

1 Paul J. Riehle (SBN 115199)  
paul.riehle@faegredrinker.com  
2 **FAEGRE DRINKER BIDDLE & REATH LLP**  
Four Embarcadero Center  
3 San Francisco, California 94111  
Telephone: (415) 591-7500  
4 Facsimile: (415) 591-7510

5 Christine A. Varney (*pro hac vice*)  
cvarney@cravath.com  
6 Katherine B. Forrest (*pro hac vice*)  
kforrest@cravath.com  
7 Gary A. Bornstein (*pro hac vice*)  
gbornstein@cravath.com  
8 Yonatan Even (*pro hac vice*)  
yeven@cravath.com  
9 Lauren A. Moskowitz (*pro hac vice*)  
lmoskowitz@cravath.com  
10 M. Brent Byars (*pro hac vice*)  
mbyars@cravath.com

11 **CRAVATH, SWAINE & MOORE LLP**  
825 Eighth Avenue  
12 New York, New York 10019  
Telephone: (212) 474-1000  
13 Facsimile: (212) 474-3700

14 *Attorneys for Plaintiff Epic Games, Inc.*

15 **UNITED STATES DISTRICT COURT**  
16 **NORTHERN DISTRICT OF CALIFORNIA**  
17 **OAKLAND DIVISION**

18  
19 EPIC GAMES, INC.,  
20 Plaintiff,  
21 vs.  
22 APPLE INC.,  
23 Defendant.  
24  
25  
26  
27  
28

Case No. 4:20-CV-05640-YGR

**REPLY MEMORANDUM OF POINTS  
AND AUTHORITIES IN SUPPORT OF  
PLAINTIFF EPIC GAMES, INC.'S  
MOTION FOR A PRELIMINARY  
INJUNCTION**

Date: September 28, 2020 at 9:30 a.m. (via  
Zoom Platform)

Courtroom: 1, 4th Floor

Judge: Hon. Yvonne Gonzalez Rogers

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**Page**

TABLE OF AUTHORITIES ..... iii

TABLE OF CITED DOCUMENTS ..... iv

I. LEGAL STANDARD .....3

II. EPIC IS HIGHLY LIKELY TO SUCCEED ON THE MERITS .....4

    A. Apple’s Conduct Violates Section 2 of the Sherman Act .....4

        1. Apple has a monopoly in the iOS App Distribution Market. ....4

        2. Apple unlawfully maintains its app distribution monopoly.....5

    B. Apple’s Conduct Violates Sections 1 and 2 of the Sherman Act. ....7

        1. Apple ties app distribution to in-app payment processing.....7

        2. Under the rule of reason, Apple’s conduct has anti-competitive effects.....9

        3. Apple’s procompetitive justifications are pretextual. ....9

III. EPIC WILL SUFFER IRREPARABLE HARM ABSENT AN INJUNCTION.....10

IV. THE BALANCE OF HARMS STRONGLY FAVORS EPIC.....12

V. EPIC’S REQUESTED RELIEF WOULD FURTHER THE PUBLIC INTEREST. ....14

**TABLE OF AUTHORITIES**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

<b>Cases</b>	<b>Page(s)</b>
<i>Acquaire v. Canada Dry Bottling Co.</i> , 24 F.3d 401 (2d Cir. 1994).....	11, 12
<i>FTC v. Qualcomm Inc.</i> , 969 F.3d 974 (9th Cir. 2020).....	14
<i>Germon v. Times Mirror Co.</i> , 520 F.2d 786 (9th Cir. 1975).....	12
<i>Milsen Co. v. Southland Corp.</i> , 454 F.2d 363 (7th Cir. 1971).....	12
<i>Newcal Indus., Inc. v. Ikon Office Sols.</i> , 513 F.3d 1038 (9th Cir. 2008).....	5
<i>Ohio v. American Express Co.</i> , 138 S. Ct. 2274 (2018).....	8
<i>S. Glazer’s Distribs. of Ohio, LLC v. Great Lakes Brewing Co.</i> , 860 F.3d 844 (6th Cir. 2017).....	14
<i>Teradata Corp. v. SAP SE</i> , 2018 WL 6528009 (N.D. Cal. Dec. 12, 2018).....	5
<i>Theme Promotions, Inc. v. News Am. Mktg. FSI</i> , 546 F.3d 991 (9th Cir. 2008).....	4
<i>trueEX, LLC v. MarkitSERV Ltd.</i> , 266 F. Supp. 3d 705 (S.D.N.Y. 2017).....	14
<i>United States v. Microsoft Corp.</i> , 253 F.3d 34 (D.C. Cir. 2001).....	9

**TABLE OF CITED DOCUMENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

<b>Citation</b>	<b>Document</b>
Opening	Plaintiff Epic Games, Inc.'s Notice of Motion and Motion for a Preliminary Injunction and Memorandum of Points and Authorities in Support Thereof (ECF No. 61)
Opp'n	Defendant Apple Inc.'s Opposition to Epic Games, Inc.'s Motion for a Preliminary Injunction (ECF No. 73)
Byars	Declaration of M. Brent Byars in Support of Plaintiff Epic Games, Inc.'s Motion for a Preliminary Injunction (ECF No. 61-1)
Evans	Declaration of Dr. David S. Evans (ECF No. 62)
Grant	Declaration of Andrew Grant in Support of Plaintiff Epic Games, Inc.'s Motion for Preliminary Injunction (ECF No. 63)
Penwarden	Declaration of Nicholas Penwarden in Support of Plaintiff Epic Games, Inc.'s Motion for a Preliminary Injunction (ECF No. 64)
Sweeney	Declaration of Timothy Sweeney in Support of Plaintiff Epic Games, Inc.'s Motion for a Preliminary Injunction (ECF No. 65)
Schiller	Declaration of Philip W. Schiller in Support of Defendant Apple Inc.'s Opposition to Plaintiff's Motion for a Preliminary Injunction (ECF No. 74)
Schmalensee	Expert Declaration of Richard Schmalensee, Ph.D (ECF No. 78)
Schmid	Declaration of Mike Schmid in Support of Defendant Apple Inc.'s Opposition to Plaintiff's Motion for a Preliminary Injunction (ECF No. 79)
Byars Reply	Declaration of M. Brent Byars in Further Support of Plaintiff Epic Games, Inc.'s Motion for Preliminary Injunction (submitted herewith)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Evans Reply

Second Declaration of Dr. David S. Evans  
(submitted herewith)

Grant Reply

Declaration of Andrew Grant in Further  
Support of Plaintiff Epic Games, Inc.’s Motion  
for Preliminary Injunction (submitted herewith)

Sweeney Reply

Declaration of Timothy Sweeney in Further  
Support of Plaintiff Epic Games, Inc.’s Motion  
for a Preliminary Injunction (submitted  
herewith)

1 This preliminary injunction motion is crucial, yet narrow. Epic seeks one thing only: to  
2 offer consumers an alternative payment processing service that allows consumer choice and  
3 lower prices while this litigation proceeds without retaliation. The issue is less complicated than  
4 the voluminous legal arguments and technical jargon before the Court suggest. Epic is prepared  
5 to do everything possible to allow this Court to resolve this case in an expeditious manner. At  
6 that point, should Apple prevail, it can be made whole. But during the pendency of the case,  
7 consumers should not be harmed by Apple’s overwhelming retaliation against Epic.

8 Apple’s papers try to make this dispute about Apple’s innovative products, rather than  
9 Apple’s practices. Many monopolists start with extraordinary products, yet courts have to step in  
10 if they use their power to stifle competition. Apple also tries to make this case about speculative  
11 security concerns. But Apple routinely allows third-party payment processing in other apps,  
12 including Amazon and Uber. And Apple identified no evidence that Epic’s direct payment, or  
13 any Epic product, posed an actual security threat. Apple’s strawman arguments should not  
14 distract from what is a simple situation supported by a long line of Supreme Court cases.

15 Turning to the merits, in its Opening Brief, Epic showed that Apple is a monopolist in  
16 two markets, for iOS app distribution and for iOS in-app payment processing, and that it illegally  
17 maintains its monopolies through unlawful contractual ties and technical restrictions that  
18 foreclose all competition. Apple does not dispute its complete control over app distribution to  
19 over a billion iOS users or over in-app payment processing, nor any of the restrictions that  
20 maintain that control. Yet Apple baldly asserts “it is no monopolist”, asking this Court to believe  
21 that iPhones are “interchangeable” with personal computers and gaming consoles. That assertion  
22 is contrary to basic antitrust principles and common sense: a Sony PlayStation does not fit in  
23 your pocket but a smartphone does.

24 Apple also argues that its web of restrictions is not anti-competitive because they create  
25 an “integrated service” that is the basis of its “iPhone business model”. (Opp’n 19.) But Apple  
26 cannot immunize these restrictions from antitrust scrutiny by labeling them a “business model”.  
27 Nor can Apple credibly insist that IAP is an inseparable aspect of the App Store—that they are a  
28 “single” product—when (a) Apple already allows many apps to use alternative pay options, and

1 (b) many in-app transactions occur days, months, or years *after* the app is downloaded from the  
2 App Store. Apple also cannot dispute direct evidence of separate demand for payment  
3 processing services, including (a) the robust demand for such services on eligible categories of  
4 iOS apps and open platforms, and (b) Apple’s new disclosure that over the years Apple has  
5 terminated the accounts of no fewer than 2,000 developers who introduced alternative payment  
6 processors. It is clear that developers are clamoring for competition.

7 Apple also does not dispute that its termination of Epic from its Developer Program  
8 would cause irreparable harm to Epic, *Fortnite* players, Epic’s *Unreal Engine* customers, and  
9 customers of those customers—in essence, that it is dispensing collective punishment. Instead of  
10 denying these harms to Epic and third parties, Apple argues that the Court should ignore them.  
11 *First*, it argues Epic “created the current situation” by offering alternative payment processing,  
12 “knowing that Apple would invoke its contractual right” to terminate Epic. (*Id.* at 2.) But Epic  
13 is doing precisely what the Supreme Court has instructed that Epic is entitled to do: refuse to  
14 comply with anti-competitive contractual conditions. Epic and the public should be protected  
15 from Apple’s retaliation. Apple has no valid response.

16 *Second*, Apple repeatedly invokes “security” and “privacy” as justifications for  
17 terminating Epic from its Developer Program, claiming that its retaliation somehow *benefits*  
18 consumers. But Apple has not pointed to a single security issue relating to Epic’s direct payment  
19 option, any of Epic’s apps, or *Unreal Engine*. Absent any evidence of harm to any user, Apple  
20 argues that the widely used hotfix update mechanism itself was malicious. But as Epic showed  
21 in its Opening papers, using hotfixes to serve updated content is common industry practice, and  
22 Apple does not dispute that the *Fortnite* app has openly used them for years without objection.  
23 Moreover, the hotfix update has come and gone, and Epic submitted several *Fortnite* builds  
24 expressly disclosing Epic’s direct payment option. Apple rejected them all, and still proceeded  
25 to terminate Epic’s Developer Program account. Apple’s retaliation is not directed against the  
26 *method* by which Epic introduced competing payment processing functionality; Apple is  
27 objecting to the *fact* that Epic introduced competition offering consumers lower prices. Apple is  
28 not protecting consumers; it is protecting its monopoly and its bottom line.

1 Finally, Apple’s papers contain a number of half-truths and outright falsities intended to  
2 paint Epic as a bad actor. Epic cannot catalogue them all here but notes a few examples below:

3 (1) Apple asserts that Epic eliminated IAP from *Fortnite*. This is false. Epic’s hotfix  
4 update offered IAP *and* Epic direct pay side-by-side. IAP remained available in *Fortnite* until  
5 Apple blocked IAP upon termination of Epic’s Team ID ’84 account. (Grant Reply ¶¶ 38-39.)

6 (2) Apple asserts that the August 13 release has security risks. That is false. Apple has  
7 not presented a shred of evidence that there is any security issue.

8 (3) An Apple declarant asserts that in 2018, Epic breached its agreement with Sony to  
9 launch cross-platform play without Sony’s consent. (Schmid ¶ 19.) That is false. Sony  
10 announced the availability of cross-platform play in September 2018 with Epic as one of the first  
11 participants in the new program. (Sweeney Reply ¶ 7, Ex. A.)

12 (4) Apple claims Epic brought this case to revive supposedly waning interest in *Fortnite*,  
13 alleging a 70% decline in “interest” between October 2019 and July 2020. (Opp’n 11.) But  
14 Apple cherry-picked Google Trends data concerning Google *search* volumes, misleadingly  
15 starting from a one-week spike that took place in October 2019 when Epic ran an in-game event  
16 that captured global attention. *Fortnite users* increased over that period. (Sweeney Reply ¶ 18.)

17 (5) Apple argues that “Epic’s own app marketplace charges users and developers a  
18 commission” just like IAP. (Opp’n 6 & n.7.) But the Epic Games Store offers developers the  
19 choice that Apple does not: they can use Epic’s payment processor for in-app purchases, or they  
20 can use another payment processor and pay Epic nothing. (Sweeney Reply ¶ 24.)

21 (6) Apple claims it placed *Fortnite* billboards in Times Square and LA Live, at its  
22 expense to the benefit of Epic. But the billboards actually promoted the availability of  
23 Marshmello’s concert playlist on Apple Music. (Sweeney Reply ¶¶ 20-22, Ex. B.)

24 Epic looks forward to demonstrating at trial the unlawfulness of Apple’s conduct. In the  
25 meantime, an injunction should issue.

## 26 **I. LEGAL STANDARD**

27 Apple does not dispute that Epic must satisfy the *Winter* test. (Opp’n 14.) Apple  
28 nonetheless suggests that this test is harder to meet here because the injunction sought is



1 “mandatory” instead of “prohibitory”. (*E.g.*, Opp’n 14-15.) Apple is wrong. The requested  
 2 injunction here is prohibitory; Epic seeks an order prohibiting Apple from retaliating against  
 3 Epic in any way on account of Epic’s introduction of a competitive alternative to Apple’s IAP.  
 4 (Opening ii (requesting an order prohibiting retaliation and undoing retaliatory actions taken).)  
 5 In any event, Epic satisfies the four preliminary injunction factors as applied to the relief sought.

## 6 **II. EPIC IS HIGHLY LIKELY TO SUCCEED ON THE MERITS.**

### 7 **A. Apple’s Conduct Violates Section 2 of the Sherman Act.**

#### 8 **1. Apple has a monopoly in the iOS App Distribution Market.**

9 In its Opening brief, Epic established a relevant product market for distribution of apps  
 10 compatible with iOS to users of mobile devices running iOS: the iOS App Distribution Market.  
 11 Apple does not and cannot dispute its complete control over this market. Instead, Apple argues  
 12 in its Opposition that Epic defined the market too narrowly. Not so.

13 Apple argues that there are “alternative means to distribute *Fortnite*”, and therefore, that  
 14 the market here must include “at least” distribution on other platforms on which *Fortnite* can be  
 15 played. (Opp’n 16.) That is inconsistent with basic antitrust principles. Markets are commonly  
 16 defined by applying the hypothetical monopoly test, which “asks whether a monopolist in the  
 17 proposed market could profitably impose a small but significant and nontransitory price  
 18 increase” on the monopolized product to a specified set of customers. *Theme Promotions, Inc. v.*  
 19 *News Am. Mktg. FSI*, 546 F.3d 991, 1002 (9th Cir. 2008); (Evans Reply ¶ 57). The iOS App  
 20 Distribution Market accordingly includes all the ways by which app developers generally  
 21 (including, but not limited to, Epic) could (absent Apple’s restrictions) distribute apps to the  
 22 billion users of iOS devices. (Evans ¶¶ 52-54.) A hypothetical monopolist in iOS app  
 23 distribution could profitably impose a price increase on iOS app developers (Apple does just  
 24 that). That is because distributing apps to users of other platforms is not an adequate substitute,  
 25 from the developer’s perspective, for accessing the one billion iOS users. (*Id.* ¶¶ 41-42.)

26 For example, by distributing on Android, a developer does not reach the billion users of  
 27 iOS devices because users typically do not have mobile devices on both OSs. As for distribution  
 28 on game consoles, many apps require mobility or are not games playable on a console.

1 Moreover, many millions of iOS users do not have those alternative devices. And even for those  
2 iOS users who do have alternatives at home, they are generally not portable and must be hooked  
3 up to a television or monitor and electrical outlet; even laptop computers are too large to fit in a  
4 pocket or a purse. The smartphone is unique: there is simply no other device that fits in your  
5 pocket and can be used anywhere and at any time. As the data show, of the *Fortnite* users on  
6 iOS, 63% access *Fortnite* only on iOS. (Sweeney Reply ¶ 17.) Those users, and iOS users more  
7 generally, are not accessible through distribution on other platforms.

8 Epic also explained in its Opening brief (at 13-14), and Epic's expert opined, how the  
9 iOS App Distribution Market reflects the characteristics of the single-brand market defined in  
10 *Newcal Indus., Inc. v. Ikon Office Sols.*, 513 F.3d 1038 (9th Cir. 2008): The primary market  
11 consists of OSs for smartphones or tablets; Apple has market power in the primary market; and  
12 competition for smartphone (or tablet) OSs cannot constrain Apple in the aftermarkets. (Evans  
13 ¶¶ 25-30; Compl. ¶¶ 156-83.) Apple contends that Epic has "no basis" to argue that  
14 "components of Apple's integrated offerings should be considered separately", and that "this is  
15 not an aftermarket case". (Opp'n 16-17.) But *Newcal* is that basis, and Apple cites no support  
16 that *Newcal* does not apply where a monopolist chooses to label its conduct in the downstream  
17 market as an "integrated offering". See *Teradata Corp. v. SAP SE*, 2018 WL 6528009 at \*17  
18 (N.D. Cal. Dec. 12, 2018) (aftermarket properly alleged despite defendant labeling its tied and  
19 tying products as "integrated"). Indeed, it is Apple's decision to contractually coerce developers  
20 to "integrate" its downstream offering that constitutes Apple's anti-competitive conduct.

## 21 **2. Apple unlawfully maintains its app distribution monopoly.**

22 Epic described in detail the web of technical and contractual restrictions Apple employs  
23 to ensure that consumer apps may be distributed on iOS solely through its own App Store,  
24 thereby unlawfully maintaining its monopoly over the iOS App Distribution Market. (Opening  
25 12-15.) Apple does not dispute that it imposes the restrictions Epic identified. Instead, it claims  
26 these are legal for two reasons, neither of which is availing.

27 *First*, Apple contends its technical and contractual restrictions are legal because there are  
28 "alternative distribution options". (Opp'n 18.) As discussed above, that is factually and legally

1 incorrect—there are no alternative options to distribute consumer apps to iOS users, and through  
2 the restrictions, Apple maintains a complete monopoly in the iOS App Distribution Market.

3 *Second*, Apple says it need not provide “unfettered and uncompensated use of its own  
4 technology”. (*Id.*) That statement mischaracterizes Epic’s argument. Microsoft is compensated  
5 for its investment in Windows without forcing all transactions on Windows PCs through a single  
6 store that it controls. Apple can be too. Apple just cannot use its market power to force  
7 developers to use its own services to the exclusion of all others. Epic is ready, willing, and able  
8 to compete by offering distribution services that would compete with Apple’s; Epic (like other  
9 would-be distributors) has been blocked from doing so by Apple’s anti-competitive conduct.  
10 (Sweeney ¶¶ 12-14.) Apple’s investment in iOS does not give it unfettered rights to maintain a  
11 monopoly in related, downstream markets, and Apple cites no case law suggesting otherwise.

12 Apple also tries to justify its total control of all iOS consumer app distribution by  
13 pointing to the need for security. (Opp’n 5.) This is a pretext. There are many methods to  
14 secure a platform aside from controlling all consumer app distribution. Indeed, Apple already  
15 has implemented many of those methods on iOS through the OS design, not through App Store  
16 control. (Grant Reply ¶¶ 30-35.) Apple does not control all app distribution on macOS.  
17 (Sweeney ¶ 10.) Apple already allows certain entities on iOS to download directly from the  
18 Internet and bypass the App Store. (Grant ¶¶ 5, 14.) Apple is also aware that security could be a  
19 factor on which different app stores could compete; if Apple’s App Store could in fact offer  
20 better security than all other stores, Apple could use this security advantage to prevail in a  
21 competitive market. Epic does not claim that Apple cannot participate in the iOS app  
22 distribution marketplace. Epic argues that Apple cannot use its market power to monopolize app  
23 distribution and that Apple should fairly compete in that market.

24 Finally, Apple asserts that “Epic’s antitrust theories . . . have nothing to do with Unreal  
25 Engine, and thus cannot support that aspect of the requested injunction”. (Opp’n 18 n.17.) But it  
26 was Apple that brought *Unreal Engine* into this dispute when it overreached in its retaliation  
27 against Epic by threatening to destroy the ability of *Unreal Engine* to provide third-party user  
28 tools for iOS and macOS development. Now it is absolutely relevant to Epic’s claims. For

1 assessing likelihood of success on the merits, Apple’s retaliation against *Unreal Engine* is further  
 2 evidence of the absolute power Apple wields on iOS and the lengths to which Apple will go to  
 3 maintain its monopolies.<sup>1</sup> Apple’s express purpose of attacking Epic’s ability to develop *Unreal*  
 4 *Engine* was to force Epic into submission and ensure compliance with Apple’s anti-competitive  
 5 scheme. (Opp’n 28.) An injunction protecting Epic’s products including *Unreal Engine* would  
 6 curtail the scope of Apple’s anti-competitive conduct.<sup>2</sup>

7 **B. Apple’s Conduct Violates Sections 1 and 2 of the Sherman Act.**

8 Apple does not dispute that it contractually conditions developers’ ability to distribute  
 9 iOS apps on their agreement to use solely Apple’s own IAP to process all in-app payments for  
 10 digital content and that it thereby forecloses all competition for the processing of such payments.  
 11 That is unlawful *per se* and rule of reason tying and monopoly maintenance. (Opening 15-23.)

12 **1. Apple ties app distribution to in-app payment processing.**

13 Epic has shown the first element of tying: two separate products. Under the purchaser  
 14 demand test, app distribution is a separate product from in-app payment processing for digital  
 15 content because there is demand for in-app payment processing separate and apart from demand  
 16 for distribution services. In-app purchases occur days, months, or years after an app has been  
 17 downloaded to a user’s device. But for Apple’s IAP restrictions, these purchases would be  
 18 between the developer and the consumer. (Evans Reply ¶ 29.) In its Opening brief (at 17), Epic  
 19 provided examples where software developers use different in-app payment processors than that  
 20 of the provider of the software distribution services. Epic also pointed to its own experience that  
 21 there is user demand for in-app payment processing from a provider other than Apple. (*Id.*)  
 22 Apple itself provides further examples. On September 11, 2020, Apple amended its App Store  
 23 Review Guidelines to liberate from its IAP requirement “app[s] . . . only sold directly by  
 24 [developers] to organizations or groups for their employees or students” and “app[s that] enable[]

25 <sup>1</sup> In the same vein, to maximize its retaliatory threats to Epic, Apple recently threatened to  
 26 shut down Sign in with Apple following its termination of the ’84 account, potentially leaving  
 hundreds of thousands of Epic users locked out of their accounts. (Grant Reply ¶¶ 16-25.)

27 <sup>2</sup> Apple argues that “Epic’s defective theory of monopoly maintenance does not provide any  
 28 legal basis for a preliminary injunction that is independent from its flawed tying theory.” (Opp’n  
 18.) If Epic is likely to prevail on monopoly maintenance, the requested injunction would be a  
 partial remedy. (Opening 12.)

1 the purchase of realtime person-to-person experiences between two individuals”. (Byars Reply  
2 Ex. F §§ 3.1.3(c), (d).) Apple also disclosed that it previously has terminated “over 2,000  
3 [developer] accounts for introducing a non-IAP payment method”. (Opp’n 8.) Clearly, separate  
4 demand exists. Schmalensee ¶¶ 46-54 and Schiller ¶ 45, on which Apple relies to argue that “no  
5 demand exists for IAP that is separate from distribution via the App Store” (Opp’n 20), do not  
6 rebut the evidence of separate demand.<sup>3</sup>

7 Apple also argues (Opp’n 20-21 n.19) that the two-sided nature of iOS gives Apple a  
8 license to foreclose all competition in the iOS aftermarkets. But *Ohio v. American Express Co.*,  
9 138 S. Ct. 2274, 2286 (2018), held only that both sides of a two-sided market must be  
10 considered, not that all downstream aftermarkets must be considered part of the primary market  
11 if the primary market is two-sided.

12 Here, Epic has shown that Apple ties these two separate products. Apple’s argument that  
13 “[t]here is no . . . conditioning here” because “[d]evelopers are free to adopt other business  
14 models that do not include in-app digital purchases” (Opp’n 19) is misguided. Under Apple’s  
15 rules, the only way to distribute consumer apps on iOS is through the App Store. The only way  
16 to sell in-app digital content on iOS is through IAP (subject to Apple’s arbitrary unilaterally  
17 determined exceptions). That is conditioning, and that is a tie. The fact that some participants  
18 who are injured by a monopolist’s unlawful acts may leave or decline to enter the market does  
19 not absolve the monopolist. Indeed, that is anti-competitive harm, as Apple’s former CEO  
20 himself recognized. (Byars Reply Ex. I (a developer cannot “buy/rent/subscribe from iOS  
21 without paying us [Apple], which we acknowledge is prohibitive for many things”).<sup>4</sup>

22 <sup>3</sup> Schmalensee, for example, argues that IAP is not just a payment processing service, but a  
23 “system” providing “a safe and secure marketplace”. (Schmalensee ¶ 50.) Yet he ignores that  
24 developers choosing other payment processing services where allowed by Apple, such as for the  
Amazon or Uber iOS apps, demonstrates that separate demand exists.

25 <sup>4</sup> Apple does not address Epic’s argument that Apple’s tying affects a not insubstantial  
26 amount of commerce in the iOS In-App Payment Processing Market. (Opening 18-19.) Apple  
27 argues that there is no *per se* tying because it integrates “its StoreKit APIs into the App Store  
28 software platform”. (Opp’n 21.) But Epic has always said that IAP can be one of the options  
available to iOS developers and users so long as the market is open to competition. There is no  
technological reason that developers must integrate StoreKit APIs, rather than the APIs of  
alternative payment processors. *Microsoft* did not undo the line of cases that apply the *per se*  
standard to “contractual ties”. See *United States v. Microsoft Corp.*, 253 F.3d 34, 89-95 (D.C.  
Cir. 2001).

1                   **2. Under the rule of reason, Apple’s conduct has anti-competitive effects.**

2                   In its Opening brief (at 20), Epic explained how Apple forecloses competition in the iOS  
3 In-App Payment Processing Market. The facts are simple: Epic offered a competing product  
4 with lower prices, and Apple ejected Epic from the market. Apple now concedes that it has  
5 taken similar steps against over 2,000 other developers seeking to introduce competition into the  
6 iOS ecosystem. (Opp’n 8.) Foreclosure on this scale is clearly anti-competitive.

7                   **3. Apple’s procompetitive justifications are pretextual.**

8                   Apple argues that this undeniable competitive harm is justified by procompetitive  
9 benefits. Apple is wrong. Apple invokes the word “security” or some variation thereof at least  
10 15 times in its Opposition brief. (*E.g.*, Opp’n 1, 3, 7-9, 27-30.) But security cannot justify the  
11 complete foreclosure of competition in a huge part of the digital economy. And security is  
12 clearly not the reason for these restrictions. Apple already allows alternative payment  
13 mechanisms for iOS apps that provide real-world goods or services (Byars Reply Ex. F  
14 § 3.1.3(e)), enterprise services (*id.* § 3.1.3(c)), or person-to-person experiences (*id.* § 3.1.3(d)).  
15 Likewise Apple does not mandate IAP for digital content purchased on Mac computers.  
16 (Sweeney ¶ 10; Byars Ex. K § 7.) Thus, IAP plainly is not necessary to maintain the security of  
17 Apple devices.

18                   Similarly, Apple’s desire to be paid in a particular manner cannot justify its foreclosure  
19 of the iOS In-App Payment Processing Market. (Opp’n 22-23.) As explained in Epic’s Opening  
20 brief (at 20-23), Apple is entitled to payment for services that it provides, but it is not entitled to  
21 force services onto users and developers when Apple’s services are not wanted. Apple  
22 repeatedly points to its investment in “the tools, education, and support services that Apple  
23 makes available to developers”, including Epic. (Opp’n 22.) The fact that Apple makes these  
24 tools, education, and support available to developers is not related to the App Store or to public  
25 good; Apple undertakes these investments to make the iOS platform more appealing to app  
26 developers and users alike. Apple’s CEO has freely acknowledged this, as has one of Apple’s  
27 experts. (Opening 21-22 & n.6.) Apple and Microsoft provide similar tools to developers of  
28 macOS and Windows OS applications, even though neither controls the distribution of such

1 applications on PCs. (*See* Penwarden ¶ 5.)

2 Apple complains that “if the Court were to enjoin one piece of the extant model . . .  
3 Apple would have to rework the entire system” and switch to one of the many other potential  
4 models that it acknowledges are possible. (Opp’n 22-23.) That is exactly the point; Apple  
5 should have to change the unlawful portions of its business model.

6 Apple argues that the “spectacular growth” of iOS is proof of the procompetitive benefits  
7 of its conduct. (*Id.* at 22.) But Apple has done nothing to show that growth is attributable to the  
8 conduct at issue—that is, that this growth is the result of Apple’s requirement that all consumer  
9 app distribution occur through the App Store and that all in-app payment processing for digital  
10 content occur through IAP.

11 Finally, Apple argues that the fact that “[o]ther app stores for computing platforms also  
12 charge similar commissions, at a similar rate . . . is strong evidence” that Apple’s conduct is  
13 procompetitive. (*Id.* at 23.) Not so. Google—the other duopolist for smartphone (or tablet)  
14 OSs—is able to adopt the same anti-competitive policies Apple has adopted because it is a  
15 monopolist in distribution of Android apps. (*See* Byars Reply Ex. G § 4.5; *id.* Ex. H.) As for  
16 gaming consoles, the comparison is apples and oranges. Apple does not address the many  
17 distinctions Epic has raised between gaming consoles and mobile devices. (Opening 22 n.7.)  
18 And there is a wide diversity of practices among app stores on the open platforms of Windows  
19 and macOS PCs (Evans Reply ¶ 12; Sweeney ¶ 10), demonstrating that competition benefits the  
20 consumer. Thus, little can be inferred from adoption of Apple’s practices in other contexts.

### 21 **III. EPIC WILL SUFFER IRREPARABLE HARM ABSENT AN INJUNCTION.**

22 Apple does not dispute that removal of *Fortnite* from the App Store will cause many Epic  
23 customers to give up on *Fortnite* and will undermine Epic’s ability to create the *Fortnite*  
24 metaverse. Apple does not dispute that cutting off Epic’s access to developer tools will cause  
25 millions of developers who rely on *Unreal Engine* to question the viability of the engine.

