signed the Apple Developer
Program License Agreement; not provide access to real money ●...
gaming, lotteries, or charitable donations; adhere to the terms of
these App Store Review Guidelines (e.g. do not include objectionable
content); and not offer digital goods or services for sale.

4.7.2

Upon request, you must provide an index of software and metadata available in your app. It must include Apple Developer Program Team IDs for the providers of the software along with a URL which App Review can use to confirm that the software complies with the requirements above.

4.8 Sign in with Apple

Apps that use a third-party or social login service (such as
Facebook Login, Google Sign-In, Sign in with Twitter, Sign In with ●...
LinkedIn, Login with Amazon, or WeChat Login) to set up or
authenticate the user's primary account with the app must also
offer Sign in with Apple as an equivalent option. A user's primary account is the account they establish with your app for the purposes of identifying themselves, signing in, and accessing your features and associated services.

Sign in with Apple is not required if:

Your app exclusively uses your company's own account setup and sign-in systems. Your app is an education, enterprise, or business app that requires the user to sign in with an existing education or enterprise account. Your app uses a government or industry-backed citizen identification system or electronic ID to authenticate users.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(3) and 3(f), and S. 2992, Sec. 3(a)(2) and (4) would interfere with the enforcement of this guideline because the provisions would prohibit Apple from limiting access to operating system, software, or device features by an app maker, and a requirement to join the Apple Developer Program, although doing so is a baseline quality and consumer protection measure, could be interpreted as imposing such restrictions.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(1) would likely interfere with the enforcement of this guideline because the provision would prohibit Apple from self-preferencing, and although requiring certain apps to offer "sign in with Apple" could benefit consumers, it could also be construed as prohibited self-preferencing.

4.9 Streaming games

Streaming games are permitted so long as they adhere to all guidelines—for example, each game update must be submitted for review, developers must provide appropriate metadata for search, [games must use in-app purchase to unlock features or functionality, etc.](#) Of course, there is always the open Internet and web browser apps to reach all users outside of the App Store.

4.9.1

Each streaming game must be submitted to the App Store as an individual app so that it has an App Store product page, appears in charts and search, has user ratings and review, can be managed with ScreenTime and other parental control apps, appears on the user's device, etc.

4.9.2

[Streaming game services may offer a catalog app on the App Store to help users sign up for the service and find the games on the App Store, provided that the app adheres to all guidelines, including offering users the option to pay for a subscription with in-app purchase and use Sign in with Apple. All the games included in the catalog app must link to an individual App Store product page.](#)

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1-3). Existence of in-app purchase cannot be used to condition distribution.

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(1-3). Existence of in-app purchase cannot be used to condition distribution. S. 2992, Sec. 3(a)(1-3). Requirement to use Sign in with Apple could be deemed self-preferencing.

LEGAL

Apps must comply with all legal requirements in any location where you make them available (if you're not sure, check with a lawyer). We know this stuff is complicated, but it is your responsibility to understand and make sure your app conforms with all local laws, not just the guidelines below. And of course, apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected. In extreme cases, such as apps that are found to facilitate human trafficking and/or the exploitation of children, appropriate authorities will be notified.

5.1 Privacy

Protecting user privacy is paramount in the Apple ecosystem, and you should use care when handling personal data to ensure you've complied with privacy best practices, applicable laws, and the terms of the Apple Developer Program License Agreement, not to mention customer expectations. More particularly:

5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly: Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data. Confirm that any third party with whom an app shares user data (in compliance with these Guidelines)—such as analytics tools, advertising networks and third-party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data—will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines. Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

(ii) Permission: Apps that collect user or usage data must secure user consent for the collection, even if such data is considered to be anonymous at the time of or immediately following collection. Paid functionality must not be dependent on or require a user to grant access to this data. Apps must also provide the customer with an easily accessible and understandable way to withdraw consent. Ensure your purpose strings clearly and completely describe your use of the data. Apps that collect data for a legitimate interest without consent by relying on the terms of the European Union's General Data Protection Regulation ("GDPR") or similar statute must comply with all terms of that law. Learn more about Requesting Permission.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2), (4), and (7), and S. 2710, Sec. 3(b), (d), and (f) would all interfere with the enforcement of these consumer protection measures because they would prohibit Apple's restrictions on communicating with consumers, access to personal data, distribution through the App Store, and access to software and device features.

Under S. 2710, a developer could challenge requirements to maintain baseline privacy practices as restricting their access to the platform, and under S. 2992, an enforcer could also interpret requirements to maintain baseline privacy protections as restrictions on access to the platform or personal data. The conflict would arise if Apple decided to enforce the guidelines by removing an app for noncompliance—for example, if the app disrespected user privacy by sharing personal data in a manner inconsistent with its privacy policy. Apple would only be able to maintain these guidelines in fact-specific circumstances if it were sued as a result of removing or rejecting an app for privacy purposes; and then successfully offered a very narrow affirmative defense to preserve the privacy guideline's application in that specific situation.