26 Instead, Apple’s argument is simply that since Epic changed its *Fortnite* app, Apple  
27 should be able to do anything in retaliation. Apple also complains that Epic publicized the fight  
28 to “engender goodwill”. (Opp’n 26.) Epic’s public statements were made to expose to the



1 public Apple’s anti-competitive conduct—which Apple takes pains to conceal. (Byars Reply  
2 Ex. F § 3.1.3.) In any event, users and developers are blaming Epic for the effects of this fight,  
3 with incalculable consequences to Epic’s goodwill, reputation, and competitive standing.  
4 (Opening 25-29.) Apple does not grapple with this quintessential evidence of irreparable harm.

5 This leaves Apple’s main argument, that Epic’s harm should be ignored because it is self-  
6 inflicted. That argument fails as a matter of law. In its Opening Brief, Epic discussed the long  
7 line of U.S. Supreme Court precedent holding that the law does not penalize, but rather protects,  
8 parties that challenge anti-competitive contract provisions, including when that challenge  
9 involves non-compliance with the terms of those contracts. The Supreme Court has said courts  
10 should not aid monopolists by enforcing unlawful provisions in contracts, and should not  
11 penalize those who, in order to break out of the grip of a monopolist, breach such provisions.  
12 These cases are binding precedent that serves the congressional intent of finding ways to ensure  
13 that the competitive process maintains vibrancy. If Epic is correct and Apple is maintaining a  
14 monopoly with anti-competitive contract restrictions, the Supreme Court instructs that what  
15 Apple characterizes as self-inflicted should be understood as protective of competition.

16 Apple’s attempt to distinguish this line of binding precedents on the basis that they did  
17 not involve injunctive relief (Opp’n 25) finds no support in the cases themselves, and is flatly  
18 contradicted by Courts of Appeals precedent, cited in Epic’s Opening brief (at 24-25), including  
19 *Acquire v. Canada Dry Bottling Co.*, 24 F.3d 401 (2d Cir. 1994). The *Acquire* court  
20 recognized that if the plaintiffs there chose to “abide by [the] terms” of the defendant’s illegal  
21 “promotional program”, the defendant would not have “withheld product” from them. *Acquire*,  
22 24 F.3d at 411. The *Acquire* court outright rejected the defendant’s argument that the harm to  
23 the plaintiffs, caused by their choice to reject the illegal provisions, was “self-inflicted”. *Id.* at  
24 411-12. Epic was faced with a similar choice: if it chose, “with a simple keystroke”,<sup>5</sup> to  
25 capitulate and provide Apple with a compliant version of *Fortnite*, Apple would return *Fortnite*  
26

---

27 <sup>5</sup> Apple argues that Epic cannot demonstrate irreparable harm because it “can solve its own  
28 problems” “with a simple keystroke”. (Opp’n 23-24; *see also id.* at 2.) This is false, or at least  
inconsistent with Apple’s statements to Epic. Apple has decreed that it “will deny [Epic’s]  
reapplication to the Apple Developer Program for at least a year”. (Grant Ex. H.)



1 to the App Store and allow Epic to keep its Developer Program accounts. If it refused, Apple  
 2 would punish Epic by terminating its accounts, cutting off its access to tools, and more. Like the  
 3 *Acquire* court, this Court should not discount irreparable harm based on the fact that Epic’s  
 4 choice was to take a stand and not abide by Apple’s anti-competitive policies.<sup>6</sup>

#### 5 **IV. THE BALANCE OF HARMS STRONGLY FAVORS EPIC.**

6 Absent relief, the harm to Epic will be significant. (*See* Section III above.) By contrast,  
 7 the parade of horrors Apple claims will occur if the injunction is granted is not credible.

8 Apple already allows many developers to offer direct payment as an alternative to IAP.  
 9 Apple did not reject Epic’s direct payment to protect iOS users—Apple rejected it because it  
 10 posed a competitive threat. Epic’s refusal to abide by Apple’s anti-competitive IAP tie does not  
 11 provide any support that *Fortnite*, *Unreal Engine*, or any other Epic app for that matter, would  
 12 become a source of malware. Apple’s entire security threat argument is destroyed by its own  
 13 practices that allow numerous other developers to offer direct payment.

14 Apple’s argument is that there is a possibility Epic’s payment service could  
 15 hypothetically create a future security issue—the “*prospect* that Epic’s alternative payment  
 16 system may compromise [users’] privacy or data security”. (Opp’n 27 (emphasis added).)  
 17 Apple offers no evidence to support this speculation. Numerous other developers already offer  
 18 direct pay safely. Epic direct pay has been on iOS for over a month. Apple has used this time to  
 19 dissect Epic direct pay to look for security threats. Apple’s failure to offer any evidence of such  
 20 a threat is conclusive. Apple already allows many payment processors other than IAP for real-  
 21 world goods or services (Byars Reply Ex. F § 3.1.3(e)), enterprise services (*id.* § 3.1.3(c)), or  
 22 person-to-person experiences (*id.* § 3.1.3(d)). Third-party payment processing is not a security  
 23

---

24 <sup>6</sup> *Milsen Co. v. Southland Corp.*, 454 F.2d 363 (7th Cir. 1971), is also on point. There, the  
 25 defendant attempted to terminate agreements because the plaintiffs had refused to pay certain  
 26 allegedly anti-competitive franchise fees due under the agreements. 454 F.2d at 364-65. The  
 27 court reversed the denial of a preliminary injunction because “defendants who are or may be  
 28 guilty of anticompetitive practices should not be permitted to terminate . . . when such  
 terminations would effectuate those practices”. *Id.* at 366; *see also Germon v. Times Mirror Co.*,  
 520 F.2d 786, 788 (9th Cir. 1975) (citing *Milsen*; “A termination might be enjoined even if  
 done pursuant to contract, if the contractual clause . . . foster[s] an unlawful anticompetitive  
 scheme.”). By contrast, none of Apple’s cited cases (Opp’n 24) involved a party that refused to  
 abide by a contract because the contract was unlawful under the antitrust laws.

1 threat. Apple opposes Epic direct pay to protect its monopoly.

2 Similarly, restoring *Fortnite* to iOS would not increase the risk of Epic sneaking malware  
3 into its apps or the *Unreal Engine* toolset. (Opp’n 28.) There is no such risk. Epic had apps on  
4 the App Store for a decade. *Fortnite* has been on the store for two years. *Unreal Engine* has  
5 powered apps on the App Store for many years. Epic is a respected, well-established company.  
6 Epic’s CEO has sworn under oath that Epic does not and will not deal in malware (Sweeney  
7 Reply ¶ 26), and Epic would suffer incalculable reputational harm if it tried to sneak in malware.  
8 Using the well-established hotfix mechanism to serve a second payment option is not malware.  
9 (Grant ¶¶ 16-22.) If Apple really believed this was a risk, it would not have requested that Epic  
10 restore *Fortnite* to the App Store by providing a compliant build. (*Id.* at Ex. B; Opp’n 12.)

11 Apple would not be harmed by the requested injunction. Nothing about the requested  
12 injunction would limit Apple’s ability to terminate accounts (or even developers) that harm users  
13 by introducing malware, hurt security, or compromise privacy. Instead, the requested injunction  
14 would limit only Apple’s ability to continue to use its absolute control over its digital platform to  
15 instill existential fear in app developers and deter any challenge to its unlawful contractual terms.  
16 That is hardly a “harm” that supports Apple’s opposition.

17 Apple suggests there is no harm to Epic because of Apple’s purported “right to terminate  
18 the developer agreements at any time, for any reason . . . for any Epic affiliate”. (Opp’n 24.)  
19 But the contracts do not permit Apple to terminate separate entities’ *contracts* for their affiliate’s  
20 breach of a *separate* contract. Apple’s having done this thousands of times in the past is no  
21 excuse. That a contract is “at will” does not suggest Epic would not suffer harm from its  
22 termination—or that termination as part of a retaliatory anti-competitive scheme is proper.

23 Importantly, the threatened termination is intended to further Apple’s anti-competitive  
24 scheme and deter resistance. As such, it is itself illegal. The law imposes a duty to deal on a  
25 monopolist like Apple “when (1) it unilaterally terminates a voluntary and profitable course of  
26 dealing; (2) the only conceivable rationale or purpose is to sacrifice short-term benefits in order  
27 to obtain higher profits in the long run from the exclusion of competition; and (3) the refusal to  
28 deal involves products that the defendant already sells in the existing market to other similarly

1 situated customers”. *FTC v. Qualcomm Inc.*, 969 F.3d 974, 994-95 (9th Cir. 2020) (internal  
 2 quotations and alterations omitted). Here, Apple is attempting unilaterally to terminate voluntary  
 3 and profitable contacts, with the express purpose of eliminating competition, denying Epic  
 4 accounts and developer tools that Apple “makes . . . available” to all developers. (Opp’n 5-6.)

5 **V. EPIC’S REQUESTED RELIEF WOULD FURTHER THE PUBLIC INTEREST.**

6 Countless *Fortnite* users and developers who rely on *Unreal Engine* are collateral  
 7 damage to Apple’s collective punishment. (*See* Section III; Opening 25-29; Byars Ex. R-S.)  
 8 Apple does not dispute that harm to these users and developers is against the public interest.

9 Instead, Apple argues that “an injunction would contravene the public’s ‘strong interest  
 10 in holding private parties to their agreement[.]’”. (Opp’n 29.) But that principle applies only to  
 11 lawful agreements, as Apple’s cited case recognizes. *See S. Glazer’s Distribs. of Ohio, LLC v.*  
 12 *Great Lakes Brewing Co.*, 860 F.3d 844, 853-54 (6th Cir. 2017) (“The public . . . has an *interest*  
 13 *in enforcing the [law],*” and that “[*b*]ecause there is no conflict [between the contract and the  
 14 law], the public’s interest in enforcing private contracts weighs against the injunction”  
 15 (emphases added)).<sup>7</sup> This case is not about enforcing lawful private contracts. The contractual  
 16 provisions on which Apple relies and against which Epic has taken a stand are unlawful. Apple  
 17 does not dispute that enforcement of the antitrust laws furthers the public interest. (*See* Opening  
 18 at 23-25.) “Where the contractual right is alleged to violate the antitrust laws, the public interest  
 19 in antitrust enforcement and preservation of competition outweighs the interest in freedom of  
 20 contract.” *trueEX, LLC v. MarkitSERV Ltd.*, 266 F. Supp. 3d 705, 726 n.143 (S.D.N.Y. 2017).

21 Apple’s suggestion that an injunction would place other App Store developers at a  
 22 competitive disadvantage vis-à-vis Epic is likewise meritless. (Opp’n 29.) Apple’s sudden  
 23 concern about equity and the concern that some app developers would “be forced to subsidize  
 24 the tools that allow Epic to succeed” rings hollow given Apple’s repeated assertion that over  
 25 80% of app developers pay nothing for those tools; presumably, in Apple’s view, they are  
 26 “subsidized” by those who do. Nor is it true that an injunction somehow would lead developers  
 27 to feel free to “compromise” users’ data. The requested injunction would not prevent Apple

28 <sup>7</sup> Apple’s other cited cases do not involve allegations of unlawful contracts. (Opp’n 29.)

1 from enforcing rules that actually pertain to security or privacy. All it would do is prevent Apple  
2 from retaliating against Epic for one thing only—the introduction of competition to IAP.

3 Apple’s attempt to downplay the harm it inflicts on users of *Fortnite* and *Unreal Engine*  
4 is also unpersuasive. (Opp’n 9-10, 30.) *Fortnite* is a forum for shared experiences, including  
5 concerts, movies, roundtables, and gaming. For the intensely social experience that *Fortnite*  
6 offers, the loss of even 10% of users impacts the entire *Fortnite* community. Estranging all iOS  
7 users has resulted in manifold more disrupted connections that affect non-iOS friends and family  
8 who keenly feel the loss, and undermines Epic’s ability to reach the crucial mass necessary to  
9 achieve the metaverse. (Sweeney ¶¶ 3, 24.) Contrary to Apple’s statement that “Unreal  
10 Engine . . . is used by a minuscule fraction of iPhone apps” (Opp’n 30), Apple’s own witness  
11 testified that “Unreal Engine is a popular development engine used by many developers on iOS  
12 and other platforms.” (Schmid ¶ 20.) *Unreal Engine* has a community of 11 million developers  
13 worldwide (Penwarden ¶ 2), and is used to develop some of the most popular games on the App  
14 Store. (Penwarden ¶ 4; Sweeney ¶ 30.) Apple’s claim that its retaliation against *Unreal Engine*  
15 would not harm developers because of the availability of *Unity*, an *Unreal Engine* competitor, is  
16 false. *Unreal Engine* developers have put time and resources into projects reliant on *Unreal*  
17 *Engine*, and moving away would cause them significant harm. (Sweeney Reply ¶ 29.) And the  
18 removal from the market of one out of two primary engines currently available to developers  
19 would likewise harm developers for years to come. (*Id.* ¶¶ 29-30; Penwarden ¶ 10.)

20 Finally, in this context as well, Apple argues that the public harm is of Epic’s making.  
21 That is not the case, for all the reasons cited above. Epic properly refused to abide by unlawful  
22 agreements. It is Apple that removed *Fortnite* from the App Store. It is Apple that threatened to  
23 terminate access to tools used by other Epic businesses, including *Unreal Engine*. It is Apple  
24 that threatened to terminate agreements that were not breached governing accounts and apps that  
25 have nothing to do with *Fortnite*. Therefore, it is Apple that should be enjoined to prevent the  
26 harm to third parties relying on *Fortnite* and other Epic businesses, including *Unreal Engine*.

1 Dated: September 18, 2020

2 Respectfully submitted,

3 By: /s/ Katherine B. Forrest

4  
5 **FAEGRE DRINKER BIDDLE & REATH  
LLP**

6 Paul J. Riehle  
7 paul.riehle@faegredrinker.com

8 Four Embarcadero Center  
9 San Francisco, California 94111  
10 Telephone: (415) 591-7500  
11 Facsimile: (415) 591-7510

12 **CRAVATH, SWAINE & MOORE LLP**

13 Christine A. Varney (*pro hac vice*)  
14 cvarney@cravath.com  
15 Katherine B. Forrest (*pro hac vice*)  
16 kforrest@cravath.com  
17 Gary A. Bornstein (*pro hac vice*)  
18 gbornstein@cravath.com  
19 Yonatan Even (*pro hac vice*)  
20 yeven@cravath.com  
21 Lauren A. Moskowitz (*pro hac vice*)  
22 lmoskowitz@cravath.com  
23 M. Brent Byars (*pro hac vice*)  
24 mbyars@cravath.com

25 825 Eighth Avenue  
26 New York, New York 10019  
27 Telephone: (212) 474-1000  
28 Facsimile: (212) 474-3700

***Attorneys for Plaintiff***  
**EPIC GAMES, INC.**

1 Paul J. Riehle (SBN 115199)  
 paul.riehle@faegredrinker.com  
 2 **FAEGRE DRINKER BIDDLE & REATH LLP**  
 Four Embarcadero Center  
 3 San Francisco, California 94111  
 Telephone: (415) 591-7500  
 4 Facsimile: (415) 591-7510

5 Christine A. Varney (*pro hac vice*)  
 cvarney@cravath.com  
 6 Katherine B. Forrest (*pro hac vice*)  
 kforrest@cravath.com  
 7 Gary A. Bornstein (*pro hac vice*)  
 gbornstein@cravath.com  
 8 Yonatan Even (*pro hac vice*)  
 yeven@cravath.com  
 9 Lauren A. Moskowitz (*pro hac vice*)  
 lmoskowitz@cravath.com  
 10 M. Brent Byars (*pro hac vice*)  
 mbyars@cravath.com

11 **CRAVATH, SWAINE & MOORE LLP**  
 825 Eighth Avenue  
 12 New York, New York 10019  
 Telephone: (212) 474-1000  
 13 Facsimile: (212) 474-3700

14 *Attorneys for Plaintiff Epic Games, Inc.*

15 **UNITED STATES DISTRICT COURT**  
 16 **NORTHERN DISTRICT OF CALIFORNIA**  
 17 **OAKLAND DIVISION**

18 EPIC GAMES, INC.,

19 Plaintiff,

20 vs.

21 APPLE INC.,

22 Defendant.

No. 4:20-CV-05640-YGR

**DECLARATION OF TIMOTHY  
 SWEENEY IN FURTHER SUPPORT  
 OF PLAINTIFF EPIC GAMES, INC.'S  
 MOTION FOR A PRELIMINARY  
 INJUNCTION**

Date: September 28, 2020 at 9:30 a.m. (via  
 Zoom Platform)

Courtroom: 1, 4th Floor

Judge: Hon. Yvonne Gonzalez Rogers

1 I, Timothy Sweeney, declare as follows:

2 1. I am the founder and Chief Executive Officer of Epic Games, Inc. (“Epic”), the  
3 plaintiff in this action. I submit this declaration in further support of Epic’s Motion for a  
4 Preliminary Injunction. (ECF No. 61.) I also submitted a declaration in support of Epic’s Motion  
5 for a Preliminary Injunction on September 4, 2020 (ECF No. 65), in which I described Epic’s  
6 most popular and successful videogame, *Fortnite*, as well as a separate part of Epic’s business, a  
7 software suite available to third-party developers called *Unreal Engine*.

8 2. I have reviewed the submission of Apple Inc. (“Apple”) in opposition to Epic’s  
9 Motion for a Preliminary Injunction and noted a number of statements that are factually incorrect.  
10 While I will not address all of those statements in responding to Apple’s submission in this  
11 declaration, several are discussed below.

12 3. The contents of this declaration are based on my personal knowledge. If called as  
13 a witness, I could and would competently testify thereto.

14 **Fortnite and Cross-Platform Play**

15 4. The Declaration of Mike Schmid, dated September 15, 2020 (ECF No. 79) asserts  
16 that in September 2018, Epic violated Sony’s rules to force Sony to enable cross-platform play  
17 between Sony’s PlayStation 4 and Microsoft’s Xbox One (*id.* ¶ 19). That is false.

18 5. Cross-platform play allows users of different digital platforms to play together in  
19 the same online space, among personal computers, dedicated gaming consoles, and mobile  
20 devices like smartphones and tablets. Because circles of friends typically include users of  
21 different digital platforms, users on all platforms (as well as their videogame developers) benefit  
22 greatly from cross-platform features.

23 6. When *Fortnite* was officially released on PlayStation 4 and Xbox One in July  
24 2017, users of each of those gaming consoles were unable to play with users of the other console  
25 due to restrictions on cross-platform capabilities that were imposed by the console makers.

26 7. In early 2018, Epic approached Sony to advocate for cross-platform play and  
27 engaged Sony in business negotiations that spanned several months. On September 18, 2018,  
28 Epic and Sony signed an agreement on the launch of a Sony cross-platform beta program that



1 would enable play on *Fortnite* across a variety of platforms, including PlayStation 4, Android,  
2 iOS, Nintendo Switch, Xbox One, Microsoft Windows, and macOS operating systems. On  
3 September 26, 2018, Sony announced this program publicly, and later that day Epic launched the  
4 feature. Contrary to Mr. Schmid’s claim that Epic acted “explicitly against PlayStation’s rules”  
5 (*id.*), Epic did not breach any Sony or PlayStation rules by enabling cross-platform play in  
6 September 2018.

7 8. Attached hereto as **Exhibit A** is a true and correct copy of Sony’s September 26,  
8 2018 announcement of cross-platform features on *Fortnite*.

9 9. Sony’s beta program was a success and cross-platform functionality is now fully  
10 supported on PlayStation 4 and Xbox One. Many different game publishers now provide cross-  
11 platform play for popular multiplayer games, including Activision’s *Call of Duty: Warzone*,  
12 Microsoft’s *Minecraft*, and Electronic Arts’ *Need for Speed Heat*.

13 10. Apple’s papers also claim that because *Fortnite* is available on multiple platforms,  
14 iOS is not an important platform for *Fortnite*. (ECF No. 77, ¶ 27.) That is false. The fact that  
15 *Fortnite* can be played on multiple platforms does not mean that Apple’s iOS platform is not  
16 independently important to *Fortnite*. Each platform is important to *Fortnite* and iOS is  
17 particularly important for the reasons discussed herein. Cross-platform functionality is important  
18 specifically because it allows *Fortnite* to reach more users and allows users to play and share  
19 experiences with other users who have access only to different platforms.

20 11. Mr. Schmid also claims that unnamed “Epic personnel” threatened to “terminate”  
21 Epic’s relationship with Apple if Apple failed to comply with Epic’s routine requests for  
22 expedited review or propagation of its apps. (ECF No. 79, ¶ 18.) As discussed in more detail in  
23 the Declaration of Andrew Grant dated September 18, 2020, Epic did often make clear to Apple  
24 that if Apple’s review process extended beyond the launch deadline for a new *Fortnite* build, Epic  
25 would launch the new build on other platforms without the iOS platform being updated. Because  
26 *Fortnite* at that time required all platforms to run the latest version of the game, this would result  
27 in *Fortnite* on iOS being unavailable to users until Apple completed its review of the new build  
28 and allowed iOS users to access an updated app. Epic has investigated Mr. Schmid’s claim that



1 “Epic personnel have told [him] that if Apple did not comply with its demands, Epic would  
2 simply terminate its relationship with Apple and remove its games off of the iOS platform” (*id.*)  
3 and found no indication that such a thing was ever said. Epic never issued such a threat and never  
4 considered such termination.

5 12. Some of Apple’s assertions related to multi-platform play are contained in the  
6 declaration of Lorin Hitt, dated September 15, 2020 (ECF No. 77). Professor Hitt states that  
7 because *Fortnite* can be played on multiple platforms, users can “freely” and “seamlessly” switch  
8 between the various platforms on which *Fortnite* is available. (*Id.* § 3.1.2.) I do not agree.

9 13. Non-mobile platforms like gaming consoles and PCs are simply not substitutes for  
10 mobile device access to *Fortnite*. It does not require an expert to establish that a home-based  
11 desktop computer is not a substitute for a personal smartphone in terms of quickly and easily  
12 accessing email or using banking software regardless of the user’s location. Similarly, dedicated  
13 gaming consoles and PCs are not substitutes for mobile phones for gaming: PCs and gaming  
14 consoles are too large to be transported with ease and require a connection to a power supply.  
15 Simply put: You cannot carry a PlayStation in your pocket.

16 14. Gaming consoles and many PCs require electrical outlets and connection to  
17 dedicated screens. PCs and gaming consoles also require a Wi-Fi or wired Internet connection in  
18 order for consumers to play online with others. By contrast, mobile devices are easily portable,  
19 battery operated, cellularly connected, and have screens integrated into them. If a consumer is in  
20 transit, is away from home, or does not have access to a reliable wired or Wi-Fi Internet  
21 connection, playing *Fortnite* on a dedicated gaming console or a PC is not an option. If the  
22 consumer wants to play *Fortnite* in those circumstances, he or she will need to play on a mobile  
23 device. Moreover, there are typically many more mobile devices per household than computer or  
24 gaming consoles. For example, if one family member is playing on PlayStation 4 or watching a  
25 show on the television connected to the PlayStation 4, then the others would need to play on their  
26 mobile phone.

27 15. I attached to my prior declaration (dated September 4, 2020) examples of  
28 consumers who had contacted our customer service group after Apple delisted *Fortnite* from the

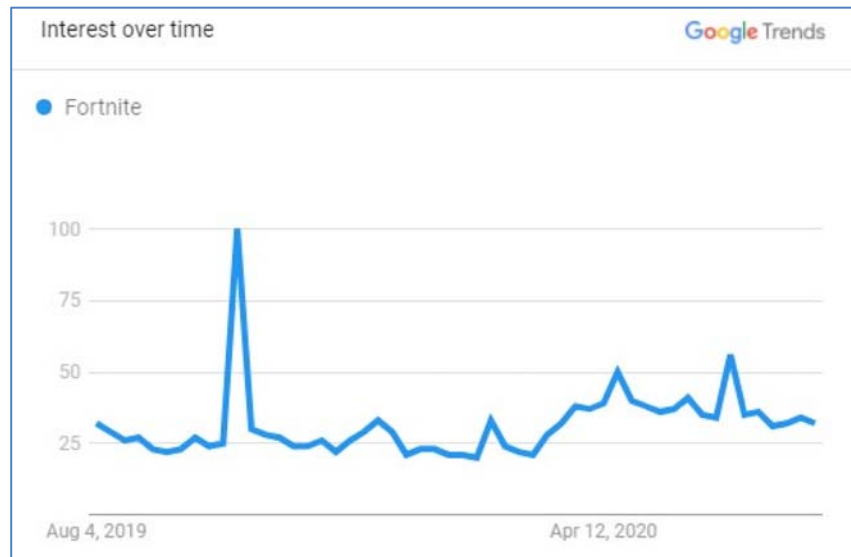
1 App Store, and said that their iPhone or iPad was the only way they had to play the game. (ECF  
2 No. 65-5.) Some expressed an inability to afford a second platform. (*Id.*)

3 16. The fact that gaming consoles or PCs are not substitutable for mobile devices is  
4 borne out by the data. There are vastly more mobile devices currently in use than there are  
5 dedicated gaming consoles. According to publicly reported figures, while there are  
6 approximately 1 billion active iPhone users, the total combined number of PlayStation 4, Xbox  
7 One, and Nintendo Switch gaming consoles is under 300 million.

8 17. *Fortnite* gaming experiences are also differentiated on dedicated gaming consoles  
9 and mobile devices. What dedicated gaming consoles and PCs lack in mobility, they make up for  
10 in performance. PCs and consoles typically offer faster processing, larger screens, better  
11 graphics, and better controls than mobile devices do. Because of these differences, I would  
12 expect players to prefer playing on a console if one is available to them. Yet our data shows that  
13 63% of *Fortnite* users on iOS play exclusively on iOS, which suggests that many iOS users do  
14 not have access to a gaming console or a PC offering a better experience.

15 **Fortnite's Continued Popularity**

16 18. In its brief, Apple claims that “[b]y July 2020, interest in *Fortnite* had decreased  
17 by nearly 70% as compared to October 2019”. (ECF No. 73 at 11.) This is misleading. To  
18 support this statistic, Apple cites to Google Trends data, which tracks *not* the number of users  
19 actually playing *Fortnite*, but instead the number of daily Google searches for *Fortnite*. In order  
20 to come up with a 70% decline, Apple cherry-picked an unusual single-week peak in October  
21 2019 with the average number of searches in July 2020, as shown in the chart below:  
22  
23  
24  
25  
26  
27  
28



10 Google Trends, [https://trends.google.com/trends/explore?date=2019-08-01%202020-07-](https://trends.google.com/trends/explore?date=2019-08-01%202020-07-31&geo=US&q=Fortnite#TIMESERIES)  
11 [31&geo=US&q=Fortnite#TIMESERIES](https://trends.google.com/trends/explore?date=2019-08-01%202020-07-31&geo=US&q=Fortnite#TIMESERIES) (last visited Sept. 18, 2020). Apple is aware that the  
12 peak in this Google search data corresponds with a two-day in-game *Fortnite* event in October  
13 2019 called “The End”, which amassed record-breaking viewership on Twitter, Twitch, and  
14 YouTube as the world of *Fortnite* was swallowed by a black hole.



24 19. Epic’s actual user engagement data reflecting the actual number of users playing  
25 *Fortnite* (not Google search results) shows Apple’s claim of declining interest in *Fortnite* to be  
26 incorrect. Over the period of time that Apple cherry-picked for its Google search volume  
27 comparison (between October 2019 and July 2020), the number of daily active users on *Fortnite*  
28 actually *increased* by more than 39%.

1 **Apple's Marketing of the DJ Marshmello Event**

2 20. Mr. Schmid's declaration states that Apple "placed billboards in New York's  
3 Times Square and LA Live to promote an in-app *Fortnite* concert with DJ Marshmello". (ECF  
4 No. 79 ¶ 11.) This statement is inaccurate.

5 21. The billboards actually promoted Apple's own Apple Music app and service,  
6 which offered a playlist containing music that DJ Marshmello had performed in a *Fortnite*  
7 concert.

8 22. An image of Apple's billboard in Times Square that DJ Marshmello posted on  
9 Twitter following the concert is attached as **Exhibit B**.

10 **Purchases Within *Fortnite* and Epic Games Stores**

11 23. Apple claims that its in-app purchase requirements are "hardly unique" and states  
12 that "Epic's own app marketplace charges users and developers a commission". (ECF No. 73 at 6  
13 & n.7.) This is inaccurate because it mixes store sales and in-game purchases.

14 24. The Epic website cited by Apple describes *software sales*, not in-game purchases.  
15 As stated in my declaration of September 4, 2020 (ECF No. 65), Epic provides developers who  
16 distribute their software through the Epic Games Store (including free games distributed at no  
17 charge) the freedom to choose their in-game purchase payment processor without any payment to  
18 Epic. (*Id.* ¶ 10.)

19 **Unreal Engine**

20 25. The dispute between Epic and Apple concerns the distribution and payment  
21 options for and in *Fortnite*, an entirely different product from *Unreal Engine* or Epic's other non-  
22 game products.

23 26. Apple has asserted that Epic might use *Unreal Engine* as a vehicle for the insertion  
24 of malware or other code intended to breach contractual obligations with Apple. (ECF No. 73  
25 at 28.) But as described in more detail in my prior declaration (ECF No. 65) and in the  
26 Declaration of Nicholas Penwarden, dated September 4, 2020 (ECF No. 64) (the "Penwarden  
27 Declaration"), *Unreal Engine* is not an iOS app. It is a development tool that has been used to  
28 create software and content on multiple platforms, including Apple iOS, for over ten years.

1 *Unreal Engine* is licensed and trusted as a software foundation by companies including  
2 Microsoft, Sony, Nintendo, Electronic Arts and Activision. Neither *Unreal Engine* nor any other  
3 Epic product was ever used by Epic as a vehicle to insert malware or other malicious code onto  
4 any platform. Epic never has and never will intentionally insert malware or other malicious code  
5 onto any platform.

6 27. Epic has taken issue with a particular set of payment processing rules that it  
7 believes are illegal and unenforceable. Epic will continue to comply with all contractual  
8 obligations with Apple relating to its non-game products and services, including *Unreal Engine*,  
9 during the pendency of this lawsuit.

10 **Competition to Unreal Engine**

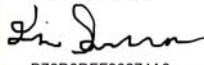
11 28. Apple also suggests that *Unreal Engine* is easily replaceable with *Unity*, another  
12 development platform. This argument is incorrect.

13 29. As described in more detail in the Penwarden Declaration, *Unreal Engine*  
14 developers have invested significant time and resources into projects reliant on *Unreal Engine*,  
15 and moving away from it would thus cause them significant harm. (ECF No. 64, ¶ 10.)

16 30. In addition, *Unity* is the only major competitive licensable alternative to *Unreal*  
17 *Engine*. As a result, eliminating *Unreal Engine* would mean that developers would have  
18 significantly less choice than before, and competition would be harmed. Therefore, if Apple is  
19 allowed to prevent iOS development on *Unreal Engine*, all developers would suffer.

20  
21 Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true  
22 and correct and that I executed this declaration on September 18, 2020, in Cary, North Carolina.

23 DocuSigned by:

24 

B76D8DFF30274A8...

25 Timothy Sweeney

# **Exhibit A**

September 26, 2018

## Extended Fortnite Cross-Play Beta Launches on PS4 Starting Today

333 0 132



Cross-platform features are coming to PS4.



John Kodera  
Deputy President, SIE

Following a comprehensive evaluation process, SIE has identified a path toward supporting cross-platform features for select third party content. We recognize that PS4 players have been eagerly awaiting an update, and we appreciate the community's continued patience as we have navigated through this issue to find a solution.

The first step will be an open beta beginning today for Fortnite that will allow for cross platform gameplay, progression and commerce across PlayStation 4, Android, iOS, Nintendo Switch, Xbox One, Microsoft Windows, and Mac operating systems. We see the beta as an opportunity to conduct thorough testing that ensures cross-platform play is best on PlayStation, while being mindful about the user experience from both a technical and social perspective.

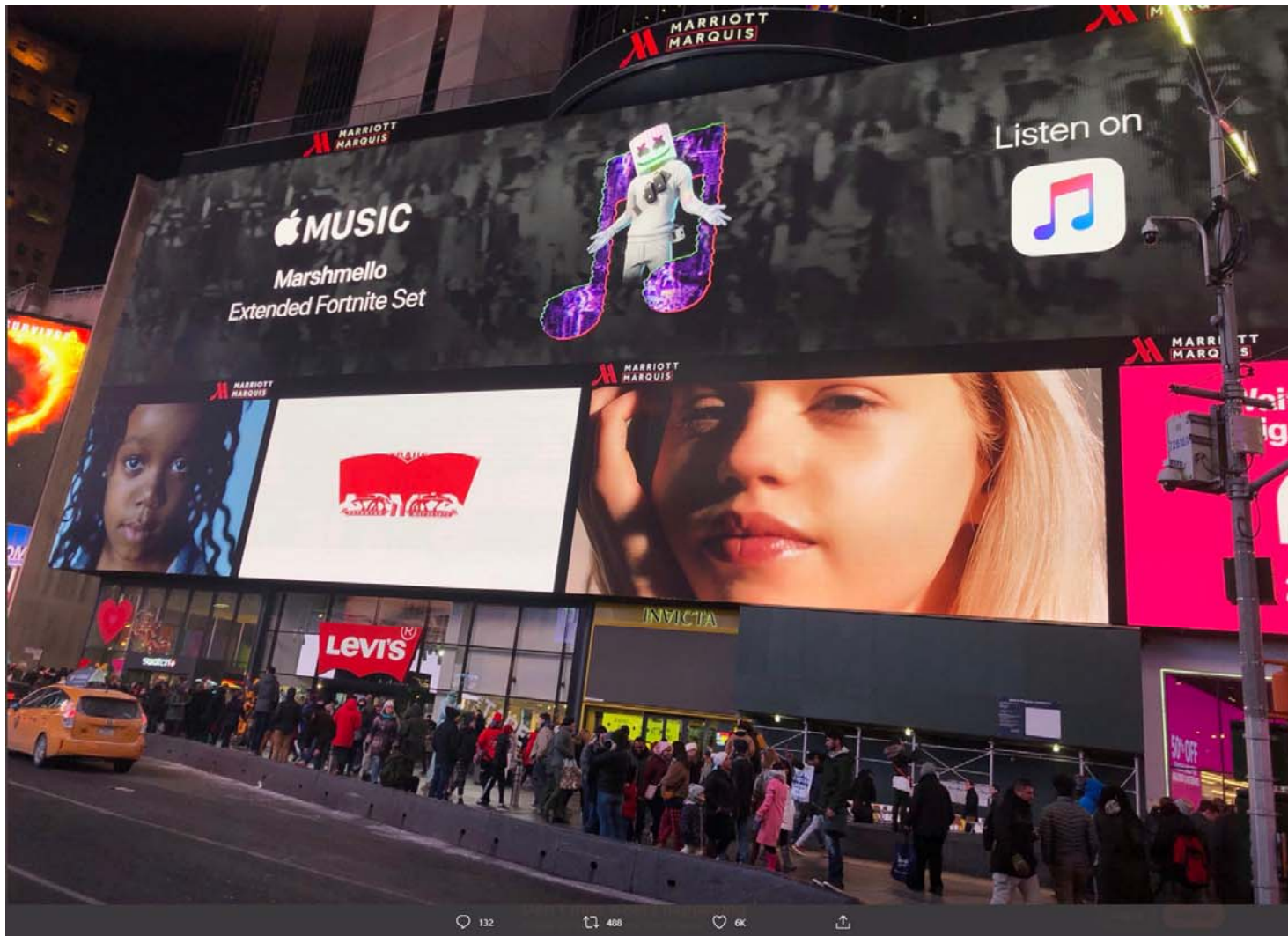
For 24 years, we have strived to deliver the best gaming experience to our fans by providing a uniquely PlayStation perspective. Today, the communities around some games have evolved to the point where cross-platform experiences add significant value to players. In recognition of this, we have completed a thorough analysis of the business mechanics required to ensure that the PlayStation experience for our users remains intact today, and in the future, as we look to open up the platform.

This represents a major policy change for SIE, and we are now in the planning process across the organization to support this change. We will update the community once we have more details to share, including more specifics regarding the beta timeframe, and what this means for other titles going forward.

In the meantime, please stay tuned for more information via PlayStation.Blog and social channels, including [Twitter](#), [Facebook](#), and [Instagram](#)



# **Exhibit B**



**marshmello** @marshmellomusic

Yesterday was incredible! If you wanna hear more, go check out @AppleMusic for my Extended Fortnite Set [apple.co/2WCBgAt](https://apple.co/2WCBgAt)

11:21 AM · Feb 3, 2019 · Twitter for iPhone

471 Retweets 17 Quote Tweets 6K Likes

**WitnessMe** @WitnessMe · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
Rreecerr

**Ryan** @RyanMa... · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
When spotify

**Ahmed Hesham** · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
Bro i love u

**quit** @CrwzEpic · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
Marsh ur a legend

**Zach Payne** @z... · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
Yo

**Zack** @MrDead... · Feb 3, 2019

Replying to @marshmellomusic and @AppleMusic  
That was amazing man thanks for the experience

This Tweet was deleted by the Tweet author. [Learn more](#)

**STEEZY** @Steez... · Feb 3, 2019

132 488 6K

1 Paul J. Riehle (SBN 115199)  
paul.riehle@faegredrinker.com  
2 **FAEGRE DRINKER BIDDLE & REATH LLP**  
Four Embarcadero Center  
3 San Francisco, California 94111  
Telephone: (415) 591-7500  
4 Facsimile: (415) 591-7510

5 Christine A. Varney (*pro hac vice*)  
cvarney@cravath.com  
6 Katherine B. Forrest (*pro hac vice*)  
kforrest@cravath.com  
7 Gary A. Bornstein (*pro hac vice*)  
gbornstein@cravath.com  
8 Yonatan Even (*pro hac vice*)  
yeven@cravath.com  
9 Lauren A. Moskowitz (*pro hac vice*)  
lmoskowitz@cravath.com  
10 M. Brent Byars (*pro hac vice*)  
mbyars@cravath.com

11 **CRAVATH, SWAINE & MOORE LLP**  
825 Eighth Avenue  
12 New York, New York 10019  
Telephone: (212) 474-1000  
13 Facsimile: (212) 474-3700

14 *Attorneys for Plaintiff Epic Games, Inc.*

15 **UNITED STATES DISTRICT COURT**  
16 **NORTHERN DISTRICT OF CALIFORNIA**  
17 **OAKLAND DIVISION**

19 EPIC GAMES, INC.,

20 Plaintiff,

21 vs.

22 APPLE INC.,

23 Defendant.

No. 4:20-CV-05640-YGR

**DECLARATION OF ANDREW  
GRANT IN FURTHER SUPPORT OF  
PLAINTIFF EPIC GAMES, INC.'S  
MOTION FOR PRELIMINARY  
INJUNCTION**

Date: September 28, 2020, 9:30 a.m. (via  
Zoom Platform)

Courtroom: 1, 4th Floor

Judge: Hon. Yvonne Gonzalez Rogers

1 I, Andrew Grant, declare as follows:

2 1. I am a Technical Director of Engineering at Epic Games, Inc. (“Epic”), the  
3 plaintiff in this action. I submit this declaration in further support of Epic’s Motion for a  
4 Preliminary Injunction. (ECF No. 61.) I also submitted a declaration in support of Epic’s Motion  
5 for a Preliminary Injunction on September 4, 2020 (ECF No. 63), in which I described my  
6 background, current position, and job responsibilities.

7 2. I have reviewed Apple Inc.’s (“Apple”) submission in opposition to Epic’s Motion  
8 for a Preliminary Injunction. In this declaration I address certain claims made by Apple related to  
9 (i) Epic’s continued use of the Sign in with Apple (“SiwA”) functionality, (ii) Epic’s interactions  
10 with Apple when *Fortnite* was still available through the App Store, and (iii) some of the  
11 consequences of Apple’s decision to terminate Epic’s Team ID ’84 account.

12 3. The contents of this declaration are based on my personal knowledge. If called as  
13 a witness, I could and would competently testify thereto.

14 **Sign in with Apple**

15 4. Apple suggests in its brief (ECF No. 73 at 13) as well as in a letter attached to the  
16 Declaration of Jay B. Srinivasan, dated September 15, 2020 (ECF No. 80), that despite  
17 terminating Epic’s Team ID ’84 developer account, Apple has acted magnanimously by  
18 preserving the ability of Epic’s users to continue using the SiwA functionality that was associated  
19 with the Team ID ’84 account.

20 5. Epic was never given a choice as to whether or not to implement SiwA. A change  
21 in Apple’s App Store Review Guidelines required it, and Epic had to comply. And SiwA is tied  
22 to *Fortnite* and Epic’s Team ID ’84 account across all Epic services because Apple did not allow  
23 Epic to implement it any other way.

24 6. In June 2019, Apple announced at its annual Worldwide Developers Conference  
25 that it would be launching a new service, SiwA, in connection with the launch of iOS 13. Similar  
26 to services offered by companies like Facebook and Google, SiwA allows Apple users to set up  
27 accounts for participating apps and websites using their Apple credentials. Specifically, using  
28 SiwA, an Apple user can set up an account with a participating app using the user’s Apple ID

1 (which is an email address) and password, instead of creating new, separate login credentials.  
2 Alternatively, users can set up an account using a private email relay address generated by SiwA,  
3 rather than using their actual email address. Either way, SiwA allows users to create accounts for  
4 participating apps without providing the app developer identification and authentication  
5 information such as name and email address; that information remains with Apple, and it is  
6 therefore Apple, rather than the app developer, that controls the relationship with the user.

7 7. When SiwA officially launched in September 2019, Apple updated its App  
8 Review Guidelines to require that “[a]pps that use a third-party or social login service . . . to set  
9 up or authenticate the user’s primary account with the app must also offer [SiwA] as an  
10 equivalent option”. (ECF No. 61-17 § 4.8.) Epic already offered Epic users, including *Fortnite*  
11 users on iOS, the option to log in into their Epic accounts with several different third-party login  
12 services, such as Google and Facebook. Under the revised App Review Guidelines, Epic was  
13 therefore required to implement SiwA. Apple originally gave developers like Epic until April  
14 2020 to update existing iOS apps to support SiwA, but subsequently extended the deadline until  
15 June 30, 2020.

16 8. Epic offers users a multi-platform, multi-product account system for all of its  
17 offerings, including *Fortnite*, the Epic Games Store, Epic Online Services, and *Unreal Engine*.  
18 When a user engages with an Epic product or service for the first time, they create an Epic  
19 account that they can then use to access any of Epic’s other products and services. For example,  
20 a user who creates an Epic account to play *Fortnite* on an iOS device would use the same account  
21 to purchase and play third-party PC games through the Epic Games Store or to access and  
22 download *Unreal Engine*. Users benefit from this multi-platform, multi-product system because  
23 they do not have to manage multiple accounts (including multiple usernames and passwords) with  
24 Epic.

25 9. If users were only able to use SiwA to create or log in to their Epic account for  
26 *Fortnite*, or do so only on iOS devices, Epic’s multi-product, multi-platform account system  
27 would quickly splinter and break down. Therefore, in order to implement SiwA as a supported  
28 login method for the iOS version of *Fortnite*, Epic had to implement SiwA for all of the products

1 and services in its ecosystem.

2 10. Epic began taking steps to implement SiwA as a supported login method for Epic  
3 accounts in February 2020. As Apple had set up the system, however, SiwA would not work  
4 unless it was associated with a designated app that was available in the App Store. In addition, it  
5 was my understanding that whenever SiwA was used, it would show the logo for that primary  
6 app. This posed a problem for Epic, because Epic intended to use SiwA across its entire  
7 ecosystem, and therefore preferred not to tie it to any particular app such as *Fortnite*, let alone to  
8 have users be shown the logo of that app even if they use their Epic account with a different Epic  
9 service or product. For example, Epic wanted to prevent a situation where an *Unreal Engine* user  
10 who created their Epic account on the *Unreal Engine* website using SiwA, would nonetheless see  
11 the *Fortnite* logo every time they logged into their account, even if that user never used their  
12 account to play *Fortnite*.

13 11. Between March and June 2020, Epic reached out to Apple on at least seven  
14 occasions requesting Apple's permission to implement SiwA without tying it to *Fortnite* or any of  
15 its other apps. Epic proposed several different technical workarounds to Apple, but Apple  
16 declined to provide Epic with any guidance about how to implement SiwA without associating it  
17 with a primary app from the App Store. Finally, in June 2020, Apple informed Epic that SiwA  
18 must be associated with an individual app available in the App Store. Given the imminent  
19 deadline for compliance with Apple's SiwA policy, Epic had to move forward with implementing  
20 SiwA as functionality tied to *Fortnite* and the Team ID '84 account.

21 12. On July 14, 2020, Epic added SiwA to its account portal as a new login method.  
22 Three days later, on July 17, 2020, Epic submitted its first *Fortnite* build that supported SiwA to  
23 Apple for review. (Epic met Apple's June 30 deadline for SiwA implementation because the  
24 July 17 submission was the first new build it had submitted to Apple following the deadline.)

25 13. Apple approved the July 17 build and it was released to iOS users. But on July 21,  
26 2020, Apple notified Epic that its build was not technically compliant with its SiwA policy.  
27 Specifically, Apple complained that after a new iOS user created an Epic account using SiwA,  
28 Epic prompted the user to provide their date of birth, country, full name, password, and an email



1 verification to complete the setup of their Epic account. Apple told Epic that the collection of this  
2 information violated the App Store Review Guidelines, and gave Epic until August 24, 2020 to  
3 cure. Epic subsequently sought guidance from Apple about how to bring *Fortnite* back into  
4 compliance, but Apple would not provide Epic with the requested information.

5 14. Ultimately, to reduce the risk that Apple would reject future *Fortnite* builds, Epic  
6 complied with Apple's guidelines by changing the flow for SiwA account creation so that Epic  
7 only collected a "Display Name" and date of birth from SiwA users. As a result, to try to comply  
8 with Apple's guidelines, Epic did not collect information from SiwA users (such as a separate  
9 Epic password or an email account) that would allow users to access their Epic account in the  
10 event that SiwA ceased to function or a user lost access to their Apple account.

11 15. Following the implementation of SiwA, hundreds of thousands of users set up  
12 Epic accounts using SiwA. Approximately 40,000 users created an Epic account using just their  
13 Apple ID and never created a separate Epic account password. Another 350,000 users created an  
14 Epic account using a private email relay address generated by SiwA. A "relay" address means a  
15 computer generated email account that relays emails to the user's actual email address, which  
16 Apple maintained but that was never disclosed to Epic.

17 16. Following Apple's August 14, 2020 threat to terminate Epic's developer accounts  
18 on August 28, 2020, Epic became concerned that following the termination of the Team ID '84  
19 account, SiwA users would lose access to their Epic accounts. If SiwA were disabled, users who  
20 had never created a separate Epic account password would lose access to their accounts until they  
21 created a password using their email on file, while users who had elected to use a private relay  
22 email address would only be able to access their accounts if they happened to remember the relay  
23 email address. This would not only affect these users' ability to play *Fortnite* or other Epic  
24 games, but also would impair their access to the Epic Games Store, Epic Online Services, and  
25 *Unreal Engine*. As a result, users could lose access to their existing purchases from Epic.

26 17. On August 27, 2020, Epic's outside counsel wrote to Apple's outside counsel to  
27 explain that if Apple terminated Epic's Team ID '84 account and disabled SiwA it would impact  
28 "third-party game developers whose Epic Games Store customers use [SiwA], Epic account

1 owners who use [SiwA] to access third-party games, and third-party developers who access the  
2 Unreal Engine using [SiwA]”. (Byars Reply Decl. Ex. A at 1.) Epic’s counsel requested “that  
3 Apple confirm that it will not take any steps that impair [SiwA for] third-parties who rely on Epic  
4 services”. (*Id.* at 2.) The following day, Apple’s counsel replied that “[SiwA] will continue to  
5 function for Apple customers for the next two weeks”, but not beyond that. (Byars Reply Decl.  
6 Ex. B at 1.) Apple’s counsel also stated that “[i]f Epic’s engineers have questions of Apple’s,  
7 they have worked together in the past and Epic knows how to reach them”. (*Id.*)

8 18. Given Apple’s response, on August 28, 2020, Epic sent an email to Apple seeking  
9 assistance with migrating SiwA to a different Apple Developer Account and guidance “on next  
10 steps to do so without breaking the process for users”. Apple did not immediately reply to Epic’s  
11 email. Attached hereto as **Exhibit A** is a true and correct copy of Epic’s August 28, 2020 email  
12 to Apple.

13 19. On September 1, 2020, Epic sent a follow-up email to Apple requesting that Apple  
14 confirm receipt of Epic’s August 28 email and “provide guidance on next steps”. Attached hereto  
15 as **Exhibit B** is a true and correct copy of Epic’s September 1, 2020 email to Apple.

16 20. On September 2, 2020, because Apple did not respond to Epic’s outreach, Epic’s  
17 outside counsel sent another email to Apple’s outside counsel to inform them that Epic had not  
18 heard back from Apple about migrating SiwA to a different developer account. (Byars Reply  
19 Decl. Ex. C at 1.) Epic’s counsel requested that “Apple personnel contact Epic tomorrow, so that  
20 the parties can resolve this issue without the need to bring it to the Court”. (*Id.*)

21 21. On September 3, 2020, Apple’s Game Developer Manager Mark Grimm replied to  
22 Epic’s September 1 email. Grimm stated that “we cannot migrate your implementation of [SiwA]  
23 to another developer account” and suggested that Epic “build a custom flow to migrate users off  
24 [SiwA] by collecting email addresses or asking users to select a different login method”.  
25 Attached hereto as **Exhibit C** is a true and correct copy of Apple’s September 3, 2020 email.

26 22. Upon receipt of Mr. Grimm’s email, Epic began to develop internally a process by  
27 which it could transition SiwA users to alternative login methods. Epic originally estimated that  
28 it would take a month of work to complete the project and fully transition the existing SiwA



1 users.

2 23. On September 8, 2020, Epic's outside counsel sent an email to Apple's outside  
3 counsel requesting that Apple extend its original two-week deadline to give Epic more time to  
4 reach out to SiwA users and transition them to alternative login methods. (Byars Reply Decl. Ex.  
5 D.) Epic requested that Apple confirm its agreement to an extension that evening, so as to guide  
6 any communications with users. Apple did not provide such confirmation on September 8.  
7 Accordingly, on the eve of September 8, Epic wrote to all SiwA users notifying them that Apple  
8 would be terminating SiwA on September 11, 2020 and instructing them to update the email  
9 and/or password for their Epic account.

10 24. On September 10, 2020, less than 24 hours before the expiration of Apple's threat  
11 to terminate SiwA, Apple's outside counsel wrote to Epic's outside counsel, stating that "Apple  
12 will leave [SiwA] in place for the time being". (Byars Reply Decl. Ex. E at 1.) Apple has not  
13 committed not to terminate SiwA at any point in the future, and Epic therefore is continuing its  
14 efforts to migrate users off of SiwA.

15 **Fortnite in the App Store**

16 25. The Declaration of Mike Schmid, dated September 15, 2020 (ECF No. 79), cites a  
17 long list of supposed benefits and accommodations Epic has received from Apple in the course of  
18 distributing *Fortnite* and its other games through the Apple App Store. Apple's account omits  
19 certain important details.

20 26. Until Apple removed *Fortnite* from the App Store, Epic required that all platforms  
21 run the same version of *Fortnite*. As described in more detail in the Declaration of Timothy  
22 Sweeney, dated September 4, 2020, ¶ 8 (ECF No. 65), the requirement that users run the same  
23 version of *Fortnite* is critical to enable cross-platform play. The regular release of new content  
24 and updates through new versions or builds is also an essential feature of the *Fortnite* user  
25 experience. Today, however, given Apple's actions, Epic supports iOS users (and Android users  
26 who have downloaded *Fortnite* through Google Play) to continue using an outdated and limited  
27 version of *Fortnite* because those users are no longer able to receive updates for their apps.

28 27. When *Fortnite* was still available through the App Store, there was a constant

1 struggle with Apple to ensure that new iOS versions of *Fortnite* would be released on the same  
2 schedule as on other platforms. In Epic’s experience, Apple’s approval process for new builds is  
3 the slowest of all the platforms that require approval for new *Fortnite* builds. Updates would  
4 often be rejected by Apple because a review would take issue with functionality or wording that  
5 had been in *Fortnite* for some time. To try and meet its launch deadline across all platforms, Epic  
6 often needed to request that Apple expedite the review of new *Fortnite* builds. Epic took the  
7 clear position with Apple that it would give Apple every chance to approve builds in a timely  
8 fashion, but if Apple was unable to do so, Epic would not hold up the release of new *Fortnite*  
9 builds on other platforms while Apple’s approval process lagged behind. In the event Apple was  
10 unable to timely approve a new *Fortnite* build, Epic was prepared to put the iOS version of  
11 *Fortnite* into “downtime”—meaning temporarily take the game offline on iOS devices until the  
12 new build is approved by Apple—to allow other platforms to receive updates while Apple  
13 approval was still pending. Mr. Schmid’s assertion that “Epic personnel have told me that if  
14 Apple did not comply with its demands, Epic would simply terminate its relationship with Apple  
15 and remove its games off of the iOS platform” (ECF No. 79 ¶ 18) is incorrect. To my knowledge,  
16 Epic did not threaten to terminate its relationship with Apple and remove its games from the App  
17 Store if Apple failed to comply with Epic’s requests for expedited review or propagation of its  
18 apps.

19 28. It should be noted that the delay in Apple’s review process was not typically  
20 caused by a long review time. Rather, Apple’s developer portal would often show that new  
21 builds were “waiting for review” for days. Once in review, however, the actual process could  
22 take as little as a few minutes. On a handful of occasions, Epic also needed to submit expedited  
23 propagation requests because new *Fortnite* builds that had *already been approved* by Apple’s  
24 review process were for some unknown reason not made available to users through the App Store  
25 in a timely manner.

26 29. Over the years, Epic has spent considerable engineering time and resources  
27 supporting requirements or requests from Apple related to *Fortnite*. One example is Epic’s  
28 months-long project described above to implement SiwA for *Fortnite* in order to comply with

1 Apple’s App Review Guidelines. On numerous occasions, Epic has optimized or made  
2 improvements to *Fortnite* to improve its performance on iOS devices at the request of Apple.  
3 And Epic spent more than a year updating *Fortnite*’s code to make it compatible with the  
4 reduction of memory resources that Apple imposed on developers with the launch of iOS 12. At  
5 Apple’s request, and like many developers with hugely popular apps like *Fortnite*, Epic has also  
6 regularly provided Apple with free marketing materials to support their marketing for devices and  
7 other services.

### 8 **iOS Security**

9 30. In its brief and supporting declarations, Apple invokes the security benefits for the  
10 iOS ecosystem that Apple says flow from Apple’s review process. In my experience, there is no  
11 reason to believe that it is the best or only way to maintain the security of the iOS ecosystem.

12 31. The critical security protection provided by iOS is the result of the hardware and  
13 operating system of the device. Apple engineers deserve credit for building these security  
14 features into the earliest versions of the iPhone, enhancing them with every new release of the  
15 operating system and hardware.

16 32. On iOS, third-party apps are isolated (or “sandboxed”) by the operating system.  
17 This isolation strictly prevents an app from reading or changing data belonging to other apps, or  
18 from accessing sensitive data held by the OS itself.

19 33. Access to areas that are permitted but considered sensitive—for example, Photo  
20 Albums, Contacts, Microphone, Camera, sending of text messages—is controlled by a robust  
21 permissions based security system. An app must make a specific API request to the operating  
22 system. The operating system in turn presents the user with a standard and easily understood  
23 message such as “<app-name> Would Like to Access Your Contacts”.

24 34. If the user declines this request then the app is not granted access to that data. It  
25 cannot bypass the message, or change the message to trick them into a more favorable response.  
26 Once denied, a user must proactively grant permission to an application by going into device  
27 settings and enabling access.

28 35. Were it possible for applications to capture sensitive data or wreak havoc on

1 telephony systems, such behavior would be trivial to hide from review.

2 **Apple's Termination of the Team ID '84 Account**

3 36. As I described in my prior declaration, on August 28, 2020, Apple terminated  
4 Epic's Team ID '84 Account, removed all associated apps from the App Store and Mac App  
5 Store (other than *Fortnite*, which had already been removed), and informed Epic that "we will  
6 deny your reapplication to the Apple Developer Program for at least a year". (ECF No. 63 ¶ 35.)

7 37. Apple complains that Epic has continued to use Apple's proprietary software.  
8 (Declaration of Phil Schiller, ECF No. 74 ¶ 69.) As a result of the termination of Epic's Team ID  
9 '84 account, Epic is no longer able to use the account to access certain Apple software, including  
10 Apple's TestFlight software for beta testing iOS or macOS apps. Apple software may still be  
11 accessed and used through developer accounts associated with *Unreal Engine* and other products,  
12 which Apple has not terminated. To be clear, since Apple terminated the Team ID '84 account,  
13 Epic can no longer use that account to access Apple's Developer Portal or otherwise access or use  
14 TestFlight. Epic programmers are still able to use Apple software tools they downloaded under  
15 separate SDK Agreements, which they use to continue development of products unrelated to the  
16 Team ID '84 account.

17 38. Apple also complains that Epic is still collecting money from iOS users at Apple's  
18 expense. (*Id.* ¶ 68.) But Apple blocked purchases through Apple's system ("IAP") in *Fortnite*  
19 with the termination of the Team ID '84 account. When the *Fortnite* app is opened on an iOS  
20 device, the app queries Epic's and Apple's servers to retrieve information about available  
21 purchases through Epic direct payment and Apple IAP, respectively. Since the termination of the  
22 Team ID '84 account, however, when the *Fortnite* app queries Apple's servers it receives "error"  
23 values rather than information about available purchases. As a result, the app is not able to  
24 receive information from Apple's servers that is necessary to process purchases using Apple IAP.

25 39. In order to avoid user confusion, the *Fortnite* app is programmed to present users  
26 with only functioning payment options. For this reason, the app currently displays only the Epic  
27 direct payment option to users while Apple IAP is non-functioning. This is an automatic and  
28 standard feature of the *Fortnite* app's coding. Epic has not made any changes to the app that have

1 resulted in Apple IAP becoming unavailable. Further, it is not possible for Epic to reinstate  
2 Apple IAP in *Fortnite* unless and until Apple restores the ability of the app to receive information  
3 about available purchases from Apple’s servers.

4  
5 Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true  
6 and correct and that I executed this declaration on September 18, 2020, in Holly Springs, North  
7 Carolina.

8  
9 DocuSigned by:  
  
10 E 16259185181495...  
Andrew Grant

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# **Exhibit A**



Alec Shobin <[REDACTED]@epicgames.com>

---

## Epic Games SiwA Migration

---

Alec Shobin <[REDACTED]@epicgames.com>

Fri, Aug 28, 2020 at 10:58 PM

To: Mark Grimm <[REDACTED]@apple.com>, Robert Partington <[REDACTED]@apple.com>

Cc: Jamal Fanaian <[REDACTED]@epicgames.com>, Graham Logan <[REDACTED]@epicgames.com>, Andrew Grant

[REDACTED]@epicgames.com>

Hey Mark,

We'd like to immediately migrate our existing Sign in with Apple from the terminated Epic Games Inc. account '84 and to a different, new account specifically for this purpose (or provide other guidance to us). Please advise on next steps to do so without breaking the process for users.

Thanks,

Alec

--

Alec Shobin

Publishing, Mobile | Epic Games



# **Exhibit B**



Alec Shobin <REDACTED@epicgames.com>

---

## Epic Games SiwA Migration

---

Alec Shobin <REDACTED@epicgames.com>

Tue, Sep 1, 2020 at 10:36 AM

To: Mark Grimm <REDACTED@apple.com>, Robert Partington <REDACTED@apple.com>

Cc: Jamal Fanaian <REDACTED@epicgames.com>, Graham Logan <REDACTED@epicgames.com>, Andrew Grant <REDACTED@epicgames.com>

Hi Mark and Robert,

Following up on this. Can you confirm receipt and provide guidance on next steps?

Thank you,

-Alec

On Fri, Aug 28, 2020 at 10:58 PM Alec Shobin <REDACTED@epicgames.com> wrote:

Hey Mark,

We'd like to immediately migrate our existing Sign in with Apple from the terminated Epic Games Inc. account '84 and to a different, new account specifically for this purpose (or provide other guidance to us). Please advise on next steps to do so without breaking the process for users.

Thanks,

Alec

--

Alec Shobin  
Publishing, Mobile | Epic Games

--

Alec Shobin  
Publishing, Mobile | Epic Games

# Exhibit C



Alec Shobin <REDACTED@epicgames.com>

---

## Epic Games SiwA Migration

---

Mark Grimm <REDACTED@apple.com>

Thu, Sep 3, 2020 at 2:50 PM

To: Alec Shobin <REDACTED@epicgames.com>

Cc: Robert Partington <REDACTED@apple.com>, Jamal Fanaian <REDACTED@epicgames.com>, Graham Logan <REDACTED@epicgames.com>, Andrew Grant <REDACTED@epicgames.com>

Dear Alec,

With the termination of Epic Games Inc.'s developer account, we cannot migrate your implementation of Sign In with Apple to another developer account. Instead, I would recommend that your team build a custom flow to migrate users off Sign In with Apple by collecting email addresses or asking users to select a different login method.