(iii) Data Minimization: Apps should only request access to data relevant to the core functionality of the app and should only collect and use data that is required to

(iv) Access: Apps must respect the user's permission settings and not attempt to manipulate, trick, or force people to consent to unnecessary data access. For example, apps that include the ability to post photos to a social network must not also require microphone access before allowing the user to upload photos. Where possible, provide alternative solutions for users who don't grant consent. For example, if a user declines to share Location, offer the ability to manually enter an address.

(v) Account Sign-In: If your app doesn't include significant account-based features, let people use it without a login. If your app supports account creation, you must also offer account deletion within the app. Apps may not require users to enter personal information to function, except when directly relevant to the core functionality of the app or required by law. If your core app functionality is not related to a specific social network (e.g. Facebook, WeChat, Weibo, Twitter, etc.), you must provide access without a login or via another mechanism. Pulling basic profile information, sharing to the social network, or inviting friends to use the app are not considered core app functionality. The app must also include a mechanism to revoke social network credentials and disable data access between the app and social network from within the app. An app may not store credentials or tokens to social networks off of the device and may only use such credentials or tokens to directly connect to the social network from the app itself while the app is in use.

(vi) Developers that use their apps to surreptitiously discover passwords or other private data will be removed from the Apple Developer Program.

(vii) [SafariViewController must be used to visibly present information to users; the controller may not be hidden or obscured by other views or layers. Additionally, an app may not use SafariViewController to track users without their knowledge and consent.](#)

.....

WHAT WOULD CHANGE

See reasoning above.

(viii) Apps that compile personal information from any source that is not directly from the user or without the user's explicit consent, even public databases, are not permitted on the App Store.

(ix) Apps that provide services in highly-regulated fields (such as banking and financial services, healthcare, gambling, legal cannabis use, and air travel) or that require sensitive user information should be submitted by a legal entity that provides the services, and not by an individual developer. Apps that facilitate the legal sale of cannabis must be geo-restricted to the corresponding legal jurisdiction.

(x) Apps may request basic contact information (such as name and email address) so long as the request is optional for the user, features and services are not conditional on providing the information, and it complies with all other provisions of these guidelines, including limitations on collecting information from kids.

5.1.2 Data Use and Sharing

(i) Unless otherwise permitted by law, you may not use, transmit, or share someone's personal data without first obtaining their permission. You must provide access to information about how and where the data will be used. [Data collected from apps may only be shared with third parties to improve the app or serve advertising \(in compliance with the Apple Developer Program License Agreement\).](#)

[You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity.](#)

Learn more about tracking. Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program.

WHAT WOULD CHANGE

See reasoning above.

WHAT WOULD CHANGE

See reasoning above.

(ii) Data collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law.

(iii) Apps should not attempt to surreptitiously build a user profile based on collected data and may not attempt, facilitate, or encourage others to identify anonymous users or reconstruct user profiles based on data collected from Apple-provided APIs or any data that you say has been collected in an “anonymized,” “aggregated,” or otherwise non-identifiable way.

(iv) [Do not use information from Contacts, Photos, or other APIs that access user data to build a contact database for your own use or for sale/distribution to third parties, and don't collect information about which other apps are installed on a user's device for the purposes of analytics or advertising/marketing.](#)

(v) [Do not contact people using information collected via a user's Contacts or Photos, except at the explicit initiative of that user on an individualized basis;](#) do not include a Select All option or default the selection of all contacts. You must provide the user with a clear description of how the message will appear to the recipient before sending it (e.g. What will the message say? Who will appear to be the sender?).

(vi) [Data gathered from the HomeKit API, HealthKit, Clinical Health Records API, MovementDisorder APIs, ClassKit or from depth and/or facial mapping tools \(e.g. ARKit, Camera APIs, or Photo APIs\) may not be used for marketing,](#) advertising or use-based data mining, including by third parties. Learn more about best practices for implementing CallKit, HealthKit, ClassKit, and ARKit.

(vii) Apps using Apple Pay may only share user data acquired via Apple Pay with third parties to facilitate or improve delivery of goods and services.

WHAT WOULD CHANGE

See reasoning above.

WHAT WOULD CHANGE

See reasoning above.

WHAT WOULD CHANGE

See reasoning above.