Best,

Mark Grimm |  Partnership Manager, Games | [REDACTED@apple.com](mailto:REDACTED@apple.com) | C: +1 (315) 254-7853

[Quoted text hidden]

**IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

**OAKLAND DIVISION**

EPIC GAMES, INC.,	)	Case No. 4:20-CV-05640-YGR
	)	
Plaintiff,	)	Date: September 28, 2020
	)	
v.	)	Courtroom: 5, 17th Floor
	)	
APPLE INC.,	)	Judge: Hon. Yvonne Gonzalez
	)	Rogers
Defendant.	)	
	)	

**Second Declaration of Dr. David S. Evans**

**September 18, 2020**

## Table of Contents

<b>I.</b>	<b>Introduction.....</b>	<b>1</b>
A.	<i>Summary of Responses to Professor Schmalensee .....</i>	<i>1</i>
B.	<i>Summary of Responses to Professor Hitt .....</i>	<i>2</i>
<b>II.</b>	<b>Professor Schmalensee’s Two-Sided Transaction Platform Analysis .....</b>	<b>4</b>
A.	<i>Professor Schmalensee’s Conclusion that the App Store Is a Two-Sided Transaction Platform Conflates the iOS Platform with the App Store and Assumes that the App Store Can Tie Distribution with Direct Transactions Between Apps Users and Developers. ....</i>	<i>8</i>
B.	<i>Calling the IAP App Administration Does Not Mean There Is No Tie.....</i>	<i>11</i>
C.	<i>Calling a Product an Input into a Transaction, or a Component, Does Not Mean There Is No Separate Material Demand for that Product and Does Not End the Antitrust Analysis .....</i>	<i>13</i>
D.	<i>Professor Schmalensee Does Not Dispute Evidence That There Is Material Demand by Developers and Consumers To Use Payment Processing Methods Other Than Those Provided by the Platform .....</i>	<i>14</i>
E.	<i>Saying That Requiring Developers To Use IAP for In-App Purchases Supports Apple’s Investments Is No Different Than Saying that a Tie Generates Revenue and Therefore Supports Investment.....</i>	<i>18</i>
F.	<i>The Analysis of Economic Efficiencies from Apple’s Practices Conflates the App Store and the iOS Platform.....</i>	<i>18</i>
<b>III.</b>	<b>Professor Hitt’s Analysis of Market Definition and Market Power Is Fatally Flawed .....</b>	<b>19</b>
A.	<i>Professor Hitt Erroneously Focuses on Substitution Possibilities for Only a Single Customer, for a Single Product, Rather Than on a Marketwide Basis .....</i>	<i>20</i>
B.	<i>Professor Hitt’s Analysis Contains Other Significant Flaws .....</i>	<i>23</i>
1.	<i>Use of Different Products in Different Circumstances Does Not Demonstrate That They Are Substitutes .....</i>	<i>23</i>
2.	<i>Professor Hitt Commits the Cellophane Fallacy .....</i>	<i>24</i>
3.	<i>Professor Hitt’s Focus on the Existence of Fortnite Users on Non-iOS Platforms Is Misplaced .....</i>	<i>25</i>
4.	<i>Professor Hitt’s Claims About the Lack of Switching from iOS to Android Are Flawed.....</i>	<i>26</i>
5.	<i>Professor Hitt’s Share Estimates Are Wrong.....</i>	<i>27</i>
6.	<i>The Fact that Some Consumers Used IAP When Offered Epic “Direct Pay” Has No Relevance.....</i>	<i>28</i>
7.	<i>Professor Hitt’s Claim that Apple’s Commission Is Not Supracompetitive Is Not Reliable .....</i>	<i>28</i>

## **I. Introduction**

1. My name is David S. Evans and I previously submitted a declaration stating my preliminary findings regarding relevant antitrust markets and market power.<sup>1</sup> This declaration responds to certain key aspects of declarations, submitted on behalf of Apple, by Professors Richard Schmalensee<sup>2</sup> and Lorin Hitt.<sup>3</sup> Given the constrained time I had to review their declarations, my declaration is not intended to provide a complete response to these declarations, and the fact that I do not address particular economic theories or empirical evidence asserted by Professor Schmalensee or Professor Hitt does not mean that I agree with them.<sup>4</sup> The following is a brief summary of my findings.

### **A. Summary of Responses to Professor Schmalensee**

2. Professor Schmalensee essentially assumes his conclusion that the mandated use of Apple's IAP check-out method for in-app payments is not a tie. He does so by asserting that the transactions that flow through Apple's check-out method are provided by a two-sided transaction platform. In the absence of the tie, however, those transactions could have taken place between the developer and its customer, just like many other transactions between app developers and users that are not subject to the tie. He has therefore relabeled transactions caused by the tie as two-sided transactions, which does nothing to disprove the tie. Likewise, labelling Apple's IAP payment processing method an "input" or a "component" in a two-sided transaction does not eliminate the need to analyze whether payment processing is a separate product.

---

<sup>1</sup> Declaration of Dr. David S. Evans, *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 62 (September 4, 2020) ("Evans Declaration").

<sup>2</sup> Expert Declaration of Richard Schmalensee, Ph.D., *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 78 (September 15, 2020) ("Schmalensee Declaration").

<sup>3</sup> Declaration of Lorin M. Hitt, Ph.D., *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 77 (September 15, 2020) ("Hitt Declaration").

<sup>4</sup> The opinions expressed in this declaration are based on information available to me at this time. My work in this matter is ongoing and I reserve the right to revise or supplement my opinion if any additional information makes that appropriate, or to correct any inadvertent errors.

3. Professor Schmalensee assumes that the App Store practices are analogous to American Express's practices, which are nothing like the practices at issue in this case.<sup>5</sup> In the case of the App Store, Apple imposes a perpetual obligation on the developer, whose app has already been distributed to a consumer for use on an iOS device, to use Apple's IAP payment processing solution to process all direct transactions between the developer and the consumer. By contrast, American Express does not require that the store use its payment network for all future direct transactions between the store and a customer who paid for a purchase using her American Express card. Nor does American Express require that the store use a separate product, such as a payment terminal, for which there is material separate demand; stores use third-party payment terminals that accept many different payment methods. Comparing the App Store to American Express glosses over and obscures the key issue for analyzing Apple's IAP requirements: that the relevant transactions are between the developer and the consumer independent of the store.

4. While much of Professor Schmalensee's declaration refers to the App Store, his analysis frequently conflates what are (absent a tie) three separate products: the iOS software platform, the App Store, and the mandatory use of IAP after an app has been distributed. This results in error because, for example, he credits the App Store and IAP with efficiencies that result from the iOS software platform and assumes that IAP-related transactions take place on the App Store, when in fact they occur (or could occur, but for the tie) directly between app user and app developer using the iOS software platform.

## **B. Summary of Responses to Professor Hitt**

5. To begin with, Professor Hitt has not attempted to refute the evidence in my opening declaration concerning the differences between smartphones and other devices, which led me to conclude that smartphone software platforms comprise a relevant antitrust market. He has also not attempted, aside from the minor exception discussed below, to refute the evidence I put forward on switching costs from iOS to Android, which led me to conclude that Apple has substantial monopoly power in the relevant market for smartphone software platforms. Those conclusions were the foundation for my subsequent finding concerning Apple's monopoly power over iOS app distribution.

---

<sup>5</sup> Schmalensee Declaration at ¶¶ 17-22, 32, 39, 53, 64.



6. Among the key flaws in Professor Hitt’s analysis are the following:

7. Professor Hitt concludes that there is a relevant antitrust market, covering all digital apps provided by numerous developers, that includes personal computers, handheld gaming devices, gaming consoles, all non-iOS handheld devices (Android smartphones and tablets and Microsoft Surface tablets), and streaming game platforms, and may include other web gaming platforms. That finding, however, is based only on analyzing gaming apps (a subset of Apple’s claimed market), for one customer (Epic), and for one product (Fortnite). His analysis is not capable of establishing the boundaries of his claimed relevant antitrust market, because he hasn’t investigated that market, and his analysis is not consistent with how industrial organization economists, or competition authorities, determine the boundaries of relevant antitrust markets.

8. Professor Hitt does not deploy any standard methodologies of market definition analysis to assess whether it would be profitable for a hypothetical monopolist to raise prices on of any set of products smaller than the expansive group he has put forward. He has just claimed that these are “good substitutes”—for Epic, for Fortnite—without any further consideration of whether a hypothetical monopolist of a smaller group of substitutes, including the ones I’ve proposed, would be able to impose a small but significant non-transitory price (SSNIP) increase on the customers in the putative market. His main response to my analysis of switching costs is that some of them may reflect value Apple provides to consumers. Of course, one of the reasons companies have market power is there are not good substitutes for their products.

9. Professor Hitt wrongly concludes that, because some consumers can use different platforms to play games, those platforms could constrain Apple’s exercise of market power. That is equivalent to concluding that, because a consumer uses several different modes of transportation, those choices necessarily constrain a hypothetical monopolist of one of those modes of transportation. It is like saying that, because people in San Francisco sometimes walk and sometimes take an Uber, it wouldn’t be possible to have a hypothetical monopolist of ride-sharing companies.

## II. Professor Schmalensee's Two-Sided Transaction Platform Analysis

10. To explain the problems with the analysis put forward by Professor Schmalensee, consider the following hypothetical conduct by Microsoft involving Windows. I will keep coming back to this hypothetical throughout this section of my declaration to highlight flaws in his reasoning.

11. Windows is a software platform for personal computers. Like other software platforms, it charges developers little. Instead, Microsoft makes money by licensing Windows to OEMs who install it on devices for consumers. Today, Windows is installed on about 80 percent of personal computers worldwide.<sup>6</sup> Developers have created more than 35 million apps for Windows, such as Salesforce and TurboTax.<sup>7</sup>

12. In the actual world that exists today, a developer distributes an application to a Windows user and can rely on a variety of channels to do so. There may be a direct, ongoing customer relationship between the user, who acquired the application and a license to use it on her Windows computer, and the application developer. In some cases, the developer may offer products and services in the application that the consumer can purchase. Those transactions take place using an application that runs on the Windows software platform. For example, when a consumer buys Intuit's TurboTax Windows application from Amazon and uses TurboTax to complete her tax return, TurboTax makes an offer in the TurboTax application to e-file her state return for her for a fee. If she takes that offer, the payment of the e-filing fee takes place directly between the consumer and TurboTax, using the check-out process offered by TurboTax (Intuit), not that operated by Amazon, or by Microsoft.<sup>8</sup>

13. Now, consider Microsoft engaging in two sequential steps.

---

<sup>6</sup> Statcounter and NetMarketShare report estimates of the market share of personal computer operating systems based on visits to websites tracked by the respective firms. The estimated Windows average share for the twelve months ending August 2020 was 78 percent based on Statcounter and 88 percent based on NetMarketShare. See Statcounter, "Desktop Operating System Market Share Worldwide," <https://gs.statcounter.com/os-market-share/desktop/worldwide/>; NetMarketShare, "Desktop/laptop Operating System Market Share," <https://netmarketshare.com/operating-system-market-share.aspx>.

<sup>7</sup> Mike Fortin, "Windows 10 Quality approach for a complex ecosystem," Microsoft, November 13, 2018, <https://blogs.windows.com/windowsexperience/2018/11/13/windows-10-quality-approach-for-a-complex-ecosystem>.

<sup>8</sup> The facts in this discussion were confirmed by purchases made by staff working under my direction.

14. Step 1: Creation of Application Distribution Monopoly. Under my hypothetical, Microsoft adopts a policy that requires all application developers who want access to the APIs for the Windows platform to distribute their applications through the Windows Store, and prohibits developers from distributing applications to users in any other way. At first, the Windows Store operates like any other store. Developers, who already have permission to access the Windows APIs, put their applications on the store “shelves”, and users can purchase them. As before, there is still a direct customer relationship between the developer and the application user. Any subsequent transactions involving that application continue to take place over the Windows software platform. The Windows Store is not involved in these subsequent transactions and only acted to initially distribute the applications.

15. Step 2: Mandated Use of Store Check-Out for In-Application Transactions. Now, under my hypothetical, Microsoft adopts another policy. Microsoft requires that developers pay the Windows Store a commission not only on all initial purchases of applications from the store, but also on all subsequent direct purchases made by the application customer from the application developer within that application, in perpetuity, such as the TurboTax purchase mentioned above.

16. To enforce this policy, Microsoft requires that developers always use a check-out method it provides. That results in the Windows Store collecting the money directly from the customer and then paying the developer this amount less the store’s commission. These transactions can be said to take place on the Windows Store only in the sense that Microsoft has required that developers use the store’s check-out method. Before the policy was put in place, these transactions took place directly between the user and developer, both of whom used the Windows software platform but not the Windows Store.

17. This hypothetical, which essentially maps the steps Microsoft would have to take to replicate the iOS ecosystem in important aspects relevant here, illustrates three fundamental flaws in Professor Schmalensee’s analysis.<sup>9</sup>

---

<sup>9</sup> While there may be other differences between the Windows hypothetical and the Apple practices at issue in this case, any such differences would not affect my basic conclusion that Professor Schmalensee’s methodology is flawed in the ways described below.

18. *First*, when applied to the Microsoft hypothetical, his analysis assumes away the tie by claiming that direct transactions that took place on the Windows platform between the user of an application and the developer of the application are Windows Store transactions simply because Microsoft has required the use of its check-out method to process them. He does so by recasting the requirement that developers use the check-out process—for transactions that, but for the tie, would have been direct transactions between the application user and the application developer—as a set of store transactions. These can only be viewed as store transactions, however, because they are the subject of the tie at issue; otherwise, they wouldn't have anything to do with the store.

19. When applied to the Microsoft hypothetical, Professor Schmalensee's methodology essentially applies the label "two-sided transaction platform" to the transactions that result from Microsoft's requirement that developers who want to use its monopoly store to distribute their applications (the tying product) also use its check-out method (the tied product) for subsequent direct transactions between themselves and customers who use their applications. He would then prematurely end the analysis of the conduct at issue by claiming that the check-out method is just the way to charge for these transactions.

20. In fact, as I discuss below in Section II.A, his analysis in this matter improperly ends the inquiry into Apple's requirement to use its IAP payment method for direct transactions between developers and users of iOS apps by labelling the result of this tie a two-sided transaction platform.

21. *Second*, the Windows example shows why, contrary to Professor Schmalensee's claims, the App Store isn't analogous to American Express when it comes to the tying conduct at issue in this case. Going back to my hypothetical, in Step 1 Microsoft establishes a store that distributes applications but doesn't impose any further requirements. The developer puts an application on the shelf and the consumer procures the application. The developer and user don't have any further interaction with the store.

22. With respect to American Express, the Amex cardholder walks into the Amex-accepting retailer and pays the retailer with her card, and American Express charges the merchant a fee

for that transaction in the course of providing payment processing.<sup>10</sup> At that point, American Express is done. Moreover, American Express is not requiring that the retailer use any other separate product, such as an American Express-supplied payment card terminal, as a condition of processing that transaction or any future ones. The retailer gets a payment card terminal, which can process many types of payment cards, including American Express, from a third party.

23. In Step 2 of my hypothetical, Microsoft imposes a perpetual obligation on the developer to use the Window Store's check-out method for all direct transactions that take place between the user and developer involving that application. That is not like American Express, which imposes no requirement that its payment card network be used for subsequent transactions between the Amex merchant and Amex cardholder. And American Express doesn't require that the retailer use a product for which there is material separate demand, such as an independently-supplied payment terminal, for any transaction.

24. For the tying conduct at issue in this matter, it is the second step in the hypothetical that matters. And at that stage, the App Store is not at all like American Express.

25. *Third*, the Windows example shows the mistake in asserting, as Professor Schmalensee does for Apple, that the conduct at issue is necessary for a "monetization strategy." In my hypothetical, Microsoft would certainly have a monetization strategy in mind for monopolizing application distribution and requiring developers to use its check-out method for direct transactions they have with application users. There is no *a priori* basis for economists to assume that this monetization strategy, resulting from the successive application of Step 1 and Step 2, is procompetitive or necessary to finance Microsoft's investments in the platform.<sup>11</sup> Indeed, if Microsoft were to engage in the hypothetical conduct described above, it is likely that competition authorities, and industrial organization economists, would find it quite alarming.

---

<sup>10</sup> *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2281 (2018).

<sup>11</sup> Professor Schmalensee might argue that Apple is different because it had the policy in place at the beginning. But there is also no presumption that conduct that was not anticompetitive when it was adopted by a firm that lacks substantial market power couldn't become anticompetitive when that firm acquires market power.

26. With this Microsoft Windows hypothetical in mind, I will turn to a discussion of some key areas where I disagree with Professor Schmalensee's analysis.

**A. Professor Schmalensee's Conclusion that the App Store Is a Two-Sided Transaction Platform Conflates the iOS Platform with the App Store and Assumes that the App Store Can Tie Distribution with Direct Transactions Between Apps Users and Developers.**

27. Professor Schmalensee claims that the App Store is a two-sided transaction platform. By that, he means that the App Store is a two-sided transaction platform *for direct transactions between iOS users, who have an app that they can use under the license on their iPhone, and iOS developers, who have developed an app that can work under that license*. His analysis is presented in paragraphs 39-45. I comment on each major step of his analysis.

28. In paragraph 39, he points out that I have not offered an opinion on whether the App Store is a two-sided transaction platform.<sup>12</sup> I'm not going to offer one here as I believe the issue is more complex than Professor Schmalensee suggests. To begin with, stores may operate under a retail model, which is considered single-sided, and a marketplace model, which is considered two-sided.<sup>13</sup> Amazon, for example, operates a hybrid: Amazon Marketplace, which connects buyers and sellers, is a two-sided marketplace; but Amazon also operates a large retail store, which isn't. Unlike payment card platforms, which mainly compete with each other, it is common for two-sided marketplaces to compete with retail stores. Retail stores do not necessarily have to have substantial indirect network effects. They can just specialize in carrying certain products. And as I noted in my earlier declaration, and as explained further below, at least at this stage, I don't think the issues in this case turn on this definitional issue.

29. But here's the critical flaw in Professor Schmalensee's analysis: the transaction platform label is being applied to a set of transactions that are taking place *directly* between users and developers using the iOS platform. Those transactions have to take place over a two-sided transaction platform involving the App Store only because Apple has imposed a

---

<sup>12</sup> Schmalensee Declaration at ¶ 39.

<sup>13</sup> Evans, David S. and Richard Schmalensee (2016), *Matchmakers: The New Economics of Multisided Platforms*, Harvard Business School Press, at pp. 104-109; Hagiu, Andrei (2007), "Merchant or Two-Sided Platform?" *Review of Network Economics* 6(2), pp. 115-133; Hagiu, Andrei and Jullian Wright (2015), "Marketplace or Reseller?" *Management Science* 61(1), pp. 184-203.

requirement—the tie at issue in this case—that they do so. That is unlike two-sided transactions platforms that arise because both sides, such as merchants and cardholders, choose to use that platform. This flaw is apparent in Professor Schmalensee’s analysis in the remaining paragraphs that he provides as support for his conclusion.

30. In paragraph 40, Professor Schmalensee says that the “App Store exhibits all the hallmarks of a two-sided platform”<sup>14</sup> and in paragraph 41, he says there are “clear indirect network effects: consumers want access to good apps, developers want access to many potential customers.”<sup>15</sup> But in both paragraphs, much of the evidence cited in support is based on the *iOS platform* providing software that enables developers to provide, and consumers to use, apps.<sup>16</sup> This evidence offered is not different than what one could provide for the Windows software platform, which in fact, and contrary to my hypothetical above, did not operate an app store as a central part of its business model.

31. In paragraph 43, Professor Schmalensee concludes “[a]s is common for two-sided platforms, the App Store earns all of its revenues from one side: developers.”<sup>17</sup> Apple’s monetization strategy, which results from its making the App Store the exclusive channel for app distribution and its requirement to use IAP for in-app transactions, is hardly a developer-pays model. First, developers that account for the preponderance of transactions within apps—developers selling physical goods and services and developers monetizing via advertising—

---

<sup>14</sup> Schmalensee Declaration at ¶ 40.

<sup>15</sup> Schmalensee Declaration at ¶ 41.

<sup>16</sup> The only factual support cited in these two paragraphs comes from Apple’s SEC Form 10-K for the Fiscal Year Ended September 29, 2018. Passages analogous to the ones quoted by Professor Schmalensee do not appear in Apple’s SEC Form 10-K for Fiscal Year Ended September 28, 2019 (its most recent 10-K). *Compare* Apple, SEC Form 10-K for the Fiscal Year Ended September 29, 2018, Item 1, *with* Apple, SEC Form 10-K for the Fiscal Year Ended September 28, 2019, Item 1. While the quoted passages do mention app distribution, the focus is on support for software development. These passages discuss the ways Apple supports the developer community, including access to beta software, advanced app capabilities, and testing software, as well as code-level technical support. The quotations also tout Xcode, Apple’s integrated development environment, which “includes project management tools; analysis tools to collect, display and compare app performance data; simulation tools to locally run, test and debug apps; and tools to simplify the design and development of user interfaces.” Apple, SEC Form 10-K for the Fiscal Year Ended September 29, 2018, pp. 1-3. All of these activities refer to Apple’s efforts to promote its iOS software platform, not its iOS App Store.

<sup>17</sup> Schmalensee Declaration at ¶ 43.



pay only nominal fees.<sup>18</sup> Second, IAP applies to direct transactions between a developer and a consumer. Generally, economists would expect that the developer would pass on some portion of the commission to the consumer in the form of higher prices.<sup>19</sup> Overall, Apple’s monetization strategy for the iOS platform and App Store is heavily skewed towards the consumer paying, especially given that most of Apple’s revenues come from sales of devices.<sup>20</sup>

32. In paragraph 44, Professor Schmalensee asserts that it is essential to decide whether the App Store is a two-sided platform.<sup>21</sup> He says the use of IAP for direct transactions between the app owner and developer is simply a feature of the transaction platform. But that substitutes a label—two-sided transaction platform—for a substantive analysis of whether the requirement to use the IAP check-out, which imposes the fees for these transactions, is a tie. It is not different than, in my Windows hypothetical, taking a set of transactions that occurred directly between application users and developers using the Windows platform before the Step 2 tie, and saying those transactions take place on a two-sided transaction platform after the Step 2 tie is in place.

33. The economic reasoning related to the Supreme Court’s decision in *American Express* summarized in paragraph 45 doesn’t support his conclusion.<sup>22</sup> American Express is a two-sided transaction platform that charges a merchant a fee for a transaction that takes place over the American Express payment network as a result of a cardholder paying the merchant with her American Express card.<sup>23</sup> IAP is a mechanism imposed on developers and that charges developers a fee for a transaction that takes place directly between them, using the iOS

---

<sup>18</sup> According to a study commissioned by Apple, ad-supported app developers earned \$45 billion for iOS apps in 2019. Physical apps accounted for \$413 billion in transactions. These apps didn’t pay Apple anything. See Borck, Jonathan, Juliette Caminade, and Markus von Wartburg, “How Large Is the Apple App Store Ecosystem?” Analysis Group, June 15, 2020, at p. 2-3, <https://www.apple.com/newsroom/pdfs/app-store-study-2019.pdf>

<sup>19</sup> Further analysis of the extent of this standard pass-through issue would be needed to determine the extent to which the consumer and developer bear the burden of the commission.

<sup>20</sup> In 2019, Apple had \$146.4 billion in iPhone sales and \$20.5 billion in iPad sales, for a total of \$166.9 billion. Apple’s App Store revenues in 2019 were approximately \$16.6 billion. Thus, approximately 91 percent ( $166.9/(166.9+16.6)$ ) of Apple’s iOS related revenues come from selling iPhones and iPads. See Evans Declaration at ¶ 19.

<sup>21</sup> Schmalensee Declaration at ¶ 44.

<sup>22</sup> Schmalensee Declaration at ¶ 45.

<sup>23</sup> *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2287 (2018).



software platform, but outside the App Store. That transaction can be said to take place over the App Store only as a result of the tie.

34. As I showed in my first declaration, and in Section II.D below, when a direct in-app transaction between an iOS app developer and an iOS app user that is not subject to Apple's requirement to use its IAP payment processing method, the transaction does not take place over Professor Schmalensee's "two-sided transaction platform." It takes place directly between the developer and user relying on whatever payment processing method the developer chooses.

### **B. Calling the IAP App Administration Does Not Mean There Is No Tie**

35. Professor Schmalensee claims that the "IAP system collects a commission on paid apps and in-app sales that is the core of Apple's strategy for capturing some of the value that the App Store creates."<sup>24</sup> That assertion doesn't address the tying allegation; it simply re-labels it conveniently. Going back to my Windows hypothetical, Microsoft could claim that requiring application developers to use the Windows Store check-out method is core to its strategy for monetizing the Windows Store. Moreover, a defendant can always claim, sometimes correctly, that a tie is core to its business model. That assertion does not transform a tie into something else.

36. It is also not correct that the "IAP system no more provides transaction processing than the payment card terminal at the grocery store."<sup>25</sup> The IAP system, which uses a payment processor, charges the consumer, processes the payment, and deposits the net receipts in the developer's bank account.<sup>26</sup> The developer can provide all of these services itself by having the consumer provide payment credentials and using its own payment processing solutions.<sup>27</sup> I provide further evidence on this point in Section II.D below.

---

<sup>24</sup> Schmalensee Declaration at ¶ 50.

<sup>25</sup> Schmalensee Declaration at ¶ 49.

<sup>26</sup> In paragraph 29, Professor Schmalensee claims that "IAP is not a payment settlement platform" because "Apple outsources payment settlement to third-party providers." This distinction is irrelevant; regardless of whether payment processing is integrated or outsourced, IAP is the means by which developers that offer in-app purchases of in-app content are required to process those transactions.

<sup>27</sup> At various points, Professor Schmalensee refers to Mastercard and Visa as payment processors. Their main businesses that are usually referred to by these brand names aren't. Visa and Mastercard are payment card networks that have affiliated issuers from whom consumers get card credentials. Payment processors are

37. I disagree with Professor Schmalensee’s claim that “Plaintiff’s tying analysis is vacuous” because “Apple does not require that developers offer any in-app purchases of digital content.”<sup>28</sup> A purchaser of a tying and tied product generally doesn’t have to buy the two products at all. The problem with tying stems from situations in which the seller of the tying product has the ability to force the purchaser to take the tied product because their customers want the tying product and don’t have an alternative. The fact that the app developer might be able to develop a different app employing a different business model does not change the fact that for the universe of apps that do sell digital upgrades and other content, Apple employs a tie.<sup>29</sup>

38. I understand that Professor Schmalensee, and Apple, contend that developers are required to pay the 30 percent commission to Apple regardless of whether it is collected through IAP.<sup>30</sup> The requirement to use IAP for in-app purchases could still be a tie even under that assumption. Shopping malls, for example, typically require that stores pay a percent of their revenue in addition to rent. Presumably, the shopping mall and the stores have developed a process to collect and audit these amounts. Malls do not install their own cash registers, connected to their payment processors, in the stores they rent to. Of course, if they did, that would be a tie, since cash registers and payment processing are generally procured by stores separately.<sup>31</sup>

---

companies like Braintree that take those card credentials and collect money from those issuers, which then bill the consumers.

<sup>28</sup> Schmalensee Declaration at ¶ 46.

<sup>29</sup> Professor Schmalensee himself observes that there are material differences in the suitability of different business models for an app developer. He finds that Epic’s use of what he calls the “Freemium” model, with no upfront app fee and with the option of in-app purchases, has allowed Fortnite to be more successful. He states that “[b]y drawing in both more price-sensitive and less price-sensitive consumers, it allows a platform like Fortnite to maximize its user base, which is important”; “this model still allows Epic to cash in on its most enthusiastic and hence potentially less price-sensitive users”; and “[t]he Freemium Model hence provides a convenient method for Epic to earn more revenue from more avid players, thereby likely contributing to Fortnite’s overall profitability”. See Schmalensee Declaration at ¶¶ 65, 67.

<sup>30</sup> Schmalensee Declaration at ¶ 54.

<sup>31</sup> Whether this practice would meet the legal definition of a tie would further depend on whether a mall had significant market power.

**C. Calling a Product an Input into a Transaction, or a Component, Does Not Mean There Is No Separate Material Demand for that Product and Does Not End the Antitrust Analysis**

39. In paragraph 53, Professor Schmalensee claims that “it makes no economic sense to consider inputs into transactions production that are simultaneously engaged in fixed proportions as actually or potentially separate products.”<sup>32</sup> He appears to be saying that if a product can be characterized as an input into a transaction, then it is not a separate product. I do not believe this is correct.

40. Instead, as economists would do for any tying claim, we would have to examine whether a product that is characterized as an input into a transaction is provided separately from the transaction. Suppose American Express, for example, required that stores that accepted its cards also use an Amex-supplied payment terminal and American Express charged a separate fee for each transaction that went through its terminal.<sup>33</sup> The payment card terminal is an input into the transactions American Express provides and its services are provided in fixed proportions with these transactions.

41. To analyze whether this conduct constitutes a tie, we would need to examine whether there is separate demand for payment terminals. In the actual world, retailers don’t get their payment terminals from American Express, and we know from common experience that payment terminals typically take payment cards from most major networks.

42. The same economic analysis applies to the products at issue in this case. We consider whether we observe demand for payment processing of in-app purchases that is separate from demand for app store services. As I discuss in Section II.D below, we observe separate demand for in-app payment processing on the part of developers and users. We also observe it being provided separately from app stores by third parties. This means that it is a separate product

---

<sup>32</sup> Schmalensee Declaration at ¶ 53.

<sup>33</sup> To take another example, consider cash register tape that the clerk gives the customer as a record of the transaction. Cash register tape can be characterized as an input into each transaction because it is used with each transaction and it is used in fixed proportion to the number of transactions. But, again, we still need to ask whether we observe demand for cash register tape that is separate from the demand for transaction services. If we observe that demand, then cash register tape is a separate product even if it could be characterized as an input into the transaction.

from the app store, whether or not one would characterize it as an input into app store services.<sup>34</sup>

43. Citing *American Express*, and referring to two-sided transactions between consumers and merchants, does not get around having to do the separate products analysis.<sup>35</sup> If it did, a two-sided transaction platform could tie anything in fixed proportions to a transaction and insist that it is just part of the platform. In my example above, American Express could claim the payment card terminals, and the associated fee structure, are just components of the transaction. Under Professor Schmalensee's approach, that ends the antitrust analysis. I don't believe anything in our amicus brief to the Supreme Court dictates that conclusion.

**D. Professor Schmalensee Does Not Dispute Evidence That There Is Material Demand by Developers and Consumers To Use Payment Processing Methods Other Than Those Provided by the Platform**

44. Professor Schmalensee does not dispute the evidence I put forward in my opening declaration that there is separate demand from iOS developers for payment processing methods other than those provided by the platform.<sup>36</sup> That same evidence shows that, in the absence of a tie, developers do not use the "two-sided transaction platform" described by Professor Schmalensee in the discussion above. These developers use their own check-out methods involving payment processors they choose to work with. The following summarizes and supplements that evidence.

---

<sup>34</sup> As I discussed above, in-app purchases are in fact unrelated to App Store services as they are removed both in location (they take place in the developer app, not in the app store) and time (they take place after the app has been distributed) from the App Store. So, in-app purchase processing is not an input into App Store services.

<sup>35</sup> Professor Schmalensee also makes the assertion in paragraph 45 that "Epic seeks to separate the distribution of apps and in-app content from the management of those transactions by the App Store." As explained in this declaration, the separate products inquiry does not concern the separation of the management of transactions from the transactions themselves. Rather, the inquiry is concerned with two different types of transactions: (1) the distribution of apps and (2) the sale of in-app content. (To be more precise, the inquiry is concerned with Apple's requirement that the App Store process the sale of in-app content, because the developer is already otherwise responsible for offering the content to the user in the developer's app.) Professor Schmalensee's description in paragraph 45 makes separate reference to "the distribution of apps" and "in-app content"—they are two discrete types of transactions. The relevant separate products inquiry is then whether there is separate demand for these two types of transactions. As I explain in this declaration, there is.

<sup>36</sup> Evans Declaration at Section III.B.

45. First, we know that developers, including Epic, Match Group<sup>37</sup>, Facebook<sup>38</sup>, Spotify<sup>39</sup>, and Hey<sup>40</sup>, would like to have the option of using a check-out method, and payment processing solution, that is not provided by Apple’s iOS App Store. We further know that when Epic offered iOS users of Fortnite the choice between IAP and Epic Direct Pay, customers utilized Epic Direct Pay for 73 percent of transactions.<sup>41</sup>

46. Second, Apple’s iOS App Store and the Google Play Store generally allow developers to use their own payment processing method for in-app purchases of physical goods or services that are consumed outside the app.<sup>42</sup> Those developers and their customers use those other methods. The fact that Apple has reasons for not wanting to require these apps to use its payment processing method does not show the absence of separate demand.

47. Third, Apple itself has made business decisions to allow developers to use their own payment processing for certain digital content that is consumed in the app. The developers then use check-out methods using their chosen payment processors. There is, again, material

---

<sup>37</sup> S&P Capital IQ, “Match Group, Inc. NasdaqGS:MTCH FQ2 2019 Earnings Call Transcripts,” August 7, 2019 at pp. 6, 11 (“[W]e introduced a credit card payment option on the Android app at Tinder in Q2. . . . To roll this out, we first had to build a web-based payment infrastructure to be able to accept credit card payments. . . . We’d love to offer the same kind of choice on Apple as we do with Google, but it’s not clear to us if or when that’s actually going to be able to happen.”)

<sup>38</sup> Salvador Rodriguez, “Facebook says Apple refused to waive 30% fee on new paid online events feature,” CNBC, August 14, 2020, <https://www.cnbc.com/2020/08/14/facebook-says-apple-refused-to-waive-30percent-fee-on-new-feature.html> (“We asked Apple to . . . allow us to offer Facebook Pay[.]”).

<sup>39</sup> Daniel Ek, “Consumers and Innovators Win on a Level Playing Field,” Spotify Newsroom, March 13, 2019, <https://newsroom.spotify.com/2019-03-13/consumers-and-innovators-win-on-a-level-playing-field> (“[C]onsumers should have a real choice of payment systems, and not be ‘locked in’ or forced to use systems with discriminatory tariffs such as Apple’s.”).

<sup>40</sup> Jason Fried, “Our CEO’s take on Apple’s App Store payment policies, and their impact on our relationship with our customers,” HEY, June 19, 2020, <https://hey.com/apple/iap/> (“Apple, please just give your developers the choice! Let us bill our own customers through our own systems, so we can help them with extensions, refunds, discounts, or whatever else *our own way*.”).

<sup>41</sup> From the start of the Direct Pay option being offered (August 13) to the point when the Apple IAP option was no longer available because Epic’s developer account ending in ’84 was terminated by Apple (midday August 28), about 73 percent of purchases were on Epic Direct Pay. Calculations based on data from Epic.

<sup>42</sup> Apple, “App Store Review Guidelines,” at 3.1.3(e), <https://developer.apple.com/app-store/review/guidelines/> (“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.”); Google, “Play Console Help, Policy Center, Payments,” <https://support.google.com/googleplay/android-developer/answer/9858738> (“Developers offering products within another category of app downloaded on Google Play must use Google Play In-app Billing as the method of payment, except for the following cases: Payment is solely for physical products”).

demand for payment processing not provided by the App Store as a separate product. Apple allows developers to use their own payment processing, which customers use, in the following cases:

- a. For Amazon Prime Video and other “qualifying premium video entertainment apps”, users “have the option to buy or rent movies and TV shows using the payment method tied to their existing video subscription.”<sup>43</sup>
- b. For tips given to creators of in-app content, which is commonly done in China.<sup>44</sup>
- c. For person-to-person content, such as an exercise class, when it is one-to-one (but not when it is one-to-two+).<sup>45</sup>
- d. For content consumed in the app but purchased outside of the app (e.g., developer’s website).<sup>46</sup>

---

<sup>43</sup> Nick Statt, “Apple now lets some video streaming apps bypass the App Store cut,” The Verge, April 1, 2020, <https://www.theverge.com/2020/4/1/21203630/apple-amazon-prime-video-ios-app-store-cut-exempt-program-deal>; see also Nicole Nguyen, “How App Makers Break Their Apps to Avoid Paying Apple,” The Wall Street Journal, June 28, 2020, <https://www.wsj.com/articles/how-app-makers-break-their-apps-to-avoid-paying-apple-11593349200>.

<sup>44</sup> Apple, “App Store Review Guidelines,” at 3.2.1(vii), <https://developer.apple.com/app-store/review/guidelines/> (“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.”); Josh Horwitz, “Thanks to China, Apple has updated its app store policy to allow tipping,” Quartz, September 15, 2017, <https://qz.com/1078374/thanks-to-china-and-tencent-hkg-0700-apple-has-updated-its-app-store-policy-to-allow-tipping/> (“A recent update to the company’s global App Store Guidelines shows that Apple now permits users to send monetary tips to one another—a practice which, while widespread in China, the company had previously shown ambivalence towards. The revision shows that Apple is now accommodating China’s vast tip economy, and also highlights the power that Chinese social media giant Tencent has over China’s internet culture, as well as the foreign companies that operate in the country.”). Apple’s guidelines allow such payments but note that “a gift that is connected to or associated at any point in time with receiving digital content or services must use in-app purchase.” See Apple, “App Store Review Guidelines,” at 3.2.1(vii), <https://developer.apple.com/app-store/review/guidelines/>. The use of tipping in China that Apple allows to bypass its IAP payment processing has been characterized as “monetary gifts to [users’] favorite video-streaming stars and content creators” that are intended “as a means to build engagement” between content providers and users. They appear to be payments by users, in appreciation for content from providers, that is made on a voluntary rather than mandatory basis. See Yoko Kubota and Alyssa Abkowitz “Apple and Tencent Reach Deal to Let WeChat Users Dole Out Tips” The Wall Street Journal, January 15, 2018, <https://www.wsj.com/articles/apple-and-tencent-reach-deal-to-let-wechat-users-dole-out-tips-1516018849>.

<sup>45</sup> Apple, “App Store Review Guidelines,” at 3.1.3(d), <https://developer.apple.com/app-store/review/guidelines/> (“Person-to-Person Experiences: If your app enables the purchase of realtime person-to-person experiences 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 realtime experiences must use in-app purchase.”).

<sup>46</sup> Apple, “App Store Review Guidelines,” at 3.1.3(a-b) (“Apps may allow a user to access previously purchased content or content subscriptions (specifically: magazines, newspapers, books, audio, music, and video). Reader

- e. For apps that are “sold directly by [developers] to organizations or groups for their employees or students”. For these iOS apps that are not distributed through the App Store but which still rely on access to the iOS platform, Apple does not mandate the use of its App Store’s payment method.<sup>47</sup>

In all these cases, the transactions take place directly between the developer of the iOS app and its customer, the iOS app user, using payment processing alternatives chosen by the developer and offered to the consumer. It is no different than a retailer that sells products directly to its customers and allows customers to use various payment cards at the check-out lane using a payment processor of the retailer’s own choosing.

48. Fourth, many Android app stores do not require that digital content providers use the store’s check-out method, and its payment processor, for in-app purchases, and developers use these app stores and their own check-out methods with their choice of payment processor.

- a. Google Play Store does not require use of its check-out method for non-gaming digital content that may be consumed outside of the app.<sup>48</sup>
- b. Significant Android app stores in South Korea and India, as well as others that operate in the US and other countries, give developers the choice of using their own check-out methods.<sup>49</sup>

---

apps may offer account creation for free tiers, and account management functionality for existing customers. . . . 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.”).

<sup>47</sup> Apple, “App Store Review Guidelines” at 3.1.3(c), <https://developer.apple.com/app-store/review/guidelines/>.

<sup>48</sup> Google, “Play Console Help, Policy Center, Payments,” <https://support.google.com/googleplay/android-developer/answer/9858738>.

<sup>49</sup> ONE Store Developer, “Service Fee,” <https://dev.onestore.co.kr/devpoc/reference/view/ServiceFee> (“In case of use 3rd party payment without ONE store In-App SDK, the service fee is 5%”). GetJar, “GetJar – How It Works,” <https://www.getjar.com/how-it-works> (“GetJar is the first and one of the biggest open app stores and open mobile app markets in the world providing a free of charge distribution for all users. Same time [*sic*] it allows for developers to upload their apps and place them in to [*sic*] our app catalog free of charge. GetJar does not control any in-app monetization, therefore each developer is in full control of their assets.”); itch.io, “Creator FAQ,” <https://itch.io/docs/creators/faq> (“itch.io costs nothing to use. You are free to create pages and upload your content without ever having to pay anything. Advertisements will never be placed on any of your pages. You get to decide how much you want to support itch.io by choosing what percentage of your sales should go towards our operational costs and continued development of the platform. . . . itch.io supports two payout models depending on your needs: Direct to you, where each purchase is a transaction to your PayPal or Stripe account, and Collected by itch.io, paid later. You can pick which mode you want to use from the seller settings page on your account.”); itch.io, “Introducing Open Revenue Sharing,” March 4, 2015, <https://itch.io/updates/introducing-open-revenue-sharing> (“As the seller you decide what percentage itch.io gets from each transaction. From 0 to 100%, set the slider to what you think is fair.”); itch.io, “Accepting Payments and Getting Paid,”



**E. Saying That Requiring Developers To Use IAP for In-App Purchases Supports Apple’s Investments Is No Different Than Saying that a Tie Generates Revenue and Therefore Supports Investment**

49. Professor Schmalensee says,

It is important to note, however, that IAP is not a payment settlement platform. In fact, Apple outsources payment settlement to third-party providers. Thus, the commission that Apple charges developers on in-app purchases is not a fee for payment processing, but rather a fee to support the services offered by the App Store and Apple’s investment in the mobile platform.<sup>50</sup>

That may be the case for Apple, but for the developer, IAP provides the same payment processing services the developer would have obtained by using a payment processor like Braintree to process transactions based on card credentials the consumer enters into the app. It is the processing method that charges the consumer’s card and deposits the funds to the merchant. Apple could claim that this helps support its investments in the mobile platform. But simply calling it a source of revenue does not, by itself, tell us whether the IAP checkout method is a separate product or whether the tying arrangement is economically efficient.

**F. The Analysis of Economic Efficiencies from Apple’s Practices Conflates the App Store and the iOS Platform**

50. Once Apple decided to operate a software platform for users and developers, it had to provide a way for users to get apps on their phones. If it didn’t, it would not have had a software platform and could not benefit from indirect network effects any more than Windows could benefit from indirect network effects if application users couldn’t install applications.

---

<https://itch.io/docs/creators/payments> (itch.io requires developers to use either Stripe or PayPal, but allows developers to use their own accounts and connections to the processors); SlideMe, “Developer Distribution Agreement (DDA)” <http://slideme.org/developers/dda> (“SlideME does not restrict developers from including third party In-App-Payments SDK’s within their freemium applications, providing such SDK’s will work for non-GMS devices too.”). In-app purchases through credit card and PayPal is available on third-party Android app store Aptoide. See Sonia Sarha, “You can now pay using Local Payment Methods! (updated),” Aptoide Official Blog, May 14, 2020, <https://blog.aptoide.com/payment-methods/>. Staff under my direction confirmed that the credit card statement of an in-app credit card transaction through Aptoide listed the developer rather than Aptoide as the merchant associated with the transaction. See also Indus, “App Bazaar Developer Distribution Agreement,” <http://www.indusos.com/app-bazaar-developer-distribution-agreement/> (“In order to charge a fee for your Products, you must have a valid payment account under a separate agreement with a payment processor.”).

<sup>50</sup> Schmalensee Declaration at ¶ 29.



51. Many of the benefits of the iOS platform that Professor Schmalensee (and Professor Hitt) point to result from Apple’s decision to provide a smartphone software platform for apps and the resulting indirect network effects. Professors Schmalensee and Hitt do not show that these benefits depend on the App Store being the exclusive method of distribution or on the requirement that IAP be used for the in-app purchases. They therefore have not done any serious analysis that would support their expansive conclusions that “App Store business strategy has led to large procompetitive benefits”<sup>51</sup> or that the “[s]ervices offered by the App Store . . . have been essential to the iPhone ecosystem.”<sup>52</sup>

52. Professor Schmalensee and Professor Hitt also claim that the App Store guarantees users security, privacy, and a quality consumer experience. The App Store could provide those same benefits absent Apple’s requirement that developers use the App Store exclusively; if in fact the App Store provides all the benefits Apple claims, Apple should not be afraid to compete on the merits. Users and developers could use app stores that provide their preferred combination of features.

### **III. Professor Hitt’s Analysis of Market Definition and Market Power Is Fatally Flawed**

53. Professor Hitt has not followed standard accepted methods used by economists or competition authorities, in my experience, for assessing the contours of relevant antitrust markets. He proceeds as follows:

- i. First, he focuses on gaming and ignores other digital apps even though these apps are distributed in the same channels (such as to PC and Android users) that are included in the market proposed by Apple. He says, “Defining relevant antitrust markets in the present case therefore requires that one evaluates the options that Epic and other developers (the customers) have in distributing and monetizing Fortnite and other videogames.”<sup>53</sup>
- ii. Second, in examining substitution possibilities, he considers only one customer, Epic, and only one game from Epic, Fortnite.<sup>54</sup>

---

<sup>51</sup> Hitt Declaration at ¶ 16.

<sup>52</sup> Schmalensee Declaration at ¶ 30.

<sup>53</sup> Hitt Declaration at ¶ 18.

<sup>54</sup> See fn. 61 below.

- iii. Third, he claims that for Epic’s Fortnite game, the following distribution channels are good substitutes for Apple’s iOS App Store: personal computers, handheld gaming devices, gaming consoles, all non-iOS handheld devices (Android smartphones and tablets and Microsoft Surface tablets), and streaming game platforms, and may include other web gaming platforms.<sup>55</sup>
- iv. Fourth, based on his proposed, purportedly good substitutes that he says are available to Epic, he concludes that the relevant antitrust market, which extends to all digital apps provided by numerous developers, includes all the channels listed in (iii).<sup>56</sup> The gaming channels he cites are obviously not relevant to non-gaming apps that are distributed through channels in his proposed relevant market.

At no point in his declaration does he consider the hypothetical monopolist test or any other standard approach for defining a relevant antitrust market.

**A. Professor Hitt Erroneously Focuses on Substitution Possibilities for Only a Single Customer, for a Single Product, Rather Than on a Marketwide Basis**

54. The relevant market that I described in my opening declaration was for the distribution of iOS apps,<sup>57</sup> which is not restricted to game apps. Neither Professor Hitt nor Apple’s counsel have proposed a relevant market for app distribution that is restricted to game apps, because other non-gaming apps are distributed via the same channels that are included in the market proposed by Apple.<sup>58</sup> Apple has stated that “Apple’s commission structures, administered through the IAP, apply equally to all developers who offer in-app purchases on the App Store.”<sup>59</sup> The conduct at issue in this matter therefore involves all those iOS app developers,

---

<sup>55</sup> Hitt Declaration at ¶ 49.

<sup>56</sup> Hitt Declaration at ¶ 49.

<sup>57</sup> Evans Declaration at ¶¶ 52-57.

<sup>58</sup> Both Apple’s counsel and Professor Hitt argue that the market should include at least the other platforms on which Epic distributes Fortnite. *See* Defendant Apple Inc.’s Opposition to Epic Games, Inc.’s Motion for a Preliminary Injunction, *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 73 at p. 17 (September 15, 2020); Hitt Declaration at ¶ 14. Neither proposes a relevant market that is restricted to the distribution of games.

<sup>59</sup> Declaration of Philip W. Schiller in Support of Defendant Apple Inc.’s Opposition to Plaintiff’s Motion for a Preliminary Injunction, *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 74, at ¶ 62 (September 15, 2020); *see also* Declaration of Philip W. Schiller in Support of Defendant Apple Inc.’s Opposition to Epic Games, Inc.’s Motion for a Temporary Restraining Order and Order to Show Cause Why a Preliminary Injunction Should Not Issue, Exhibit E, *Epic Games, Inc. vs Apple Inc.*, Case No. 3:20-cv-05640-YGR, ECF No. 37-5, at 5 (August 21, 2020) (“Apple treats all developers according to the same terms . . .”). Relevant markets can consist of sales to targeted customers when those customers are treated differently from other customers. *See*

and not just game developers. As noted above, Professor Hitt has excluded all non-game developers from consideration so that his inquiry is incapable of addressing any relevant market that has been put forward in connection with this motion, including the one that Professor Hitt ultimately posits.

55. Even as to game developers, however, Professor Hitt has focused solely on Epic's Fortnite game.<sup>60</sup> Other than some largely conclusory assertions in the introduction to Section 3 and the first paragraph of Section 3.1, the empirical evidence he provides concerns substitution options for Fortnite.<sup>61</sup> Games other than Fortnite may not be suited for play on gaming consoles or PCs. Casual games designed for quick sessions on-the-go may not be attractive as console or PC games.<sup>62</sup> And some games, like Pokémon Go, are designed to be played when interacting

---

Horizontal Merger Guidelines, US Department of Justice and Federal Trade Commission, Section 7, August 19, 2010, at 3, <https://www.justice.gov/atr/horizontal-merger-guidelines-08192010>. This is not applicable here because Apple's IAP policies apply generally to all app developers that are subject to them.

<sup>60</sup> For convenience, I refer generally to game "developers" below. My understanding is that in the gaming industry, there can be distinctions between game "developers" that create games and game "publishers" that market and sell the games on different platforms. Some gaming companies perform all of these roles itself. When the "developer" and "publisher" roles are performed by separate companies, it is the publisher that would list the app in the iOS App Store. In those circumstances, the term "developer" as I use it in this declaration and in my opening declaration also includes the publisher.

<sup>61</sup> Paragraph 19 makes the claim that "It is clear that videogame developers do have [alternative distribution and monetization] options" without providing any evidence. Hitt Declaration at ¶ 19. Paragraph 20 makes the claim that "[Dr. Evans] largely ignores developers' ability to distribute and monetize their videogames on multiple platforms commonly used to play videogames, such as Microsoft Windows PCs ('PC'), Microsoft's Xbox One, Sony's PlayStation 4 ('PS4'), the Nintendo Switch, Apple macOS computers ('Mac'), and tablets (both Android-based and Microsoft's Surface series). Developers can also make their games available on game streaming platforms, such as GeForce Now, which consumers can access on various hardware." Hitt Declaration at ¶ 20 (footnote omitted).

Other than these statements, all of the specific empirical evidence in paragraphs 21-44 on market definition that Professor Hitt claims support his claims that game developers have attractive options to substitute to other platforms are specific to Fortnite. The only exceptions are two surveys on the use of multiple platforms to play games (cited in footnotes 39, 51, and 52), which Professor Hitt cites to support his claim that Epic has other options for distributing Fortnite to users. Professor Hitt's analysis is of the options for Epic for distributing Fortnite, not the options for game developers generally, nor the options for all app developers.

<sup>62</sup> Jeff Dunn, "The video game industry now gets more money making games for smartphones and tablets than for consoles or PCs," Business Insider, June 22, 2017, <https://www.businessinsider.com/mobile-games-more-money-than-console-pc-chart-2017-6> ("There's a common feeling among video game enthusiasts that mobile games don't really count. . . . Smartphones have been a big catalyst for the industry's growth in recent years, thanks in big part to their ubiquity. In the developed world, nearly everyone has a smartphone in his or her pocket these days. While the quality of those games typically isn't as high as that on PC or Xbox games, they have expanded gaming's horizons, and made the art form accessible to more people."); Arjun Kharpal, "Sony set to make PlayStation games for iOS, Android," CNBC, March 24, 2016, <https://www.cnbc.com/2016/03/24/sony-set-to-make-playstation-games-for-ios-android.html> ("Smartphone games have done well at attracting so-called 'casual gamers' who may not necessarily be into console gaming."); Tushar Tajane, "The Rise of Mobile Games: Will

with the outside real world and are hence not suitable for use on gaming consoles or PCs.<sup>63</sup> Thus, Professor Hitt's focus on Fortnite provides an incomplete picture of what's available to game publishers generally.

56. I do not agree with Professor Hitt's claims that, even as to Epic, other distribution channels are close substitutes for Apple's iOS App Store to reach iOS users. But if I were to assume, strictly for the sake of argument, that Professor Hitt were correct, his evidence is incapable of establishing that the relevant market for the distribution of apps to iOS users is broader than Apple's iOS App Store for the following reasons.

57. One standard tool in market definition analysis is the hypothetical monopolist test, which is set out, for example, in the *Horizontal Merger Guidelines* issued by the US Department of Justice and the Federal Trade Commission. The hypothetical monopolist test asks whether a hypothetical monopolist of a candidate market can impose a "small but significant and non-transitory increase in price ('SSNIP')".<sup>64</sup> When one conducts the hypothetical monopolist test, it is almost always the case that some marginal consumers will react to the price increase by substituting to products that are outside the candidate market.

58. The relevant question for market definition is whether there is *enough* switching by marginal customers to make a SSNIP by the hypothetical monopolist unprofitable. Identifying and focusing only on a single alleged marginal customer is not meaningful evidence that the relevant market is too narrow. As the *Horizontal Merger Guidelines* state:

Groups of products may satisfy the hypothetical monopolist test without including the full range of substitutes from which customers choose. The hypothetical monopolist test may identify a group of products as a relevant

---

Smartphones Replace Consoles?" December 4, 2018, <https://techzoom.org/rise-mobile-games-smartphones-replace-consoles/> ("It isn't like traditional PC and Console gamers have switched over to mobile games, but more like the accessibility of mobile games have attracted a huge number of casual gamers to the industry. Most of the people who play and spend money on mobile games do not usually play on consoles or PCs, while PC and console gamers might play a few mobile games every now and then; it is very rare to find gamers who have switched over completely to the mobile platform.").

<sup>63</sup> Pokémon Go is only available on Android and iOS devices. See Pokémon Go, "Pokémon Go Homepage," <https://www.pokemongo.com/en-us/>.

<sup>64</sup> See, e.g., Horizontal Merger Guidelines, US Department of Justice and Federal Trade Commission, Section 7, August 19, 2010, at 4.1.1, <https://www.justice.gov/atr/horizontal-merger-guidelines-08192010>.

market even if customers would substitute significantly to products outside that group in response to a price increase.<sup>65</sup>

Any given antitrust market will almost always include some marginal consumers that would switch to products outside the defined market in the face of a price increase imposed by the hypothetical monopolist. That is, even if Professor Hitt had shown that Epic has good alternatives to Apple's iOS App Store to reach iOS users, which he did not, this does not disprove the finding I reached in my opening declaration that Apple is a monopoly supplier of iOS app distribution.

## **B. Professor Hitt's Analysis Contains Other Significant Flaws**

59. In this section, I address other significant flaws in Professor Hitt's analysis of market definition and market power.

### **1. Use of Different Products in Different Circumstances Does Not Demonstrate That They Are Substitutes**

60. Professor Hitt claims that Epic has a number of alternatives for distributing Fortnite to iOS users other than through Apple's iOS App Store. He presents information that some users who play Fortnite on the Fortnite iOS app also play Fortnite on other platforms (although most do not, as he noted).<sup>66</sup>

61. This type of evidence is not meaningful as to whether users would be willing to switch, in response to a SSNIP, from playing Fortnite on iOS to playing Fortnite on other platforms for those use cases where they play on iOS. For example, if someone plays Fortnite while outside the home or does not have access to a reliable non-cellular Internet connection, playing Fortnite on a gaming console or gaming PC are not good alternatives. My understanding is that Epic believes, based on its experience, that non-mobile platforms are not good substitutes for playing Fortnite on mobile devices.

62. To illustrate the flaw in Professor Hitt's methodology, consider the options that consumers have for transportation in the normal state of the world when there's no pandemic.

---

<sup>65</sup> Horizontal Merger Guidelines, US Department of Justice and Federal Trade Commission, Section 7, August 19, 2010, at 4.1.1, <https://www.justice.gov/atr/horizontal-merger-guidelines-08192010>.

<sup>66</sup> Hitt Declaration at ¶ 34.

Someone living in San Francisco, for example, could use a range of options, including BART, Muni trains, buses, taxis, ride-sharing services (like Uber or Lyft), driving (if they own a car), biking, and walking. Most consumers likely use many of these options in different circumstances. Sometimes, if time is tight and it's raining, they might take an Uber. At other times, if the weather is nice and they want a little exercise, they might walk or bike. Or, if there is a convenient route, they might take the BART.

63. The fact that many consumers use different alternatives when faced with different circumstances does not mean that, for example, there might not be a relevant antitrust market consisting of taxis and ride-sharing services.<sup>67</sup> Nor does the fact that a consumer who sometimes uses Uber and sometimes bikes mean that she is not harmed if the provision of taxis and ride-sharing services is monopolized. The mere fact that some consumers use different products in different circumstances does not provide reliable information that they are willing to substitute among them in a way that prevents the exercise of market power.<sup>68</sup>

## **2. Professor Hitt Commits the Cellophane Fallacy**

64. In Professor Hitt's analysis of market definition, he presents evidence that he claims shows the existence of alternatives available to Epic for distributing Fortnite to iOS users other than through the iOS App Store.<sup>69</sup> Professor Hitt has committed the classic "Cellophane Fallacy", which was named after a case in which DuPont was found not to have had market power over its Cellophane wrapping product because of the existence of consumers who substituted to alternative wrapping products.<sup>70</sup> The analytical error results from considering the substitution behavior of consumers when the monopolist has already exercised market power.

---

<sup>67</sup> This example is illustrative. I have not undertaken an analysis of market definition in the context of transportation services.

<sup>68</sup> I discuss these issues in more detail in Sections II.B and II.C.1 of my opening declaration.

<sup>69</sup> As I discuss in Section III.B.3 below, the fact that some consumers use different platforms in different circumstances does not demonstrate that those alternatives are in the same relevant market.

<sup>70</sup> Landes, William and Richard A. Posner (1981), "Market Power in Antitrust Cases," *Harvard Law Review* 94(5), pp. 937-996; Schaerr, Gene (1985) "The Cellophane Fallacy and the Justice Department's Guidelines for Horizontal Mergers," *Yale Law Journal* 94(3), pp. 670-693; Werden, Gregory (2000), "Market Delineation under the Merger Guidelines: Monopoly Cases and Alternative Approaches," *Review of Industrial Organization* 16(2), pp. 211-218.

65. Basic economic principles tell us that a profit-maximizing monopolist will raise prices to the point that enough consumers would, in fact, switch to alternative products (or stop buying the monopolist's product altogether) to make any further increase in price unprofitable. The monopolist is basically trying to find the point at which the increased profit from charging higher prices to consumers who don't switch outweighs the decreased profits from those who do switch. It is always profitable for the monopolist to continue raising prices until there is switching.

66. Suppose, contrary to Professor Hitt, that Apple is a monopolist over the distribution of apps to iOS users. In that case, economists would expect to observe switching behavior between iOS and other platforms as a result of Apple having exercised its monopoly power. Professor Hitt does not provide any meaningful support for his claims that Apple's iOS App Store practices are competitive, as I discuss in Section III.B.7 below. Given this lack of evidence, Professor Hitt's claims about the existence of substitution options suffers from the Cellophane Fallacy, which tell us that, in this context, if Apple were exercising monopoly power, exercise of such power would be expected to result in switching behavior, but that switching behavior is not relevant to the assessment of the relevant market because it is not switching that results from a SSNIP from competitive levels.

### **3. Professor Hitt's Focus on the Existence of Fortnite Users on Non-iOS Platforms Is Misplaced**

67. Professor Hitt argues that, "Only a minority of Fortnite's users play exclusively on iPhones and iPads, consistent with a broader relevant antitrust market."<sup>71</sup> The fact that Fortnite has many users who play on other platforms rather than on iOS does not provide any reliable evidence that those alternative platforms are good substitutes for iOS users. Simply observing that Fortnite has many users who play on a gaming PC, for example, does not tell us anything about whether Fortnite users who play on iOS have gaming PCs at all or are willing to buy a new gaming PC in order to play Fortnite, or have access to those gaming PCs at the times that they want to play Fortnite on iOS.

---

<sup>71</sup> Hitt Declaration at Section 3.2.1 (heading title).



68. The fact that much of Fortnite’s revenues comes from platforms other than iOS does not tell us anything reliable about Epic’s ability to reach iOS users on those other platforms. For example, suppose an app was used on a worldwide basis, with 20 percent of users and revenues coming from Europe. If the app developer was prevented from distributing the app in Europe because of government restrictions, the fact that 80 percent of its sales are in other countries doesn’t mean that distribution in those other countries are alternative channels of reaching European customers. And it doesn’t mean that the developer can sell “more” to non-European customers to make up for its lack of access to European customers—we would expect the developer to already be selling as much as is profitable to non-European customers.

#### **4. Professor Hitt’s Claims About the Lack of Switching from iOS to Android Are Flawed**

69. Professor Hitt claims that “Dr. Evans also exaggerates the difficulty of switching from iOS to Android devices in at least two ways. First, consumers do switch. Second, consumers that do not switch are not necessarily locked in.”<sup>72</sup> He cites statistics that “almost half of consumers replace their smartphones every 2 years.”<sup>73</sup> Professor Hitt, however, ignores the fact that, as I discussed in my opening declaration, iPhone sales in 2019 were only about one fifth of Apple’s total installed base of about 1 billion active iPhones.<sup>74</sup> That leaves about four fifths, or up to 800 million active iPhones, for which users are not buying new smartphones in a given year.

70. Professor Hitt does not address the substance of the eight sources of switching costs I discussed in my opening report.<sup>75</sup> Instead, he argues that “Several of the ‘switching costs’ that Dr. Evans identifies are properly understood as real value that Apple has added to the iOS ecosystem in its efforts to compete, not as switching costs that are locking consumers in.”<sup>76</sup> He argued that “iCloud Photos, iCloud Drive, Apple News, and Apple TV+” are not switching costs because “[t]hese services exist in the first place precisely because Apple continuously

---

<sup>72</sup> Hitt Declaration at ¶ 45.

<sup>73</sup> Hitt Declaration at ¶ 45.

<sup>74</sup> Evans Declaration at ¶¶ 41, 44.

<sup>75</sup> For a discussion of those switching costs, *see* Evans Declaration at Section II.B.2.c.