5.1.3 Health and Health Research

Health, fitness, and medical data are especially sensitive and apps in this space have some additional rules to make sure customer privacy is protected:

- (i) Apps may not use or disclose to third parties data gathered in the health, fitness, and medical research context—including from the Clinical Health Records API, HealthKit API, Motion and Fitness, MovementDisorderAPIs, or health-related human subject research—for advertising, marketing, or other use-based data mining purposes other than improving health management, or for the purpose of health research, and then only with permission. Apps may, however, use a user's health or fitness data to provide a benefit directly to that user (such as a reduced insurance premium), provided that the app is submitted by the entity providing the benefit, and the data is not be shared with a third party. You must disclose the specific health data that you are collecting from the device.
- (ii) Apps must not write false or inaccurate data into HealthKit or any other medical research or health management apps, and may not store personal health information in iCloud.
- (iii) Apps conducting health-related human subject research must obtain consent from participants or, in the case of minors, their parent or guardian. Such consent must include the (a) nature, purpose, and duration of the research; (b) procedures, risks, and benefits to the participant; (c) information about confidentiality and handling of data (including any sharing with third parties); (d) a point of contact for participant questions; and (e) the withdrawal process.
- (iv) Apps conducting health-related human subject research must secure approval from an independent ethics review board. Proof of such approval must be provided upon request.

WHAT WOULD CHANGE

See reasoning above.

5.1.4 Kids

For many reasons, it is critical to use care when dealing with personal data from kids, and we encourage you to carefully review all the requirements for complying with laws like the Children's Online Privacy Protection Act ("COPPA"), the European Union's General Data Protection Regulation ("GDPR"), and any other applicable regulations or laws. Apps may ask for birthdate and parental contact information only for the purpose of complying with these statutes, but must include some useful functionality or entertainment value regardless of a person's age. Apps intended primarily for kids should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics and third-party advertising may be permitted provided that the services adhere to the same terms set forth in Guideline 1.3.

Moreover, apps in the Kids Category or those that collect, transmit, or have the capability to share personal information (e.g. name, address, email, location, photos, videos, drawings, the ability to chat, other personal data, or persistent identifiers used in combination with any of the above) from a minor must include a privacy policy and must comply with all applicable children's privacy statutes. For the sake of clarity, the parental gate requirement for the Kid's Category is generally not the same as securing parental consent to collect personal data under these privacy statutes. As a reminder, Guideline 2.3.8 requires that use of terms like "For Kids" and "For Children" in app metadata is reserved for the Kids Category. Apps not in the Kids Category cannot include any terms in app name, subtitle, icon, screenshots or description that imply the main audience for the app is children.

5.1.5 Location Services

Use Location services in your app only when it is directly relevant to the features and services provided by the app. Location-based APIs shouldn't be used to provide emergency services or autonomous control over vehicles, aircraft, and other devices, except for small devices such as lightweight drones and toys, or remote control car alarm systems, etc. Ensure that you notify and obtain consent before collecting, transmitting, or using location data. If your app uses location services, be sure to explain the purpose in your app; refer to the Human Interface Guidelines for best practices for doing so.

5.2 Intellectual Property

Make sure your app only includes content that you created or that you have a license to use. Your app may be removed if you've stepped over the line and used content without permission. Of course, this also means someone else's app may be removed if they've "borrowed" from your work. If you believe your intellectual property has been infringed by another developer on the App Store, submit a claim via our web form. Laws differ in different countries, but at the very least, make sure to avoid the following common errors:

5.2.1 Generally:

Don't use protected third-party material such as trademarks, copyrighted works, or patented ideas in your app without permission, and don't include misleading

5.2.2 Third-Party Sites/Services:

If your app uses, accesses, monetizes access to, or displays content from a third-party service, ensure that you are specifically permitted to do so under the service's terms of use. Authorization must be provided upon request.

5.2.3 Audio/Video Downloading:

Apps should not facilitate illegal file sharing or include the ability to save, convert, or download media from third-party sources (e.g. Apple Music, YouTube, SoundCloud, Vimeo, etc.) without explicit authorization from those sources. Streaming of audio/video content may also violate Terms of Use, so be sure to check before your app accesses those services.
Documentation must be provided upon request.

5.2.4 Apple Endorsements:

Don't suggest or imply that Apple is a source or supplier of the App, or that Apple endorses any particular representation regarding quality or functionality. If your app is selected as an "Editor's Choice," Apple will apply the badge automatically.

5.2.5 Apple Products:

Don't create an app that appears confusingly similar to an existing Apple product, interface (e.g. Finder), app (such as the App Store, iTunes Store, or Messages) or advertising theme. Apps and extensions, including third-party keyboards and Sticker packs, may not include Apple emoji. iTunes music previews may not be used for their entertainment value (e.g. as the background music to a photo collage or the soundtrack to a game) or in any other unauthorized manner. If your app displays Activity rings, they should not visualize Move, Exercise, or Stand data in a way that resembles the Activity control. The Human Interface Guidelines have more information on how to use Activity rings.

5.4 VPN Apps

Apps offering VPN services must utilize the NEVPNManager API and may only be offered by developers enrolled as an organization. You must make a clear declaration of what user data will be collected and how it will be used on an app screen prior to any user action to purchase or otherwise use the service.