<sup>76</sup> Hitt Declaration at ¶ 45.



innovates and rolls out new features and service to make its platform more attractive than the platforms of its competitors.”<sup>77</sup>

71. Professor Hitt has misinterpreted the evidence on switching costs I documented. The point I made was not that iCloud Photos, for example, is a switching cost because users love iCloud Photos so much that they would not want to use a different cloud photo service on Android. Rather, iCloud Photos constitutes a switching cost because an iPhone user who switched to Android would need to figure out how to transfer her entire photo library over to an Android cloud photo service and would lose the synchronization of her photos with any other Apple devices she owned and anyone sharing her iCloud Photos. I also note that the specific examples he raised apply only to portions of four of the eight sources of switching costs I identified. He did not provide a specific response to the other four sources of switching costs I identified.<sup>78</sup>

## **5. Professor Hitt’s Share Estimates Are Wrong**

72. Professor Hitt claims that the relevant antitrust market includes at least personal computers, handheld gaming devices, gaming consoles, handheld devices (iOS and Android smartphones and tablets and Microsoft Surface tablets), and streaming game platforms, and may include other web gaming platforms.<sup>79</sup> He then reports “market shares” that are based not on transactions in this proposed market, but on transactions involving Fortnite only. As an economic matter, these single customer shares are not relevant to measuring any aspect of a relevant antitrust market because they do not in fact pertain to that market.

---

<sup>77</sup> Hitt Declaration at ¶ 45.

<sup>78</sup> As I have explained, Professor Hitt has incorrectly interpreted the switching cost evidence documented in my opening declaration. But, even if I assumed Professor Hitt were correct that some of the switching costs reflect “real value” provided by Apple, this value would mean that those features provide Apple with market power because iOS users are less willing to substitute to Android devices and give up those features. A monopolist that, hypothetically, has a legitimately earned monopoly by selling a much better product than any rival is still a monopolist. Its customers will be resistant to substituting to a competitor’s products. Lack of good substitutes is often an explanation for why a firm has substantial market power.

<sup>79</sup> Hitt Declaration at ¶ 49.

**6. The Fact that Some Consumers Used IAP When Offered Epic “Direct Pay” Has No Relevance**

73. Professor Hitt claims that the experience from iOS Fortnite users having a choice of Epic “Direct Pay” in addition to Apple’s IAP payment processing showed that “nearly half of all consumers valued Apple’s platform services enough to overcome a 20 percent price differential.”<sup>80</sup> The percentage of users who chose the Epic Direct Pay option increased over time—from the start of the Direct Pay option being offered (August 13) to the point when the Apple IAP option was no longer available because Epic’s developer account ending in ’84 was terminated by Apple (midday August 28), about 73 percent of purchases were on Epic Direct Pay.<sup>81</sup>

74. The fact that material numbers of consumers chose Direct Pay is strong evidence that payment processing methods, including IAP, are separate products. The fact that some consumers also chose IAP instead of Direct Pay is not relevant to the separate products inquiry. We would generally expect that after removing a tie, some consumers would continue to purchase the tied product from the seller of the tying product.

**7. Professor Hitt’s Claim that Apple’s Commission Is Not Supracompetitive Is Not Reliable**

75. Professor Hitt claims that “Apple’s commission is not supracompetitive.”<sup>82</sup> The overarching problem with this assertion is that Professor Hitt makes no attempt to consider a counterfactual world in which the Apple restraints at issue were not in place. Without doing so, he cannot reliably reach a conclusion that Apple’s restraints have not harmed competition.

76. He makes three main points in support of this claim. First, he states that Apple has never raised its 30 percent base fee since it was introduced in 2008 and that it has reduced it for subscriptions after the first year.<sup>83</sup> He does not consider the profit that Apple makes on in-app purchases or analyze whether those profits have increased over time. This information is not available publicly and would have to come directly from Apple. The fact that Apple has never

---

<sup>80</sup> Hitt Declaration at ¶ 70.

<sup>81</sup> Calculations based on data from Epic.

<sup>82</sup> Hitt Declaration at Section 4.3 (heading title).

<sup>83</sup> Hitt Declaration at ¶ 57.

raised its commission is uninformative of whether Apple's price is supracompetitive, and stating this fact is not a substitute for a serious analysis of the issue.

77. Professor Hitt's second point is that "Apple's commission structure and its base 30 percent rate is not unique. Many other app stores have a similar payment structure and the same base level of commissions."<sup>84</sup> The commission rate charged by other app stores, in other markets, does not tell us how much developers would pay in the absence of the conduct at issue in this matter. Information on the profitability of the App Store, and the contribution from commissions on in-app payments, would be useful for assessing this. Moreover, as I discussed in Section II.D, commissions are not charged at all for many types of in-app purchases. And in the case of some app stores, no commissions are charged for any in-app purchases.

78. Professor Hitt's last point is that the quality of services provided to developers has increased over time.<sup>85</sup> Apple's commission, however, is expressed as a percentage of the developer's revenue. To the extent that iOS developers can earn more revenue as a result of an increase in quality, Apple's fee increases. So, Apple earns more in fee revenue if it provides an increase in quality that allows developers to sell more to users. Moreover, as noted above, Professor Hitt does not consider whether Apple's profits from its App Store, as opposed to its commission rate, have increased.

---

<sup>84</sup> Hitt Declaration at ¶ 58.

<sup>85</sup> Hitt Declaration at ¶ 59.

Pursuant to 28 U.S.C. § 1746, I, David S. Evans, declare under penalty of perjury that the foregoing is true and correct and that I executed this declaration on September 18, 2020 PT in Marblehead, Massachusetts.



A handwritten signature in black ink, appearing to read "D S Evans", written above a horizontal line.

1 Paul J. Riehle (SBN 115199)  
paul.riehle@faegredrinker.com  
2 **FAEGRE DRINKER BIDDLE & REATH LLP**  
Four Embarcadero Center  
3 San Francisco, California 94111  
Telephone: (415) 591-7500  
4 Facsimile: (415) 591-7510

5 Christine A. Varney (*pro hac vice*)  
cvarney@cravath.com  
6 Katherine B. Forrest (*pro hac vice*)  
kforrest@cravath.com  
7 Gary A. Bornstein (*pro hac vice*)  
gbornstein@cravath.com  
8 Yonatan Even (*pro hac vice*)  
yeven@cravath.com  
9 Lauren A. Moskowitz (*pro hac vice*)  
lmoskowitz@cravath.com  
10 M. Brent Byars (*pro hac vice*)  
mbyars@cravath.com

11 **CRAVATH, SWAINE & MOORE LLP**  
825 Eighth Avenue  
12 New York, New York 10019  
Telephone: (212) 474-1000  
13 Facsimile: (212) 474-3700

14 *Attorneys for Plaintiff Epic Games, Inc.*

15 **UNITED STATES DISTRICT COURT**  
16 **NORTHERN DISTRICT OF CALIFORNIA**  
17 **OAKLAND DIVISION**

19 EPIC GAMES, INC.,

21 Plaintiff,

22 vs.

23 APPLE INC.,

24 Defendant.

No. 4:20-CV-05640-YGR

**DECLARATION OF M. BRENT  
BYARS IN FURTHER SUPPORT OF  
PLAINTIFF EPIC GAMES INC.'S  
MOTION FOR PRELIMINARY  
INJUNCTION**

Date: September 28, 2020, 9:30 a.m. (via  
Zoom Platform)

Courtroom: 1, 4th Floor

Judge: Hon. Yvonne Gonzalez Rogers

1 I, M. Brent Byars, declare as follows:

2 1. I am an attorney at the law firm of Cravath, Swaine & Moore LLP, and am one of  
3 the attorneys representing Epic Games, Inc. in this action. I am admitted to appear before this  
4 Court *pro hac vice*.

5 2. I submit this declaration in further support of Plaintiff Epic Games, Inc.'s Motion  
6 for Preliminary Injunction (ECF No. 61). The contents of this declaration are based on my  
7 personal knowledge and on information and documents provided to me by Epic Games, Inc. If  
8 called as a witness, I could and would competently testify thereto.

9 3. Attached hereto as **Exhibit A** is a true and correct copy of a letter from Katherine  
10 B. Forrest to counsel for Apple, Inc., dated August 27, 2020.

11 4. Attached hereto as **Exhibit B** is a true and correct copy of a letter from Richard J.  
12 Doren to Katherine B. Forrest, dated August 28, 2020.

13 5. Attached hereto as **Exhibit C** is a true and correct copy of an email thread,  
14 including an email from M. Brent Byars to Jay P. Srinivasan, dated September 2, 2020.

15 6. Attached hereto as **Exhibit D** is a true and correct copy of an email from Yonatan  
16 Even to Richard J. Doren and Jay Srinivasan, dated September 8, 2020.

17 7. Attached hereto as **Exhibit E** is a true and correct copy of a letter from Richard J.  
18 Doren to Yonatan Even, dated September 10, 2020.

19 8. Attached hereto as **Exhibit F** is a true and correct copy of Apple's App Store  
20 Review Guidelines, updated September 11, 2020 (last accessed September 18, 2020), available at  
21 <https://developer.apple.com/app-store/review/guidelines/>.

22 9. Attached hereto as **Exhibit G** is a true and correct copy of Google's Google Play  
23 Developer Distribution Agreement, effective as of June 12, 2020 (last accessed September 18,  
24 2020), available at <https://play.google.com/about/developer-distribution-agreement.html>.

25 10. Attached hereto as **Exhibit H** is a true and correct copy of Google's Developer  
26 Program Policy, effective as of August 12, 2020 (last accessed September 18, 2020), available at  
27 [https://support.google.com/googleplay/android-](https://support.google.com/googleplay/android-developer/answer/9914283?visit_id=637360682421231288-1413471540&rd=1)  
28 [developer/answer/9914283?visit\\_id=637360682421231288-1413471540&rd=1](https://support.google.com/googleplay/android-developer/answer/9914283?visit_id=637360682421231288-1413471540&rd=1).

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

11. Attached hereto as **Exhibit I** is a true and correct copy of an email from Steve Jobs to Eddy Cue, dated February 6, 2011, which I obtained from the website of the House Committee on the Judiciary (last accessed September 18, 2020), available at <https://judiciary.house.gov/uploadedfiles/014816.pdf>.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct and that I executed this declaration on September 18, 2020 in New York City, New York.



---

M. Brent Byars

# **Exhibit A**



## CRAVATH, SWAINE & MOORE LLP

WORLDWIDE PLAZA  
825 EIGHTH AVENUE  
NEW YORK, NY 10019-7475

TELEPHONE: +1-212-474-1000  
FACSIMILE: +1-212-474-3700

CITYPOINT  
ONE ROPEMAKER STREET  
LONDON EC2Y 9HR  
TELEPHONE: +44-20-7453-1000  
FACSIMILE: +44-20-7860-1150

WRITER'S DIRECT DIAL NUMBER  
kforrest@cravath.com

WRITER'S EMAIL ADDRESS  
(212) 474-1151

JOHN W. WHITE  
EVAN R. CHESLER  
RICHARD W. CLARY  
STEPHEN L. GORDON  
ROBERT H. BARON  
DAVID MERCADO  
CHRISTINE A. VARNEY  
PETER T. BARBUR  
THOMAS G. RAFFERTY  
MICHAEL S. GOLDMAN  
RICHARD HALL  
JULIE A. NORTH  
ANDREW W. NEEDHAM  
STEPHEN L. BURNS  
KATHERINE B. FORREST  
KEITH R. HUMMEL  
DAVID J. KAPPOS  
DANIEL SLIFKIN  
ROBERT I. TOWNSEND, III  
PHILIP J. BOECKMAN  
WILLIAM V. FOGG  
FAIZA J. SAEED  
RICHARD J. STARK  
THOMAS E. DUNN  
MARK I. GREENE

DAVID R. MARRIOTT  
MICHAEL A. PASKIN  
ANDREW J. PITTS  
MICHAEL T. REYNOLDS  
ANTONY L. RYAN  
GEORGE E. ZOBITZ  
GEORGE A. STEPHANAKIS  
DARIN P. MCATEE  
GARY A. BORNSTEIN  
TIMOTHY G. CAMERON  
KARIN A. DEMASI  
DAVID S. FINKELSTEIN  
DAVID GREENWALD  
RACHEL G. SKAISTIS  
PAUL H. ZUMBRO  
ERIC W. HILFERS  
GEORGE F. SCHOEN  
ERIK R. TAVZEL  
CRAIG F. ARCELLA  
DAMIEN R. ZOUBEK  
LAUREN ANGELILLI  
TATIANA LAPUSHCHIK  
ALYSSA K. CAPLES  
JENNIFER S. CONWAY  
MINH VAN NGO

KEVIN J. ORSINI  
MATTHEW MORREALE  
JOHN D. BURETTA  
J. WESLEY EARNHARDT  
YONATAN EVEN  
BENJAMIN GRUENSTEIN  
JOSEPH D. ZAVAGLIA  
STEPHEN M. KESSING  
LAUREN A. MOSKOWITZ  
DAVID J. PERKINS  
JOHNNY G. SKUMPIJA  
J. LEONARD TETI, II  
D. SCOTT BENNETT  
TING S. CHEN  
CHRISTOPHER K. FARGO  
KENNETH C. HALCOM  
DAVID M. STUART  
AARON M. GRUBER  
O. KEITH HALLAM, III  
OMID H. NASAB  
DAMARIS HERNÁNDEZ  
JONATHAN J. KATZ  
MARGARET SEGALL D'AMICO  
RORY A. LERARIS  
KARA L. MUNGOVAN

NICHOLAS A. DORSEY  
ANDREW C. ELKEN  
JENNY HOCHENBERG  
VANESSA A. LAVELY  
G.J. LIGELIS JR.  
MICHAEL E. MARIANI  
LAUREN R. KENNEDY  
SASHA ROSENTHAL-LARREA  
ALLISON M. WEIN  
MICHAEL P. ADDIS  
JUSTIN C. CLARKE  
SHARONMOYEE GOSWAMI  
C. DANIEL HAAREN  
EVAN MEHRAN NORRIS  
LAUREN M. ROSENBERG  
  
SPECIAL COUNSEL  
SAMUEL C. BUTLER  
  
OF COUNSEL  
MICHAEL L. SCHLER  
CHRISTOPHER J. KELLY

August 27, 2020

*Epic Games, Inc. v. Apple Inc.*, No. 20-cv-05640-YGR

Dear Counsel:

We write on behalf of Epic Games, Inc. (“Epic”) to raise an urgent concern about Apple’s proposed termination of Epic’s developer account (Team ID # 8XJ6WJ8Z84, “the ’84 account”) and potential consequential effects on third-party game developers whose Epic Games Store customers use the Sign In with Apple service, Epic account owners who use the Sign In with Apple service to access third-party games, and third-party developers who access the Unreal Engine using the Sign In with Apple service.

As you know, in the Temporary Restraining Order entered on Monday, the Court wrote that the dispute between Apple and Epic “should not create havoc to bystanders”. (ECF No. 48 at 7.) The Court wrote that “during the period of a temporary restraining order the status quo in this regard should be maintained”. (*Id.*) That status quo is one which third-party game developers whose Epic Games Store customers use the Sign In with Apple service, Epic account owners who use the Sign In with Apple service to access third-party games, and third-party developers who access the Unreal Engine using the Sign In with Apple service continue to have unimpaired access to those services. Epic is concerned that Apple’s termination of the ’84 account may disrupt this status quo for third parties, contrary to the Temporary Restraining Order.

Certain users of services provided by Epic must create and use accounts in Epic’s systems. When users of Apple devices create or access an Epic account, they may choose to use Apple’s Sign In with Apple service. For many of these users, the Sign in with Apple service is the only way users have accessed their Epic accounts, and the only way such users could access their accounts in the future. Other users have requested, as part of their use of the Sign in with Apple service, that Apple create private email relay addresses rather than providing their email addresses directly to Epic. If Apple takes steps that prevent the use of the Sign In with Apple

service to access Epic accounts, many users will be unable to access their Epic accounts, and Epic could even lose the ability to communicate with its own users through private email relays.

Epic therefore requests that Apple confirm that it will not take any steps that impair the Sign in with Apple service used by third-parties who rely on Epic services. We are available to discuss this issue on an urgent basis during the course of the day today and to work cooperatively with Apple to ensure that third parties are not harmed. Epic reserves all rights.

Sincerely,

s/ Katherine B. Forrest

Theodore J. Boutrous, Jr.  
Richard Doren  
Cynthia Richman  
Daniel Swanson  
Jay Srinivasan  
Veronica Lewis  
GIBSON, DUNN & CRUTCHER LLP  
tboutrous@gibsondunn.com  
rdoren@gibsondunn.com  
crichman@gibsondunn.com  
dswanson@gibsondunn.com  
jsrinivasan@gibsondunn.com  
vlewis@gibsondunn.com

VIA EMAIL

# **Exhibit B**

Gibson, Dunn & Crutcher LLP  
333 South Grand Avenue  
Los Angeles, CA 90071-3197  
Tel 213.229.7000  
www.gibsondunn.com

Richard J. Doren  
Direct: +1 213.229.7038  
Fax: +1 213.229.6038  
RDoren@gibsondunn.com

August 28, 2020

VIA ELECTRONIC MAIL

Katherine Forrest  
Cravath, Swaine & Moore LLP  
Worldwide Plaza  
825 Eighth Avenue  
New York, NY 10019-7475

Re: *Epic Games, Inc. v. Apple Inc.*, No. 20-cv-05640-YGR

Dear Katherine:

Two weeks ago, Apple informed Epic Games, Inc. (“Epic”) that, because of its willful breaches of the Developer Program License Agreement and violations of the App Store App Review Guidelines, Apple would terminate Epic’s Developer Program account unless Epic submitted a compliant Fortnite app. You sought a TRO in favor of Epic Games, Inc. and its affiliates. That request was denied as to Epic Games, Inc. because of your gross violations of your agreements with Apple. Apple is entirely within its rights to terminate Epic Games, Inc.’s developer account and all related functionality, but Sign In with Apple will continue to function for Apple customers for the next two weeks.

This is a problem of Epic’s making, and the resolution is entirely within Epic’s control. It is not a matter of “urgent concern” for either Apple or the Court. If the future loss of this functionality is of concern to Epic, Apple suggests Epic start the relevant engineering work immediately. If Epic’s engineers have questions of Apple’s, they have worked together in the past and Epic knows how to reach them.

Sincerely,  
20200828 10:45:00 AM Document 88-5 Filed 08/28/20 Page 5 of 5

s/ Richard J. Doren

RJD/bxy

# Exhibit C

**From:** Brent Byars <[MByars@cravath.com](mailto:MByars@cravath.com)>  
**Date:** September 2, 2020 at 11:02:13 PM EDT  
**To:** "Srinivasan, Jay P." <[JSrinivasan@gibsondunn.com](mailto:JSrinivasan@gibsondunn.com)>  
**Cc:** "Richman, Cynthia" <[CRichman@gibsondunn.com](mailto:CRichman@gibsondunn.com)>, Christine Varney <[cvarney@cravath.com](mailto:cvarney@cravath.com)>, "[dwanson@gibsondunn.com](mailto:dwanson@gibsondunn.com)" <[dwanson@gibsondunn.com](mailto:dwanson@gibsondunn.com)>, Gary Bornstein <[GBornstein@cravath.com](mailto:GBornstein@cravath.com)>, Katherine Forrest <[kforrest@cravath.com](mailto:kforrest@cravath.com)>, Lauren Moskowitz <[LMoskowitz@cravath.com](mailto:LMoskowitz@cravath.com)>, "Doren, Richard J." <[RDoren@gibsondunn.com](mailto:RDoren@gibsondunn.com)>, "Boutrous Jr., Theodore J." <[TBoutrous@gibsondunn.com](mailto:TBoutrous@gibsondunn.com)>, "Lewis, Veronica S." <[VLewis@gibsondunn.com](mailto:VLewis@gibsondunn.com)>, Yonatan Even <[YEven@cravath.com](mailto:YEven@cravath.com)>  
**Subject: Re: Epic Games, Inc. v. Apple Inc.--Urgent correspondence from Katherine Forrest**

Richard and Jay,

We've not heard back from Apple about this. Please have the appropriate Apple personnel contact Epic tomorrow, so that the parties can resolve this issue without the need to bring it to the Court.

Brent

On Aug 29, 2020, at 7:14 PM, Brent Byars <[MByars@cravath.com](mailto:MByars@cravath.com)> wrote:

Richard and Jay,

We disagree with a number of the assertions and characterizations in your letter, but do not feel that it would be productive to catalog or debate them here. Epic employees have initiated contact with the Apple employees with whom they have interacted regarding Sign in with Apple during the normal course of business--see attached email. We expect that Apple and Epic will have a cooperative relationship to ensure that third parties who rely on Sign in with Apple to access Epic accounts retain that access after the two-week period mentioned in your letter. Epic reserves all rights.

Brent

*(See attached file: Epic Games Mail - Epic Games SiwA Migration.pdf)*

"Srinivasan, Jay P." ---08/28/2020 03:31:56 PM---Brent, See letter attached.

From: "Srinivasan, Jay P." <[JSrinivasan@gibsondunn.com](mailto:JSrinivasan@gibsondunn.com)>  
To: "Brent Byars" <[MByars@cravath.com](mailto:MByars@cravath.com)>, "Boutrous Jr., Theodore J." <[TBoutrous@gibsondunn.com](mailto:TBoutrous@gibsondunn.com)>, "Doren, Richard J." <[RDoren@gibsondunn.com](mailto:RDoren@gibsondunn.com)>, "Richman, Cynthia" <[CRichman@gibsondunn.com](mailto:CRichman@gibsondunn.com)>, "[dwanson@gibsondunn.com](mailto:dwanson@gibsondunn.com)" <[dwanson@gibsondunn.com](mailto:dwanson@gibsondunn.com)>, "Lewis, Veronica S." <[VLewis@gibsondunn.com](mailto:VLewis@gibsondunn.com)>  
Cc: "[cvarney@cravath.com](mailto:cvarney@cravath.com)" <[cvarney@cravath.com](mailto:cvarney@cravath.com)>, "Katherine Forrest" <[kforrest@cravath.com](mailto:kforrest@cravath.com)>, "Gary Bornstein" <[GBornstein@cravath.com](mailto:GBornstein@cravath.com)>, "Yonatan Even" <[YEven@cravath.com](mailto:YEven@cravath.com)>, "Lauren Moskowitz" <[LMoskowitz@cravath.com](mailto:LMoskowitz@cravath.com)>  
Date: 08/28/2020 03:31 PM  
Subject: RE: Epic Games, Inc. v. Apple Inc.--Urgent correspondence from Katherine Forrest

---

External ([jsrinivasan@gibsondunn.com](mailto:jsrinivasan@gibsondunn.com))

[Report This Email](#) [FAQ](#)

Brent,

See letter attached.

Thanks,

Jay

**Jay P. Srinivasan**

**GIBSON DUNN**

Gibson, Dunn & Crutcher LLP  
333 South Grand Avenue, Los Angeles, CA 90071-3197  
Tel +1 213.229.7296 • Fax +1 213.229.6296  
[JSrinivasan@gibsondunn.com](mailto:JSrinivasan@gibsondunn.com) • [www.gibsondunn.com](http://www.gibsondunn.com)

**From:** Brent Byars <[MByars@cravath.com](mailto:MByars@cravath.com)>

**Sent:** Thursday, August 27, 2020 11:28 AM

**To:** Boutrous Jr., Theodore J. <[TBoutrous@gibsondunn.com](mailto:TBoutrous@gibsondunn.com)>; Doren, Richard J. <[RDoren@gibsondunn.com](mailto:RDoren@gibsondunn.com)>; Richman, Cynthia <[CRichman@gibsondunn.com](mailto:CRichman@gibsondunn.com)>; [dwanon@gibsondunn.com](mailto:dwanon@gibsondunn.com); Srinivasan, Jay P. <[JSrinivasan@gibsondunn.com](mailto:JSrinivasan@gibsondunn.com)>; Lewis, Veronica S. <[VLewis@gibsondunn.com](mailto:VLewis@gibsondunn.com)>

**Cc:** [cvarney@cravath.com](mailto:cvarney@cravath.com); Katherine Forrest <[kforrest@cravath.com](mailto:kforrest@cravath.com)>; Gary Bornstein <[GBornstein@cravath.com](mailto:GBornstein@cravath.com)>; Yonatan Even <[YEven@cravath.com](mailto:YEven@cravath.com)>; Lauren Moskowitz <[LMoskowitz@cravath.com](mailto:LMoskowitz@cravath.com)>

**Subject:** Epic Games, Inc. v. Apple Inc.--Urgent correspondence from Katherine Forrest

[External Email]

Counsel,

Please see the attached urgent correspondence from Katherine Forrest.

Brent

---

This e-mail is confidential and may be privileged. Use or disclosure of it by anyone other than a designated addressee is unauthorized. If you are not an intended recipient, please delete this e-mail from the computer on which you received it.

---

This message may contain confidential and privileged information for the sole use of the intended recipient. Any review, disclosure, distribution by others or forwarding without express permission is strictly prohibited. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message.

Please see our website at <https://www.gibsondunn.com/> for information regarding the firm and/or our privacy policy. [attachment "8.28 Response from R. Doren to K. Forrest.pdf" deleted by Brent Byars/NYC/Cravath]

---

<Epic Games Mail - Epic Games SiwA Migration.pdf>

# Exhibit D



**From:** Yonatan Even  
**Sent:** Tuesday, September 8, 2020 2:24 PM  
**To:** rdoren@gibsondunn.com; jsrinivasan@gibsondunn.com  
**Cc:** Christine Varney; Katherine Forrest; Gary Bornstein; Brent Byars; John Karin  
**Subject:** Epic v. Apple / Sign in with Apple

Richard and Jay,

As you know, prior to Apple's termination of Epic's '84 Apple developer account on August 28, Epic expressed concern that third parties who use the Sign in with Apple service to access their Epic accounts would lose that access as a result of that termination, contrary to the Temporary Restraining Order. Third parties that are affected by this issue include Unreal Engine users, as well as third-party game developers who use Epic services and their customers.

In Mr. Doren's letter of August 28, 2020, Apple indicated that these third parties would retain access to Sign in with Apple for two weeks from that date, demonstrating that loss of access to the Sign in with Apple service was not a necessary consequence of the termination of the '84 developer account, but rather Apple's choice. You suggested in that letter that Apple engineers would assist Epic in finding a solution that would ensure that Sign in with Apple users would not lose access to their Epic accounts after the two-week period.

Six days later, on the afternoon (ET) of Thursday, September 3, Apple responded, clarifying that its engineers will *not* work with Epic to solve the issue in a way that would be transparent to users, and suggesting instead that Epic "build a custom flow to migrate users off Sign In with Apple by collecting email addresses or asking users to select a different login method" – in other words, that Epic reach out to hundreds of thousands of users currently using SiwA and prompt them to take action to replace SiwA with an alternative mechanism.

Apple's response is both contrary to Mr. Doren's representations and unsatisfactory. Nonetheless, to avoid the need to involve the Court, Epic has been working diligently to prepare a mass email to the affected users, with instructions that, if followed, should resolve this issue for most (though likely not all) users. However, given the change in Apple's position and the time it has taken Apple to respond to Epic's outreach, any email Epic will send users will now be very close to the deadline Apple has arbitrarily chosen to turn off SiwA. Users deserve more time to implement the necessary steps to ensure continued access to their accounts.

Epic will send out an email to users tonight or tomorrow. In the meantime, and in order to provide users with the correct instructions, please confirm **by 5pm PST today** that Apple will not take any steps that impair the Sign in with Apple service used by third-parties who rely on Epic services until after the Court resolves Epic's pending motion for a preliminary injunction.

Epic reserves all rights.

Yonatan Even  
Cravath, Swaine & Moore LLP  
825 Eighth Avenue  
New York, NY 10019  
Telephone: (212) 474-1958  
Fax: (212) 474-3700

# **Exhibit E**

Richard J. Doren  
Direct: +1 213.229.7038  
RDoren@gjbsondunn.com

September 10, 2020

VIA ELECTRONIC MAIL

Yonatan Even  
Cravath, Swaine & Moore LLP  
825 Eighth Ave.  
New York, NY 10019

Re: *Epic Games, Inc. v. Apple Inc.*, No. 20-cv-05640-YGR

Yonatan,

We are in receipt of your email of September 8. I will reiterate that the difficulties you complain of are entirely of Epic’s own making. Epic chose to violate its agreements with Apple, knowing that this would lead to the termination of its developer account, and chose to do nothing to accommodate its users with respect to Sign in With Apple (“SIWA”). The Court denied your request for a temporary restraining order against the termination of Epic Games, Inc., which occurred on August 28. Nonetheless, as indicated in my letter to Katherine Forrest on that date, Apple voluntarily allowed an extra two weeks before it terminates Epic Games, Inc.’s access to SIWA. Nothing in the Court’s decision required Apple to do this.

I understand that, as I suggested in my August 28 letter, Epic personnel contacted Apple’s engineers with regard to this issue. One week ago today, Apple’s engineers responded by proposing a solution—that Epic build a custom flow to migrate users off SIWA by collecting email addresses or asking users to select a different login method. I further understand that (despite having had all the guidance necessary to do so for the prior six days) it was not until yesterday that Epic implemented the solution that Apple recommended. Epic’s unexplained delays notwithstanding, Apple will leave SIWA in place for the time being. Again, Apple does this voluntarily and while reserving all rights.

It should also be noted that we are surprised and puzzled by your assertion that terminating SIWA for the Epic Games, Inc. account will affect users of the *Unreal Engine*. Your client has repeatedly and consistently represented to the Court that the *Unreal Engine* is run by “a different company. It’s in Switzerland. It’s a totally different set of circumstances.” (Aug. 19, 2020 Hearing Tr. 10:25-11:2.) Your client’s briefs have assured the Court that the game production business of Epic Games, Inc. is distinct from “the separate *Unreal Engine* business” (Epic TRO Br. at 1), and that “the developer tools” that are “necessary to

Yonatan Even  
September 10, 2020  
Page 2

support . . . *Unreal Engine* . . . are covered by *separate* integrated agreements.” (Epic PI Br. at 30 (emphasis in original).) It is indeed true that the Developer Program account of Epic Games International, S.à.r.l. gives it the ability to use SIWA. If Epic has set up its *Unreal Engine* business to use this functionality through the Epic Games, Inc. account, that is Epic’s own doing. Further, it would again reflect the spuriousness of your client’s claim that *Unreal Engine* is a separate business from Epic Games, Inc. and an innocent, collateral victim of the crisis that Epic Games, Inc. has created.

Epic is fully aware of what it needs to do to remedy the problems that Epic has created for itself.

Sincerely,

/s/ Richard J. Doren

Richard J. Doren

RJD/eml

# **Exhibit F**

# App Store Review Guidelines

Apps are changing the world, enriching people’s lives, and enabling developers like you to innovate like never before. As a result, the App Store has grown into an exciting and vibrant ecosystem for millions of developers and more than a billion users. Whether you are a first time developer or a large team of experienced programmers, we are excited that you are creating apps for the App Store and want to help you understand our guidelines so you can be confident your app will get through the review process quickly.

- Introduction
- Before You Submit
  - 1. Safety
  - 2. Performance
  - 3. Business
  - 4. Design
  - 5. Legal
- After You Submit

## 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 Developer Program.
- You are responsible for making sure everything in your app complies with these guidelines, including ad networks, analytics services, and third-party SDKs, so review and choose them carefully.
- Some features and technologies that are not generally available to developers may be offered as an entitlement for limited use cases. For example, we offer entitlements for CarPlay Audio, HyperVisor, and Privileged File Operations. Review our documentation on developer.apple.com to learn more about entitlements.

We hope these guidelines help you sail through the App Review process, and that approvals and rejections remain consistent across the board. This is a living document; new apps presenting new questions may result in new rules at any time. Perhaps your app will trigger this. We love this stuff too, and honor what you do. We're really trying our best to create the best platform in the world for you to express your talents and make a living, too.

---

## Before You Submit

To help your app approval go as smoothly as possible, review the common missteps listed below that can slow down the review process or trigger a rejection. This doesn't replace the guidelines or guarantee approval, but making sure you can check every item on the list is a good start. If your app no longer functions as intended or you're no longer actively supporting it, it will be removed from the App Store. Learn more about App Store Improvements.

Make sure you:

- Test your app for crashes and bugs
- Ensure that all app information and metadata is complete and accurate
- Update your contact information in case App Review needs to reach you
- Provide an active demo account and login information, plus any other hardware or resources that might be needed to review your app (e.g. login credentials or a sample QR code)
- Enable backend services so that they're live and accessible during review
- Include detailed explanations of non-obvious features and in-app purchases in the App Review notes, including supporting documentation where appropriate.
- Check whether your app follows guidance in other documentation, such as:

### Development Guidelines

- UIKit
- AppKit
- WatchKit
- App Extensions
- iOS Data Storage Guidelines
- Apple File System
- App Store Connect Help
- Developer Account Help

### Design Guidelines

- Human Interface Guidelines

### Brand and Marketing Guidelines

- Marketing Resources and Identity Guidelines
- Apple Pay Marketing Guidelines
- Add to Apple Wallet Guidelines
- Guidelines for Using Apple Trademarks and Copyrights

---

## 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:

- 1.1.1 Defamatory, discriminatory, or mean-spirited content, including references or commentary about religion, race, sexual orientation, gender, national/ethnic origin, or other targeted groups, particularly if the app is likely to humiliate, intimidate, or harm a targeted individual or group. Professional political satirists and humorists are generally exempt from this requirement.
- 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."
- 1.1.5 Inflammatory religious commentary or inaccurate or misleading quotations of religious texts.
- 1.1.6 False information and features, including inaccurate device data or trick/joke functionality, such as fake location trackers. Stating that the app is "for entertainment purposes" won't overcome this guideline. Apps that enable anonymous or prank phone calls or SMS/MMS messaging will be rejected.

### 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 web-based 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.

### 1.3 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 third-party 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, 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 marijuana, tobacco, or controlled substances (except for licensed pharmacies) isn't 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.

### 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.

---

## 2. 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 login. 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.

## 2.3 Accurate Metadata

Customers should know what they're getting when they download or buy your app, so make sure your app description, screenshots, and previews accurately reflect the app's core experience and remember to keep them up-to-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, you should not market your app on the App Store or offline as including content or services that it does not actually offer (e.g. iOS-based virus and malware scanners). Egregious or repeated behavior is grounds for removal from the 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, log-in 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.

**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 for you.

**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 and should not include prices, terms, or descriptions that are not the name of the app. 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.

**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, Mac, Apple TV or Apple Watch 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, including but not limited to information about Apple or the development process.

**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.

## 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 application. 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 application 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 their icons to the Dock or leave short cuts on the user desktop.

**(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, Rosetta)

(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 may, in limited circumstances, download code provided that such code is not used for other purposes. Such apps must make the source code provided by the Application completely viewable and editable by the user.

**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 Developer Program.

**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.

### 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.

---

## 3. 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 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" 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.
- Remember to assign the correct purchasability type or your app will be rejected.
- 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.
- 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.

**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 a 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 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.
- 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.
- 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 or engage in bait-and-switch and scam practices will be removed from the App Store and you may be removed from the Apple Developer Program. Learn more about Subscription Free Trials.
- Apps that offer auto-renewing music and video subscriptions with prior approval by Apple may also be included in pre-defined bundles with cellular data plans offered in cellular carrier apps.

**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. Apps in this section cannot, either within the app or through communications sent to points of contact obtained from account registration within the app (like email or text), encourage users to use a purchasing method 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 video). Reader apps may offer account creation for free tiers, and account management functionality for existing customers.

**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 use purchase methods in addition to in-app purchase to collect those payments. Consumer, single user, or family sales must use in-app purchase.

**3.1.3(d) Person-to-Person Experiences:** If your app enables the purchase of realtime person-to-person experiences 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 realtime experiences 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.

**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.

### 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.

**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 Identity 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

**3.1.7 Advertising:** Display advertising should be limited to your main app executable, 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.

### 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 come from the financial institution performing such services or must use a public API offered by the institution in compliance with its Terms & Conditions.

#### 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.

(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 must not force users to rate the app, review the app, download other apps, or perform other similar actions in order to access functionality, content, or use of the app.

(x) 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.

---

## 4. 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, 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.

**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, 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.

**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, 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 Developer Program.

### 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 Developer Program. Safari extensions should not claim access to more websites than strictly necessary to function.

#### 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 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.

#### 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 Musicstream 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 Musicservices 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.

**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 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.

**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 (1) is free or purchased using in-app purchase; (2) only uses capabilities available in a standard WebKit view (e.g. it must open and run natively in Safari without modifications or additional software); your app must 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; (3) is offered by developers that have joined the Apple Developer Program and signed the Apple Developer Program License Agreement; (4) does not provide access to real money gaming, lotteries, or charitable donations; (5) adheres to the terms of these App Review Guidelines (e.g. does not include objectionable content); and (6) does not offer digital goods or services for sale. 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.
- Your app is a client for a specific third-party service and users are required to sign in to their mail, social media, or other third-party account directly to access their content.

#### **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.



## 5. 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.

**(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 accomplish the relevant task. Where possible, use the out-of-process picker or a share sheet rather than requesting full access to protected resources like Photos or Contacts.

**(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 log-in. 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 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.

(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, 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.

### 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). 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.

(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.

### 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, MovementDisorder APIs, 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.

#### 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 on 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, false, or copycat representations, names, or metadata in your app bundle or developer name. Apps should be submitted by the person or legal entity that owns or has licensed the intellectual property and other relevant rights.

**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.

### **5.3 Gaming, Gambling, and Lotteries**

Gambling, gaming, and lotteries can be tricky to manage and tend to be one of the most regulated offerings on the App Store. Only include this functionality if you've fully vetted your legal obligations everywhere you make your app available and are prepared for extra time during the review process. Some things to keep in mind:

**5.3.1 Sweepstakes and contests** must be sponsored by the developer of the app.

**5.3.2 Official rules** for sweepstakes, contests, and raffles must be presented in the app and make clear that Apple is not a sponsor or involved in the activity in any manner.

**5.3.3 Apps** may not use in-app purchase to purchase credit or currency for use in conjunction with real money gaming of any kind, and may not enable people to purchase lottery or raffle tickets or initiate fund transfers in the app.

**5.3.4 Apps** that offer real money gaming (e.g. sports betting, poker, casino games, horse racing) or lotteries must have necessary licensing and permissions in the locations where the App is used, must be geo-restricted to those locations, and must be free on the App Store. Illegal gambling aids, including card counters, are not permitted on the App Store. Lottery apps must have consideration, chance, and a prize.

### **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. 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.

### **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 (such as business organizations, 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.

### **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.

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.

### 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.

---

## After You Submit

Once you've submitted your app and metadata in App Store Connect and you're in the review process, here are some things to keep in mind:

- **Timing:** App Review will examine your app as soon as we can. However, if your app is complex or presents new issues, it may require greater scrutiny and consideration. And remember that if your app is repeatedly rejected for the same guideline violation or you've attempted to manipulate the App Review process, review of your app will take longer to complete. Learn more about App Review.
- **Status Updates:** The current status of your app will be reflected in App Store Connect, so you can keep an eye on things from there.
- **Expedite Requests:** If you have a critical timing issue, you can request an expedited review. Please respect your fellow developers by seeking expedited review only when you truly need it. If we find you're abusing this system, we may reject your requests going forward.
- **Release Date:** If your release date is set for the future, the app will not appear on the App Store until that date, even if it is approved by App Review. And remember that it can take up to 24-hours for your app to appear on all selected storefronts.
- **Rejections:** Our goal is to apply these guidelines fairly and consistently, but nobody's perfect. If your app has been rejected and you have questions or would like to provide additional information, please use the Resolution Center to communicate directly with the App Review team. This may help get your app on the store, and it can help us improve the App Review process or identify a need for clarity in our policies. If you still disagree with the outcome, or would like to suggest a change to the guideline itself, please submit an appeal.
- **Bug Fix Submissions:** For apps that are already on the App Store, bug fixes will no longer be delayed over guideline violations except for those related to legal issues. If your app has been rejected, and qualifies for this process, please use the Resolution Center to communicate directly with the App Review team indicating that you would like to take advantage of this process and plan to address the issue in your next submission.

We're excited to see what you come up with next!

Last Updated: 11 Sep 2020

# **Exhibit G**



# Google Play Developer Distribution Agreement

Effective as of June 12, 2020 ([view archived version](#))

## 1. Definitions

**Authorized Provider:** An entity authorized to receive a distribution fee for Products that are sold to users of Devices.

**Brand Features:** The trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as owned (or licensed) by such party from time to time.

**Developer or You:** Any person or company who provides Products for distribution through Google Play in accordance with the terms of this Agreement.

**Developer Account:** A publishing account issued to a Developer in connection with the distribution of Developer Products via Google Play.

**Device:** Any device that can access Google Play.

**Google:** Google LLC, a Delaware limited liability company with principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States; Google Ireland Limited, a company incorporated in Ireland with principal place of business at Gordon House, Barrow Street, Dublin 4, Ireland; Google Commerce Limited, a company incorporated in Ireland with principal place of business at Gordon House, Barrow Street, Dublin 4, Ireland; or Google Asia Pacific Pte. Limited, a company incorporated in Singapore with principal place of business at 70 Pasir Panjang Road, #03-71, Mapletree Business City, Singapore 117371. Google may update the Google entities and their addresses from time to time.

**Google Play:** The software and services, including the Play Console, which allow Developers to distribute Products to users of Devices.

**Intellectual Property Rights:** All patent rights, copyrights, trademark rights, rights in trade secrets, database rights, moral rights, and any other intellectual property rights (registered or unregistered)

throughout the world.

**Payment Account:** A financial account issued by a Payment Processor to a Developer that authorizes the Payment Processor to collect and remit payments on the Developer's behalf for Products sold via Google Play.

**Payment Processor(s):** The entity authorized by Google to provide services that enable Developers with Payment Accounts to be paid for Products distributed via Google Play.

**Play Console:** The Google Play Console and other online tools or services provided by Google to developers at <https://play.google.com/apps/publish>, as may be updated from time to time. The Play Console is also available through an app to developers.

**Products:** Software, content, digital materials, and other items and services as made available by Developers via the Play Console.

**Tax:** Any Federal, state, or local sales, use, value added, goods and services, or other similar transaction taxes. This term excludes telecommunication taxes and similar tax types, property taxes, and taxes based on Your income, including, Withholding Taxes, income, franchise, business and occupation, and other similar tax types.

## 2. Accepting this Agreement

2.1 This agreement ("**Agreement**") forms a legally binding contract between You and Google in relation to Your use of Google Play to distribute Products. You are contracting with the applicable Google entity based on where You have selected to distribute Your Product (as set forth [here](#)). You acknowledge that Google will, solely at Your direction, and acting pursuant to the relationship identified in Section 3.1, display and make Your Products available for viewing, download, and purchase by users. In order to use Google Play to distribute Products, You accept this Agreement and will provide and maintain complete and accurate information in the Play Console.

2.2 Google will not permit the distribution of Your Products through Google Play, and You may not accept the Agreement, unless You are verified as a Developer in good standing.

2.3 If You are agreeing to be bound by this Agreement on behalf of Your employer or other entity, You represent and warrant that You have full legal authority to bind Your employer or such entity to this Agreement. If You do not have the requisite authority, You may not accept the Agreement or use Google Play on behalf of Your employer or other entity.

## 3. Commercial Relationship, Pricing, Payments, and Taxes

3.1 You hereby appoint Google as Your agent or marketplace service provider as outlined here to make Your Products available in Google Play.

3.2 This Agreement covers both Products that users can access for free and Products that users pay a fee to access. In order for You to charge a fee for Your Products and to be paid for Products distributed via Google Play, You must have a valid Payment Account under a separate agreement with a Payment Processor, be approved by a Payment Processor for a Payment Account, and maintain that account in good standing. If there is a conflict between Your Payment Processor agreement and this Agreement, the terms of this Agreement will apply.

3.3 Products are displayed to users at prices You establish in Your sole discretion. If Google believes that Taxes may be owed by You or Google on the sale of Products, You grant Google permission to include any such Taxes in the price charged to users. You may set the price for Your Products in the currencies permitted by the Payment Processor. Google may display the price of Products to users in their native currency, but Google is not responsible to You for the accuracy of currency rates or currency conversion.

3.4 Acting as Your agent, and with You acting as a principal, Google is the merchant of record for Products sold or made available to users in the European Economic Area (EEA) and in the United Kingdom. You are the merchant of record for Products You sell or make available via Google Play to all other users. The price You set for Products will determine the amount of payment You will receive. A "**Service Fee**", as set forth here and as may be revised by Google from time to time with notice to Developer as described in Section 15, will be charged on the sales price and apportioned to the Payment Processor and, if one exists, the Authorized Provider.

3.5 In certain countries/territories as described here, Google will determine if a Product is taxable and if so, the applicable Tax rate will be collected either by Google, the Payment Processor, or the Authorized Provider, and remitted to the appropriate taxing authority for Products sold to users. Google may update the countries/territories where it will determine and remit the Taxes with notice to You. In all other countries/territories, You are responsible for determining if a Product is taxable, the applicable rate of Tax to be collected, and for remitting the Taxes to the appropriate taxing authority. All Taxes will be deducted from the sales price of Products sold and the remainder (sales price less Service Fee and Taxes, if any) will be remitted to You. Where Google collects and remits Taxes in applicable countries/territories, You and Google will recognize a supply from You to Google for Tax purposes, and You will comply with the relevant Tax obligations arising from this additional supply.

3.6 Where either the Payment Processor, or the Authorized Provider notifies Google that it is required by applicable (local) legislation or by the applicable governmental tax authority to withhold any taxes, or where Google is required by applicable (local) legislation or by the applicable governmental tax authority to withhold any taxes (in each case, "**Withholding Taxes**"), Google will also deduct an amount equal to such Withholding Taxes from the amount Google remits to You.

Withholding Taxes include, but are not limited to, withholding tax obligations on cross-border payments or imposed by telecommunications taxes.

3.7 You may also choose to make Products available for free. If the Product is free, You will not be charged a Service Fee. To avoid unexpected fees for users, You agree that Products that were initially offered free of charge to users will remain free of charge. Any additional charges will correlate with an alternative or supplemental version of the Product.

3.8 You authorize Google to give users refunds in accordance with the Google Play refund policies as located [here](#) or the local versions made available to You, and You agree that Google may deduct the amount of those refunds from payments to You. In all other respects, the Payment Processor's standard terms and conditions regarding refunds will apply. User refunds may be exclusive of taxes previously charged to users for Product purchases.

3.9 Users are allowed unlimited reinstalls of each Product distributed via Google Play without any additional fee, provided however, that if You remove any Product from Google Play due to a Legal Takedown (as defined in Section 8.2), that Product will be removed from all portions of Google Play, and users will no longer have a right or ability to reinstall the affected Product.

## 4. Use of Google Play by You

4.1 You and Your Product(s) must adhere to the [Developer Program Policies](#).

4.2 You are responsible for uploading Your Products to Google Play, providing required Product information and support to users, and accurately disclosing the permissions necessary for the Product to function on user Devices.

4.3 You are responsible for maintaining the confidentiality of any developer credentials that Google may issue to You or that You may choose Yourself, and You are solely responsible for all Products that are developed under Your developer credentials. Google may limit the number of Developer Accounts issued to You or to the company or organization You work for.

4.4 Except for the license rights granted by You in this Agreement, Google agrees that it obtains no right, title, or interest from You (or Your licensors) under this Agreement in or to any of Your Products, including any Intellectual Property Rights in those Products.

4.5 You may not use Google Play to distribute or make available any Product that has a purpose that facilitates the distribution of software applications and games for use on Android devices outside of Google Play.

4.6 You agree to use Google Play only for purposes that are permitted by this Agreement and any applicable law, regulation, or generally accepted practices or guidelines in the relevant jurisdictions



(including any laws regarding the export of data or software to and from the United States or other relevant countries).

4.7 Users are instructed to contact You concerning any defects or performance issues in Your Products. As between You and Google, You will be solely responsible, and Google will have no responsibility, for undertaking or handling the support and maintenance of Your Products and any complaints about Your Products. You agree to supply and maintain valid and accurate contact information that will be displayed in each of Your Products' detail page and made available to users for customer support and legal purposes. For Your paid Products or in-app transactions, You agree to respond to customer support inquiries within 3 business days, and within 24 hours to any support or Product concerns stated to be urgent by Google.

4.8 You agree that if You make Your Products available through Google Play, You will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and You agree to provide legally adequate privacy notice and protection for those users. Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so. If Your Product stores personal or sensitive information provided by users, You agree to do so securely and only for as long as it is needed. However, if the user has opted into a separate agreement with You that allows You or Your Product to store or use personal or sensitive information directly related to Your Product (not including other products or applications), then the terms of that separate agreement will govern Your use of such information. If the user provides Your Product with Google Account information, Your Product may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given You permission to do so.

4.9 You will not engage in any activity with Google Play, including making Your Products available via Google Play, that interferes with, disrupts, damages, or accesses in an unauthorized manner the devices, servers, networks, or other properties or services of any third party including, but not limited to, Google or any Authorized Provider. You may not use user information obtained via Google Play to sell or distribute Products outside of Google Play.

4.10 You are solely responsible for, and Google has no responsibility to You for, Your Products, including use of any Google Play APIs and for the consequences of Your actions, including any loss or damage which Google may suffer.

4.11 Google Play allows users to rate and review Products. Only users who download the applicable Product will be able to rate and review it on Google Play. For new Developers without Product history, Google may use or publish performance measurements such as uninstall and/or refund rates to identify or remove Products that are not meeting acceptable standards, as determined by Google. Google reserves the right to display Products to users in a manner that will be determined at Google's sole discretion. Your Products may be subject to user ratings and

reviews to which You may not agree. If you have concerns regarding such ratings and reviews, you may report it via the Play Console.

## 5. Authorizations

5.1 In furtherance of Google's appointment (as set forth [here](#)), You authorize Google on a non-exclusive, worldwide, and royalty-free basis to: reproduce, perform, display, analyze, and use Your Products in connection with (a) the operation and marketing of Google Play; (b) the marketing of devices and services that support the use of the Products and the marketing of the Products on Google Play and Devices; (c) the provision of hosting services to You and on Your behalf to allow for the storage of and user access to the Products and to enable third-party hosting of such Products; (d) making improvements to Google Play, Play Console, and Android platform; and (e) checking for compliance with this Agreement and the Developer Program Policies. The authorization in clause (e) is sublicensable to application security partners. You also authorize such application security partners to use the results of their review in their products and research that may be publicly available.

5.2 You authorize Google to perform the acts described in this section subject to Your control and direction in the manner indicated in the Play Console.

5.3 You grant to the user a nonexclusive, worldwide, and perpetual license to perform, display, and use the Product. The user may include, but is not limited to, a family group and family members whose accounts are joined together for the purpose of creating a family group. Family groups on Google Play will be subject to reasonable limits designed to prevent abuse of family sharing features. Users in a family group may purchase a single copy of the Product (unless otherwise prohibited, as for in-app and subscription Products) and share it with other family members in their family group. If, in the Play Console, You opt in to allowing users to share previously purchased Products, Your authorization of sharing of those purchases by those users is subject to this Agreement. If You choose, You may include a separate end user license agreement ("**EULA**") in Your Product that will govern the user's rights to the Product, but, to the extent that EULA conflicts with this Agreement, this Agreement will supersede the EULA. You acknowledge that the EULA for each of the Products is solely between You and the user. Google will not be responsible for, and will not have any liability whatsoever under, any EULA.

## 6. Brand Features and Publicity

6.1 Each party will own all right, title, and interest, including, without limitation, all Intellectual Property Rights, relating to its Brand Features. Except to the limited extent expressly provided in this Agreement, neither party grants, nor will the other party acquire, any right, title, or interest (including, without limitation, any implied license) in or to any Brand Features of the other party.



6.2 Subject to the terms and conditions of this Agreement, Developer grants to Google and its affiliates a limited, nonexclusive, royalty-free license during the term of this Agreement to display Developer Brand Features, submitted by Developer to Google, for use solely within Google Play, online or on Devices and in each case solely in connection with the distribution and sale of Developer's Product via Google Play or to otherwise fulfill its obligations under this Agreement.

6.3 In addition to the license granted in Section 6.2 above, for purposes of marketing the presence, distribution, and sale of Your Product via Google Play and its availability for use on devices and through other Google services, Google and its affiliates may include visual elements from Your Product (including characters and videos of game play) and Developer Brand Features (a) within Google Play, on Devices, and in any Google-owned online or mobile properties; (b) in online, mobile, television, out of home (e.g. billboard), and print advertising formats outside Google Play; (c) when making announcements of the availability of the Product; (d) in presentations; and (e) in customer lists which appear either online or on mobile devices (which includes, without limitation, customer lists posted on Google websites).

6.4 Google grants to Developer a limited, nonexclusive, worldwide, royalty-free license to use the Android Brand Features for the term of this Agreement solely for marketing purposes and only in accordance with the Android Brand Guidelines.

6.5 If Developer discontinues the distribution of specific Products via Google Play, Google will cease use of the discontinued Products' Brand Features pursuant to this Section 6, except as necessary to allow Google to effectuate reinstalls by users.

## 7. Promotional Activities

7.1 Google may run promotional activities offering coupons, credits, and/or other promotional incentives for paid transactions and/or user actions for Your Products and in-app transactions solely in connection with Google Play promotions and, for gift card promotions, also on Google authorized third-party channels ("**Promotion(s)**"), provided that (a) amounts payable to You will not be impacted; (b) there will be clear communication to users that the Promotion is from Google and not You; (c) the prices You establish will be clearly communicated to users; (d) any redemption of the Promotion will be fulfilled by Google or, for gift card Promotions, through a Google authorized third party; and (e) Google will be responsible for compliance with applicable law for the Promotion.

7.2 In addition to the rights granted in Section 6, You grant Google the right to use Your Brand Features (in the form and manner provided by You) for purposes of marketing Promotions in connection with Google Play and, for gift card Promotions, on Google authorized third-party channels; provided however, that Google will only use Brand Features owned by You on authorized third-party channels.

## 8. Product Takedowns

8.1 You may remove Your Products from future distribution via Google Play at any time, but You agree to comply with this Agreement and the Payment Processor's Payment Account terms of service for any Products distributed via Google Play prior to removal, including, but not limited to, refund requirements. Removing Your Products from future distribution via Google Play does not (a) affect the rights of users who have previously purchased or downloaded Your Products; (b) remove Your Products from Devices or from any part of Google Play where previously purchased or downloaded applications are stored on behalf of users; or (c) change Your obligation to deliver or support Products or services that have been previously purchased or downloaded by users.

8.2 Notwithstanding Section 8.1, in no event will Google maintain on any portion of Google Play (including, without limitation, the part of Google Play where previously purchased or downloaded applications are stored on behalf of users) any Product that You have removed from Google Play and provided written notice to Google that such removal was due to (a) an allegation of infringement, or actual infringement, of any third party Intellectual Property Right; (b) an allegation of, or actual violation of, third party rights; or (c) an allegation or determination that such Product does not comply with applicable law (collectively "**Legal Takedowns**"). If a Product is removed from Google Play due to a Legal Takedown and an end user purchased such Product within a year (or a longer period as local consumer law mandates) before the date of takedown, at Google's request, You agree to refund to the end user all amounts paid by such end user for such Product.

8.3 Google does not undertake an obligation to monitor the Products or their content. If Google becomes aware and determines in its sole discretion that a Product or any portion thereof (a) violates any applicable law; (b) violates this Agreement, applicable policies, or other terms of service, as may be updated by Google from time to time; (c) violates terms of distribution agreements with device manufacturers and Authorized Providers; or (d) creates potential liability for, or may have an adverse impact on, Google or Authorized Providers (for example, if a Product has an adverse economic, reputational or security-related impact); then Google may reject, remove, suspend, limit the visibility of a Product on Google Play, or reclassify the Product from Google Play or from Devices. Google reserves the right to suspend and/or bar any Product and/or Developer from Google Play or from Devices as described in this Section. If Your Product contains elements that could cause serious harm to user devices or data, Google reserves the right to disable the Product or remove it from Devices on which it has been installed. If Your Product is rejected, removed, or suspended from Google Play or from Devices pursuant to this Section 8.3, then Google may withhold payments due to Developer.

8.4 Google enters into distribution agreements with device manufacturers and Authorized Providers to place the Google Play software client application(s) on Devices. These distribution agreements may require the involuntary removal of Products in violation of the Device manufacturer's or Authorized Provider's terms of service.

## 9. Privacy and Information

9.1 Any data collected or used pursuant to this Agreement is in accordance with Google's [Privacy Policy](#).

9.2 In order to continually innovate and improve Google Play, related products and services, and the user and Developer experience across Google products and services, Google may collect certain usage statistics from Google Play and Devices including, but not limited to, information on how the Product, Google Play, and Devices are being used.

9.3 The data collected is used in the aggregate to improve Google Play, related products and services, and the user and Developer experience across Google products and services. Developers have access to certain data collected by Google via the Play Console.

## 10. Terminating this Agreement

10.1 This Agreement will continue to apply until terminated, subject to the terms that survive pursuant to Section 16.9, by either You or Google as set forth below.

10.2 If You want to terminate this Agreement, You will unpublish all of Your Products and cease Your use of the Play Console and any relevant developer credentials.

10.3 Google may terminate this Agreement with You immediately upon written notice or with thirty (30) days prior written notice if required under applicable law if (a) You have breached any provision of this Agreement, any non-disclosure agreement, or other agreement relating to Google Play or the Android platform; (b) Google is required to do so by law; (c) You cease being an authorized developer, a developer in good standing, or are barred from using Android software; (d) Google decides to no longer provide Google Play; or (e) You or Your Product pose a potential risk for economic, reputational, or security-related harm to Google, users, or other third-party partners. Where allowed under applicable law, Google may also terminate this Agreement with You for any reason with thirty (30) days prior written notice. If Google terminates this Agreement, You will no longer have access to the Play Console. More information on account termination is located [here](#).

10.4 After termination of this Agreement, Google will not distribute Your Product, but may retain and use copies of the Product for support of Google Play and the Android platform.

## 11. Representations and Warranties

11.1 You represent and warrant that You have all Intellectual Property Rights in and to Your Product(s).

11.2 If You use third-party materials, You represent and warrant that You have the right to distribute the third-party material in the Product. You agree that You will not submit material to Google Play that is subject to third -party Intellectual Property Rights unless You are the owner of such rights or have permission from their rightful owner to submit the material.

11.3 You represent and warrant that, as the principal to the transaction with the user, You are solely responsible for compliance worldwide with all applicable laws and other obligations.

## **12. DISCLAIMER OF WARRANTIES**

12.1 TO THE MAXIMUM EXTENT PERMITTED BY LAW, YOU UNDERSTAND AND EXPRESSLY AGREE THAT YOUR USE OF THE PLAY CONSOLE AND GOOGLE PLAY IS AT YOUR SOLE RISK AND THAT THE PLAY CONSOLE AND GOOGLE PLAY ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTY OF ANY KIND.

12.2 YOUR USE OF THE PLAY CONSOLE AND GOOGLE PLAY AND ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE PLAY CONSOLE AND GOOGLE PLAY IS AT YOUR OWN DISCRETION AND RISK AND YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM SUCH USE.

12.3 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

## **13. LIMITATION OF LIABILITY**

TO THE MAXIMUM EXTENT PERMITTED BY LAW, YOU UNDERSTAND AND EXPRESSLY AGREE THAT GOOGLE, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS WILL NOT BE LIABLE TO YOU UNDER ANY THEORY OF LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES THAT MAY BE INCURRED BY YOU, INCLUDING ANY LOSS OF DATA, WHETHER OR NOT GOOGLE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

## **14. Indemnification**

14.1 To the maximum extent permitted by law, You agree to defend, indemnify, and hold harmless Google, its affiliates, and their respective directors, officers, employees and agents, and Authorized Providers from and against any and all third party claims, actions, suits, or proceedings, as well as

any and all losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or accruing from (a) Your use of the Play Console and Google Play in violation of this Agreement; (b) infringement or violation by Your Product(s) of any Intellectual Property Right or any other right of any person; or (c) You or Your Product(s)' violation of any law.

14.2 To the maximum extent permitted by law, You agree to defend, indemnify, and hold harmless the applicable Payment Processors (which may include Google and/or third parties) and the Payment Processors' affiliates, directors, officers, employees, and agents from and against any and all third party claims, actions, suits, or proceedings, as well as any and all losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or accruing from Your distribution of Products via Google Play.

## 15. Changes to the Agreement

15.1 Google may make changes to this Agreement at any time with notice to Developer and the opportunity to decline further use of Google Play. You should look at the Agreement and check for notice of any changes regularly.

15.2 Changes will not be retroactive. They will become effective, and will be deemed accepted by Developer, (a) immediately for those who become Developers after the notification is posted; or (b) for pre-existing Developers, on the date specified in the notice, which will be no sooner than 30 days after the changes are posted (except changes required by law which will be effective immediately).

15.3 If You do not agree with the modifications to the Agreement, You may terminate Your use of Google Play, which will be Your sole and exclusive remedy. You agree that Your continued use of Google Play constitutes Your agreement to the modified terms of this Agreement.

## 16. General Legal Terms

16.1 This Agreement, including any addenda You may have agreed to separately, constitutes the entire legal agreement between You and Google and governs Your use of Google Play and completely replaces any prior agreements between You and Google in relation to Google Play. The English language version of this Agreement will control and translations, if any, are non-binding and for reference only.

16.2 You agree that if Google does not exercise or enforce any legal right or remedy contained in this Agreement (or which Google has the benefit of under any applicable law), this will not be taken to be a formal waiver of Google's rights and that those rights or remedies will still be available to Google.



16.3 If any court of law having the jurisdiction to decide on this matter rules that any provision of this Agreement is invalid, then that provision will be removed from this Agreement without affecting the rest of this Agreement. The remaining provisions of this Agreement will continue to be valid and enforceable.

16.4 You acknowledge and agree that each member of the group of companies comprising Google will be a third -party beneficiary to this Agreement and that such other companies will be entitled to directly enforce, and rely upon, any provision of this Agreement that confers a benefit on (or rights in favor of) them. Other than this, no other person or company will be a third -party beneficiary to this Agreement.