• ...

WHAT WOULD CHANGE

S. 2710, Sec. 3(a)(3) and 3(f), and S. 2992, Sec. 3(a)(2) and (4) would interfere with the enforcement of this guideline because the provisions would prohibit Apple from limiting access to operating system, software, or device features by an app maker, and a requirement to be enrolled as an organization, although doing so is a baseline quality and consumer protection measure, could be interpreted as imposing such restrictions.

Apps offering VPN services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy. VPN apps must not violate local laws, and if you choose to make your VPN app available in a territory that requires a VPN license, you must provide your license information in the App Review Notes field. Parental control, content blocking, and security apps, among others, from approved providers may also use the NEVPNManager API. Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program.

• ...

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(4) and (7), and S. 2710, Sec. 3(f) would interfere with the enforcement of this consumer protection measure because the provisions would bar Apple from restricting access to the platform and from restricting access to personal data, and Apple's prohibition on VPNs' selling consumer data could be characterized as restrictions on access to personal data and to the platform.

5.5 Mobile Device Management

Mobile Device Management Apps that offer Mobile Device Management (MDM) services must request this capability from Apple. [Such apps may only be offered by commercial enterprises, educational institutions, or government agencies, and in limited cases, companies using MDM for parental control services or device security.](#) You must make a clear declaration of what user data will be collected and how it will be used on an app screen prior to any user action to purchase or otherwise use the service. MDM apps must not violate any applicable laws. Apps offering MDM services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy. In limited cases, third-party analytics may be permitted provided that the services only collect or transmit data about the performance of the developer's MDM app, and not any data about the user, the user's device, or other apps used on that device. Apps offering configuration profiles must also adhere to these requirements. Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program.

WHAT WOULD CHANGE

See reasoning above.

5.6 Developer Code of Conduct

Please treat everyone with respect, whether in your responses to App Store reviews, customer support requests, or when communicating with Apple, including your responses in Resolution Center. Do not engage in harassment of any kind, discriminatory practices, intimidation, bullying, and don't encourage others to engage in any of the above. Repeated manipulative or misleading behavior or other fraudulent conduct will lead to your removal from the Apple Developer Program. Customer trust is the cornerstone of the App Store's success. Apps should never prey on users or attempt to rip off customers, trick them into making unwanted purchases, force them to share unnecessary data, raise prices in a tricky manner, charge for features or content that are not delivered, or engage in any other manipulative practices within or outside of the app. Your Developer Program account will be terminated if you engage in activities or actions that are not in accordance with the Developer Code of Conduct. To restore your account, you may provide a written statement detailing the improvements you plan to make. If your plan is approved by Apple and we confirm the changes have been made, your account may be restored.

5.6.1 App Store Reviews

[App Store customer reviews can be an integral part of the app experience, so you should treat customers with respect when responding to their comments. Keep your responses targeted to the user's comments and do not include personal information, spam, or marketing in your response.](#)
[Use the provided API to prompt users to review your app; this functionality allows customers to provide an App Store rating and review without the inconvenience of leaving your app, and we will disallow custom review prompts.](#)

5.6.2 Developer Identity

Providing verifiable information to Apple and customers is critical to customer trust. Your representation of yourself, your business, and your offerings on the App Store must be accurate. The information you provide must be truthful, relevant, and up-to-date so that

Apple and customers understand who they are engaging with and can contact you regarding any issues.

5.6.3 Discovery Fraud

Participating in the App Store requires integrity and a commitment to building and maintaining customer trust. Manipulating any element of the App Store customer experience such as charts, search reviews, or referrals to your app erodes customer trust and is not permitted.

5.6.4 App Quality

Customers expect the highest quality from the App Store, and maintaining high quality content, services, and experiences promotes customer trust. Indications that this expectation is not being met include excessive customer reports about concerns with your app, such as negative customer reviews, and excessive refund requests. [Inability to maintain high quality may be a factor in deciding whether a developer is abiding by the Developer Code of Conduct.](#)

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2) and S. 2710, Sec. 3(b) would interfere with the enforcement of this quality and consumer protection measure because the provisions would bar self-preferencing and restrictions on developer communications concerning "legitimate business offers," and it could be argued that a requirement to use the referenced API and restrictions on responses to reviews are self-preferencing and a restriction on legitimate business communications, respectively.

WHAT WOULD CHANGE

S. 2992, Sec. 3(a)(2) and (4), and S. 2710, Sec. 3(d) and (f) would interfere with the enforcement of this quality control measure because the provisions would prohibit Apple from restricting access to the platform, even if the app at issue is extremely low quality by any commonly accepted measure.



1401 K Street NW Suite 501
Washington, DC 20005

 202.331.2130  @ACTonline
 ACTonline.org/  actonline.org