16.5 PRODUCTS ON GOOGLE PLAY MAY BE SUBJECT TO UNITED STATES' AND OTHER JURISDICTIONS' EXPORT CONTROL AND SANCTIONS LAWS AND REGULATIONS. YOU AGREE TO COMPLY WITH ALL EXPORT CONTROL AND SANCTIONS LAWS AND REGULATIONS THAT APPLY TO YOUR DISTRIBUTION OR USE OF PRODUCTS, INCLUDING BUT NOT LIMITED TO (A) THE EXPORT ADMINISTRATION REGULATIONS MAINTAINED BY THE U.S. DEPARTMENT OF COMMERCE, (B) TRADE AND ECONOMIC SANCTIONS MAINTAINED BY THE U.S. TREASURY DEPARTMENT'S OFFICE OF FOREIGN ASSETS CONTROL, AND (C) THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS MAINTAINED BY THE U.S. DEPARTMENT OF STATE. THESE LAWS AND REGULATIONS INCLUDE RESTRICTIONS ON DESTINATIONS, USERS, AND END USE.

16.6 Except in the case of a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction), the rights granted in this Agreement may not be assigned or transferred by either You or Google without the prior approval of the other party. Any other attempt to assign is void.

16.7 If You experience a change of control, Google may, at its discretion, elect to immediately terminate this Agreement.

16.8 All claims arising out of or relating to this Agreement or Your relationship with Google under this Agreement will be governed by the laws of the State of California, excluding California's conflict of laws provisions. You and Google further agree to submit to the exclusive jurisdiction of the federal or state courts located within the county of Santa Clara, California to resolve any legal matter arising from or relating to this Agreement or Your relationship with Google under this Agreement, except that You agree that Google will be allowed to apply for injunctive relief in any jurisdiction. To the extent required under applicable law, You may have other ways to resolve disputes with Google as described in the Developer Program Policies. If You are accepting the Agreement on behalf of a United States government entity or a United States city, county, or state government entity, then the following applies instead of the foregoing: the parties agree to remain silent regarding governing law and venue.

16.9 Sections 1 (Definitions), 6.5, 10.4, 11 (Representations and Warranties), 12 (Disclaimer of Warranties), 13 (Limitation of Liability), 14 (Indemnification), and 16 (General Legal Terms) will survive any expiration or termination of this Agreement.

---

[© Google](#) · [Privacy & Terms](#) · [Help](#)

Change language or region: United States - English ▼



# Exhibit H

## Developer Program Policy (effective August 12, 2020)

### Let's build the world's most trusted source for apps and games

Your innovation is what drives our shared success, but with it comes responsibility. These Developer Program Policies, along with the [Developer Distribution Agreement](#), ensure that together we continue to deliver the world's most innovative and trusted apps to over a billion people through Google Play. We invite you to explore our policies below.

### Restricted Content

People from all over the world use Google Play to access apps and games every day. Before submitting an app, ask yourself if your app is appropriate for Google Play and compliant with local laws.

### Child Endangerment

Apps that include content that sexualizes minors are subject to immediate removal from the Store, including but not limited to, apps that promote pedophilia or inappropriate interaction targeted at a minor (e.g. groping or caressing).

In addition, apps that appeal to children but contain adult themes are not allowed, including but not limited to, apps with excessive violence, blood, and gore; apps that depict or encourage harmful and dangerous activities. We also don't allow apps that promote negative body or self image including apps that depict for entertainment purposes plastic surgery, weight loss, and other cosmetic adjustments to a person's physical appearance.

If we become aware of content with child sexual abuse imagery, we will report it to the appropriate authorities and delete the Google Accounts of those involved with the distribution.

### Inappropriate Content

To ensure that Google Play remains a safe and respectful platform, we've created standards defining and prohibiting content that is harmful or inappropriate for our users.

### Sexual Content and Profanity

We don't allow apps that contain or promote sexual content or profanity, including pornography, or any content or services intended to be sexually gratifying. Content that contains nudity may be allowed if the primary purpose is educational, documentary, scientific, or artistic, and is not gratuitous.

Here are some examples of common violations:

- Depictions of sexual nudity, or sexually suggestive poses in which the subject is nude, blurred or minimally clothed, and/or where the clothing would not be acceptable in an appropriate public context.
- Depictions, animations or illustrations of sex acts, sexually suggestive poses or the sexual depiction of body parts.
- Content that depicts or are functionally sexual aids, sex guides, illegal sexual themes and fetishes.
- Content that is lewd or profane - including but not limited to content which may contain profanity, slurs, explicit text, adult/sexual keywords in the store listing or in-app.
- Content that depicts, describes, or encourages bestiality.
- Apps that promote sex-related entertainment, escort services, or other services that may be interpreted as providing sexual acts in exchange for compensation.
- Apps that degrade or objectify people.

### Hate Speech

We don't allow apps that promote violence, or incite hatred against individuals or groups based on race or ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender, gender identity, or any other characteristic that is associated with systemic discrimination or marginalization.

Apps which contain EDSA (Educational, Documentary, Scientific, or Artistic) content related to Nazis may be blocked in certain countries, in accordance with local laws and regulations.

Here are examples of common violations:

- Content or speech asserting that a protected group is inhuman, inferior or worthy of being hated.
- Apps that contain hateful slurs, stereotypes, or theories about a protected group possessing negative characteristics (e.g. malicious, corrupt, evil, etc.), or explicitly or implicitly claims the group is a threat.
- Content or speech trying to encourage others to believe that people should be hated or discriminated against because they are a member of a protected group.
- Content which promotes hate symbols such as flags, symbols, insignias, paraphernalia or behaviors associated with hate groups.

## Violence

We don't allow apps that depict or facilitate gratuitous violence or other dangerous activities. Apps that depict fictional violence in the context of a game, such as cartoons, hunting or fishing, are generally allowed.

Here are some examples of common violations:

- Graphic depictions or descriptions of realistic violence or violent threats to any person or animal.
- Apps that promote self harm, suicide, bullying, harassment, eating disorders, choking games or other acts where serious injury or death may result.

## Terrorist Content

We do not permit terrorist organizations to publish apps on Google Play for any purpose, including recruitment.

We don't allow apps with content related to terrorism, such as content that promotes terrorist acts, incites violence, or celebrates terrorist attacks. If posting content related to terrorism for an educational, documentary, scientific, or artistic purpose, be mindful to provide enough information so users understand the context.

## Sensitive Events

We don't allow apps that lack reasonable sensitivity towards or capitalize on a natural disaster, atrocity, conflict, death, or other tragic event. Apps with content related to a sensitive event are generally allowed if that content has EDSA (Educational, Documentary, Scientific, or Artistic) value or intends to alert users to or raise awareness for the sensitive event.

Here are examples of common violations:

- Lacking sensitivity regarding the death of a real person or group of people due to suicide, overdose, natural causes, etc.
- Denying a major tragic event.
- Appearing to profit from a tragic event with no discernible benefit to the victims.

## Bullying and Harassment

We don't allow apps that contain or facilitate threats, harassment, or bullying.

Here are examples of common violations:

- Bullying victims of international or religious conflicts.
- Content that seeks to exploit others, including extortion, blackmail, etc.
- Posting content in order to humiliate someone publicly.
- Harassing victims, or their friends and families, of a tragic event.

## Dangerous Products

We don't allow apps that facilitate the sale of explosives, firearms, ammunition, or certain firearms accessories.

- Restricted accessories include those that enable a firearm to simulate automatic fire or convert a firearm to automatic fire (e.g. bump stocks, gatling triggers, drop-in auto sears, conversion kits), and magazines or belts carrying more than 30 rounds.

We don't allow apps that provide instructions for the manufacture of explosives, firearms, ammunition, restricted firearm accessories, or other weapons. This includes instructions on how to convert a firearm to automatic, or simulated automatic, firing capabilities.

## Marijuana

We don't allow apps that facilitate the sale of marijuana or marijuana products, regardless of legality.

Here are some examples of common violations:

- Allowing users to order marijuana through an in-app shopping cart feature.
- Assisting users in arranging delivery or pick up of marijuana.
- Facilitating the sale of products containing THC (Tetrahydrocannabinol), including products such as CBD oils containing THC.

## Tobacco and Alcohol

We don't allow apps that facilitate the sale of tobacco (including e-cigarettes and vape pens) or encourage the illegal or inappropriate use of alcohol or tobacco.

Here are examples of common violations:

- Depicting or encouraging the use or sale of alcohol or tobacco to minors.
- Implying that consuming tobacco can improve social, sexual, professional, intellectual, or athletic standing.
- Portraying excessive drinking favorably, including the favorable portrayal of excessive, binge or competition drinking.

## Financial Services

We don't allow apps that expose users to deceptive or harmful financial products and services.

For the purposes of this policy, we consider financial products and services to be those related to the management or investment of money and cryptocurrencies, including personalized advice.

If your app contains or promotes financial products and services, you must comply with state and local regulations for any region or country that your app targets - for example, include specific disclosures required by local law.

## Binary Options

We do not allow apps that provide users with the ability to trade binary options.

## Cryptocurrencies

We don't allow apps that mine cryptocurrency on devices. We permit apps that remotely manage the mining of cryptocurrency.

## Personal loans

We define personal loans as lending money from one individual, organization, or entity to an individual consumer on a nonrecurring basis, not for the purpose of financing purchase of a fixed asset or education. Personal loan consumers require information about the quality, features, fees, repayment schedule, risks, and benefits of loan products in order to make informed decisions about whether to undertake the loan.

- Examples: Personal loans, payday loans, peer-to-peer loans, title loans
- Not included: Mortgages, car loans, student loans, revolving lines of credit (such as credit cards, personal lines of credit)

Apps that provide personal loans, including but not limited to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders, must disclose the following information in the app metadata:

- Minimum and maximum period for repayment
- Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law
- A representative example of the total cost of the loan, including all applicable fees
- A privacy policy that comprehensively discloses the access, collection, use and sharing of personal and sensitive user data.

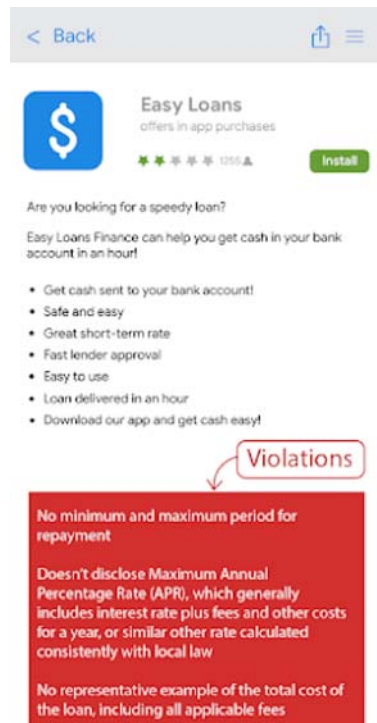
We do not allow apps that promote personal loans which require repayment in full in 60 days or less from the date the loan is issued (we refer to these as "short-term personal loans").

### High APR personal loans

In the United States, we do not allow apps for personal loans where the Annual Percentage Rate (APR) is 36% or higher. Apps for personal loans in the United States must display their maximum APR, calculated consistently with the [Truth in Lending Act \(TILA\)](#).

This policy applies to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders.

Here is an example of common violations:



## Real-Money Gambling, Games, and Contests

We allow real-money gambling apps, ads related to real-money gambling, and daily fantasy sports apps that meet certain requirements.

### Gambling Apps

(Currently permitted in the UK, Ireland, and France only)

For all other locations, we don't allow apps containing content or services that facilitate online gambling.

We allow content and services that facilitate online gambling, as long as they meet the following requirements:

- Developer must successfully [complete the application process](#) in order to distribute the app on Play;
- App must comply with all applicable laws and industry standards for each country in which it is distributed;
- Developer must have a valid gambling license for each country in which the app is distributed;
- App must prevent under-age users from gambling in the app;
- App must prevent use from countries not covered by the developer-provided gambling license;
- App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-app Billing;
- App must be free to download and install from the Store;
- App must be rated AO (Adult Only) or IARC equivalent; and
- App and its app listing must clearly display information about responsible gambling.

### Other Real-Money Games, Contests, and Tournament Apps

We don't allow content or services that enable or facilitate users' ability to wager, stake, or participate using real money (including in-app items purchased with money) to obtain a prize of real world monetary value. This includes but is not limited to, online casinos, sports betting, and lotteries that fail to meet the requirements for Gambling apps noted above, and games that offer prizes of cash or other real world value.

Here are examples of violations:

- Games that accept money in exchange for an opportunity to win a physical or monetary prize
- Games with "loyalty" (e.g. engagement or activity) points that (1) are accrued or accelerated via real-money purchases which (2) can be exchanged for items or prizes of real world monetary value

- Apps that accept or manage gambling wagers, in-app currencies required for participation, winnings, or deposits in order to obtain or accelerate eligibility for a physical or monetary prize.
- Apps that provide a “call to action” to wager, stake, or participate in real-money games, contests, or tournaments using real money, such as apps with navigational elements (menu items, tabs, buttons, etc.) that invite users to “REGISTER!” or “COMPETE!” in a tournament for a chance to win a cash prize.

## Ads for Gambling or Real-Money Games, Contests, and Tournaments within Play-distributed Apps

We allow apps that advertise gambling or real-money games, context, and tournaments if they meet the following requirements:

- App and ad (including advertisers) must comply with all applicable laws and industry standards for any location where the ad is displayed;
- Ad must meet local licensing requirements for all gambling-related products and services being promoted;
- App must not display a gambling ad to individuals known to be under the age of 18;
- App must not be enrolled in the Designed for Families program;
- App must not target individuals under the age of 18;
- If advertising a Gambling App (as defined above), ad must clearly display information about responsible gambling on its landing page, the advertised app listing itself or within the app;-
- App must not provide simulated gambling content (e.g. social casino apps; apps with virtual slot machines);
- App must not provide gambling or real-money games, lotteries or tournament support functionality (e.g. functionality that assists with wagering, payouts, sports score/odds tracking, or management of participation funds);
- You must not have an ownership interest in gambling or real-money games, lotteries or tournament services advertised within the app;
- App content must not promote or direct users to gambling or real-money games, lotteries or tournament services

Only Gambling apps (as defined above) or apps that meet all of these Gambling Ads requirements may include ads for real-money gambling or real-money games, lotteries or tournaments.

Here are some examples of violations:

- An app that’s designed for under-age users and shows an ad promoting gambling services
- A simulated casino game that promotes or directs users to real money casinos
- A dedicated sports odds tracker app containing integrated gambling ads linking to a sports betting site
- A news app that shows ads for a gambling service owned or operated by the app’s developer
- Apps that have gambling ads that violate our [Deceptive Ads](#) policy, such as ads that appear to users as buttons, icons, or other interactive in-app elements

## Daily Fantasy Sports (DFS) Apps

We only allow daily fantasy sports (DFS) apps, as defined by applicable local law, if they meet the following requirements:

- App is either 1)-only distributed in the United States or 2) eligible under the Gambling Apps requirements noted above;
- Developer must successfully complete [the DFS application](#) process and be accepted in order to distribute the app on Play;
- App must comply with all applicable laws and industry standards for the countries in which it is distributed;
- App must prevent under-age users from wagering or conducting monetary transactions within the app;
- App must NOT be purchasable as a paid app on Google Play, nor use Google Play In-app Billing;
- App must be free to download and install from the Store;
- App must be rated AO (Adult Only) or IARC equivalent; and
- App and its app listing must clearly display information about responsible gambling.

If distributed in the US, the following additional requirements apply;

- App must comply with all applicable laws and industry standards for any US state or US territory in which it is distributed;
- Developer must have a valid license for each US state or US territory in which a license is required for daily fantasy sports apps;
- App must prevent use from US States or US territories in which the developer does not hold a license required for daily fantasy sports apps; and
- App must prevent use from US States or US territories where daily fantasy sports apps are not legal.

## Illegal Activities

We don't allow apps that facilitate or promote illegal activities.

Here are some examples of common violations:

- Facilitating the sale or purchase of illegal drugs or prescription drugs without a prescription.
- Depicting or encouraging the use or sale of drugs, alcohol, or tobacco by minors.
- Instructions for growing or manufacturing illegal drugs.

## User Generated Content

User-generated content (UGC) is content that users contribute to an app, and which is visible to or accessible by at least a subset of the app's users.

Apps that contain or feature UGC must:

- require that users accept the app's terms of use and/or user policy before users can create or upload UGC;
- define objectionable content and behaviors (in a way that complies with Play's Developer Program Policies), and prohibit them in the app's terms of use or user policies;
- implement robust, effective and ongoing UGC moderation, as is reasonable and consistent with the type of UGC hosted by the app
  - In the case of live-streaming apps, objectionable UGC must be removed as close to real-time as reasonably possible;
  - In the case of augmented reality (AR) apps, UGC moderation (including the in-app reporting system) must account for both objectionable AR UGC (e.g. a sexually explicit AR image) and sensitive AR anchoring location (e.g. AR content anchored to a restricted area, such as a military base, or a private property where AR anchoring may cause issues for the property owner);
- provide a user-friendly, in-app system for reporting objectionable UGC and take action against that UGC where appropriate;
- remove or block abusive users who violate the app's terms of use and/or user policy;
- provide safeguards to prevent in-app monetization from encouraging objectionable user behavior.

Apps whose primary purpose is featuring objectionable UGC will be removed from Google Play. Similarly, apps that end up being used primarily for hosting objectionable UGC, or that develop a reputation among users of being a place where such content thrives, will also be removed from Google Play.

Here are some examples of common violations:

- Promoting sexually explicit user-generated content, including implementing or permitting paid features that principally encourage the sharing of objectionable content.
- Apps with user generated content (UGC) that lack sufficient safeguards against threats, harassment, or bullying, particularly toward minors.
- Posts, comments, or photos within an app that are primarily intended to harass or single out another person for abuse, malicious attack, or ridicule.
- Apps that continually fail to address user complaints about objectionable content.

## Unapproved Substances

Google Play doesn't allow apps that promote or sell unapproved substances, irrespective of any claims of legality.

Examples:

- All items on this non-exhaustive list of [prohibited pharmaceuticals and supplements](#)
- Products that contain ephedra
- Products containing human chorionic gonadotropin (hCG) in relation to weight loss or weight control, or when promoted in conjunction with anabolic steroids
- Herbal and dietary supplements with active pharmaceutical or dangerous ingredients
- False or misleading health claims, including claims implying that a product is as effective as prescription drugs or controlled substances
- Non-government approved products that are marketed in a way that implies that they're safe or effective for use in preventing, curing, or treating a particular disease or ailment
- Products that have been subject to any government or regulatory action or warning
- Products with names that are confusingly similar to an unapproved pharmaceutical or supplement or controlled substance



For additional information on the unapproved or misleading pharmaceuticals and supplements that we monitor, please visit [www.legitscript.com](http://www.legitscript.com).

## Intellectual Property

When developers copy someone else's work or use it without required permission, it might harm the owner of that work. Don't rely on unfair use of other people's work.

### Intellectual Property

We don't allow apps or developer accounts that infringe on the intellectual property rights of others (including trademark, copyright, patent, trade secret, and other proprietary rights). We also don't allow apps that encourage or induce infringement of intellectual property rights.

We will respond to clear notices of alleged copyright infringement. For more information or to file a DMCA request, please visit our [copyright procedures](#).

To submit a complaint regarding the sale or promotion for sale of counterfeit goods within an app, please submit a [counterfeit notice](#).

If you are a trademark owner and you believe there is an app on Google Play that infringes on your trademark rights, we encourage you to reach out to the developer directly to resolve your concern. If you are unable to reach a resolution with the developer, please submit a trademark complaint through this [form](#).

If you have written documentation proving that you have permission to use a third party's intellectual property in your app or store listing (such as brand names, logos and graphic assets), [contact the Google Play team](#) in advance of your submission to ensure that your app is not rejected for an intellectual property violation.

## Unauthorized Use of Copyrighted Content

We don't allow apps that infringe copyright. Modifying copyrighted content may still lead to a violation. Developers may be required to provide evidence of their rights to use copyrighted content.

Please be careful when using copyrighted content to demonstrate the functionality of your app. In general, the safest approach is to create something that's original.

**Here are some examples of copyrighted content that is often used without authorization or a legally valid reason:**

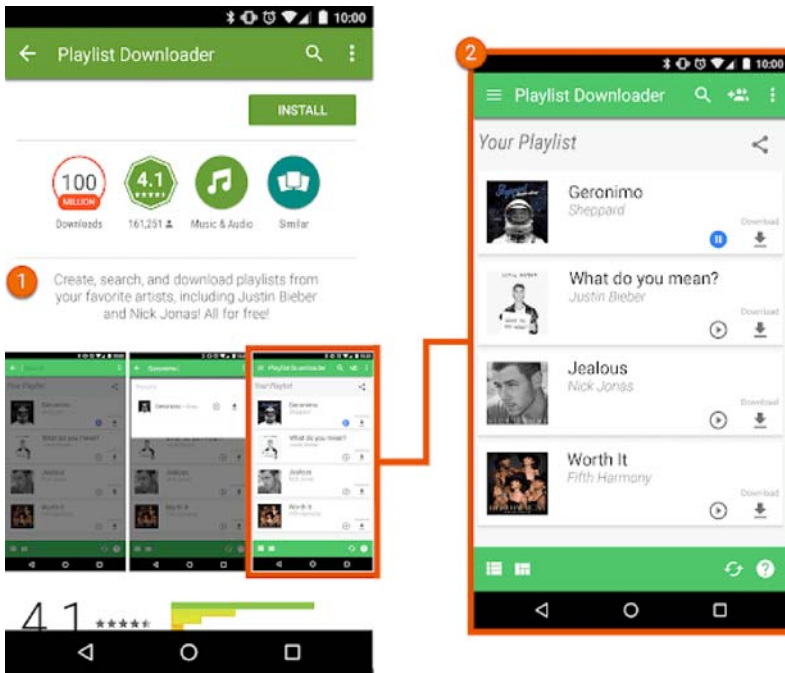
- Cover art for music albums, video games, and books.
- Marketing images from movies, television, or video games.
- Artwork or images from comic books, cartoons, movies, music videos, or television.
- College and professional sports team logos.
- Photos taken from a public figure's social media account.
- Professional images of public figures.
- Reproductions or "fan art" indistinguishable from the original work under copyright.
- Apps that have soundboards that play audio clips from copyrighted content.
- Full reproductions or translations of books that are not in the public domain.

## Encouraging Infringement of Copyright

We don't allow apps that induce or encourage copyright infringement. Before you publish your app, look for ways your app may be encouraging copyright infringement and get legal advice if necessary.

**Here are some examples of common violations:**

- Streaming apps that allow users to download a local copy of copyrighted content without authorization.
- Apps that encourage users to stream and download copyrighted works, including music and video, in violation of applicable copyright law:



- ① The description in this app listing encourages users to download copyrighted content without authorization.
- ② The screenshot in the app listing encourages users to download copyrighted content without authorization.

## Trademark Infringement

We don't allow apps that infringe on others' trademarks. A trademark is a word, symbol, or combination that identifies the source of a good or service. Once acquired, a trademark gives the owner exclusive rights to the trademark usage with respect to certain goods or services.

Trademark infringement is improper or unauthorized use of an identical or similar trademark in a way that is likely to cause confusion as to the source of that product. If your app uses another party's trademarks in a way that is likely to cause confusion, your app may be suspended.

## Counterfeit

We don't allow apps that sell or promote for sale counterfeit goods. Counterfeit goods contain a trademark or logo that is identical to or substantially indistinguishable from the trademark of another. They mimic the brand features of the product in an attempt to pass themselves off as a genuine product of the brand owner.

## Privacy, Deception and Device Abuse

We're committed to protecting user privacy and providing a safe and secure environment for our users. Apps that are deceptive, malicious, or intended to abuse or misuse any network, device, or personal data are strictly prohibited.

## User Data

You must be transparent in how you handle user data (e.g., information collected from or about a user, including device information). That means disclosing your app's access, collection, use, and sharing of the data, and limiting the use of the data to the purposes disclosed. In addition, if your app handles personal or sensitive user data, please also refer to the additional requirements in the "Personal and Sensitive Information" section below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

## Personal and Sensitive Information

Personal and sensitive user data includes, but isn't limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts, [device location](#), SMS and call - related data, microphone, camera, and other sensitive device or usage data. If your app handles sensitive user data, then you must:

- Limit your access, collection, use, and sharing of personal or sensitive data acquired through the app to purposes directly related to providing and improving the features of the app (e.g., user anticipated functionality that is documented and promoted in the app's description in the Play Store). Apps that extend usage of this data for serving advertising must be in compliance with our [Ads Policy](#).

- Post a privacy policy in both the designated field in the Play Console and within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app accesses, collects, uses, and shares user data. Your privacy policy must disclose the types of personal and sensitive data your app accesses, collects, uses, and shares and the types of parties with which any personal or sensitive user data is shared.
- Handle all personal or sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).
- Use a runtime permissions request whenever available, prior to accessing data gated by [Android permissions](#).
- Not sell personal or sensitive user data.

### Prominent Disclosure and Consent Requirement

In cases where users may not reasonably expect that their personal or sensitive user data will be required to provide or improve the policy compliant features or functionality within your app (e.g., data collection occurs in the background of your app), you must meet the following requirements:

**You must provide an in-app disclosure of your data access, collection, use, and sharing. The in-app disclosure:**

- Must be within the app itself, not only in the app description or on a website;
- Must be displayed in the normal usage of the app and not require the user to navigate into a menu or settings;
- Must describe the data being accessed or collected;
- Must explain how the data will be used and/or shared;
- **Cannot** only be placed in a privacy policy or terms of service; and
- **Cannot** be included with other disclosures unrelated to personal or sensitive data collection.

**Your in-app disclosure must accompany and immediately precede a request for user consent and, where available, an associated runtime permission. You may not access or collect any personal or sensitive data until the user consents.**

**The app's request for consent:**

- Must present the consent dialog clearly and unambiguously;
- Must require affirmative user action (e.g. tap to accept, tick a check-box);
- **Must not** interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent; and
- **Must not** use auto-dismissing or expiring messages as a means of obtaining user consent.

**Here are some examples of common violations:**

- An app that accesses a user's inventory of installed apps and doesn't treat this data as personal or sensitive data subject to the above Privacy Policy, data handling, and Prominent Disclosure and Consent requirements.
- An app that accesses a user's phone or contact book data and doesn't treat this data as personal or sensitive data subject to the above Privacy Policy, data handling, and Prominent Disclosure and Consent requirements.
- An app that records a user's screen and doesn't treat this data as personal or sensitive data subject to this policy.
- An app that collects [device location](#) and does not comprehensively disclose its use and obtain consent in accordance with the above requirements
- An app that collects restricted permissions in the background of the app including for tracking, research, or marketing purposes and does not comprehensively disclose its use and obtain consent in accordance with the above requirements.

### Specific Restrictions for Sensitive Data Access

In addition to the requirements above, the table below describes requirements for specific activities.

Activity	Requirement
Your app handles financial or payment information or government identification numbers	Your app must never publicly disclose any personal or sensitive user data related to financial or payment activities or any government identification numbers.
Your app handles non-public phonebook or contact information	We don't allow unauthorized publishing or disclosure of people's non-public contacts.
Your app contains anti-virus or security functionality, such as anti-virus, anti-malware, or security-related features	Your app must post a privacy policy that, together with any in-app disclosures, explain what user data your app collects and transmits, how it's used, and the type of parties with whom it's shared.

## EU-U.S. Privacy Shield

### Privacy Shield

If you access, use, or process personal information made available by Google that directly or indirectly identifies an individual and that originated in the European Union or Switzerland ("EU Personal Information"), then you must:

- comply with all applicable privacy, data security, and data protection laws, directives, regulations, and rules;
- access, use or process EU Personal Information only for purposes that are consistent with the consent obtained from the individual to whom the EU Personal Information relates;
- implement appropriate organizational and technical measures to protect EU Personal Information against loss, misuse, and unauthorized or unlawful access, disclosure, alteration and destruction; and
- provide the same level of protection as is required by the [Privacy Shield Principles](#).

You must monitor your compliance with these conditions on a regular basis. If, at any time, you cannot meet these conditions (or if there is a significant risk that you will not be able to meet them), you must immediately notify us by email to [data-protection-office@google.com](mailto:data-protection-office@google.com) and immediately either stop processing EU Personal Information or take reasonable and appropriate steps to restore an adequate level of protection.

## Permissions

Permission requests should make sense to users. You may only request permissions that are necessary to implement current features or services in your app that are promoted in your Play Store listing. You may not use permissions that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes. Personal or sensitive data accessed through permissions may never be sold.

Request permissions to access data in context (via incremental auth), so that users understand why your app is requesting the permission. Use the data only for purposes that the user has consented to. If you later wish to use the data for other purposes, you must ask users and make sure they affirmatively agree to the additional uses.

### Restricted Permissions

In addition to the above, restricted permissions are permissions that are designated as [Dangerous](#), [Special](#), or [Signature](#), and are subject to the following additional requirements and restrictions:

- Sensitive user or device data accessed through Restricted Permissions may only be transferred to third parties if necessary to provide or improve current features or services in the app from which the data was collected. You may also transfer data as necessary to comply with applicable law or as part of a merger, acquisition, or sale of assets with legally adequate notice to users. All other transfers or sales of the user data are prohibited.
- Respect users' decisions if they decline a request for a Restricted Permission, and users may not be manipulated or forced into consenting to any non-critical permission. You must make a reasonable effort to accommodate users who do not grant access to sensitive permissions (e.g., allowing a user to manually enter a phone number if they've restricted access to Call Logs).

Certain Restricted Permissions may be subject to additional requirements as detailed below. The objective of these restrictions is to safeguard user privacy. We may make limited exceptions to the requirements below in very rare cases where apps provide a highly compelling or critical feature and where there is no alternative method available to provide the feature. We evaluate proposed exceptions against the potential privacy or security impacts on users.

### SMS and Call Log Permissions

SMS and Call Log Permissions are regarded as personal and sensitive user data subject to the [Personal and Sensitive Information](#) policy, and the following restrictions:

Restricted Permission	Requirement
Your app manifest requests the Call Log permission group (e.g. <code>READ_CALL_LOG</code> , <code>WRITE_CALL_LOG</code> , <code>PROCESS_OUTGOING_CALLS</code> )	It must be actively registered as the default Phone or Assistant handler on the device.
Your app manifest requests the SMS permission group (e.g. <code>READ_SMS</code> , <code>SEND_SMS</code> , <code>WRITE_SMS</code> , <code>RECEIVE_SMS</code> , <code>RECEIVE_WAP_PUSH</code> , <code>RECEIVE_MMS</code> )	It must be actively registered as the default SMS or Assistant handler on the device.

Apps lacking default SMS, Phone, or Assistant handler capability may not declare use of the above permissions in the manifest. This includes placeholder text in the manifest. Additionally, apps must be actively registered as the default SMS, Phone, or Assistant handler before prompting users to accept any of the above permissions and must immediately stop using the permission when they're no longer the default handler. The permitted uses and exceptions are available on [this Help Center page](#).

Apps may only use the permission (and any data derived from the permission) to provide approved core app functionality. Core functionality is defined as the main purpose of the app. This may include a set of core features, which must all be prominently documented and promoted in the app's description. Without the core feature, the app is "broken" or rendered unusable. The transfer, sharing, or licensed use of this data must only be for providing core features or services within the app, and its use may not be extended for any other purpose (e.g., improving other apps or services, advertising, or marketing purposes). You may not use alternative methods (including other permissions, APIs, or third-party sources) to derive data attributed to Call Log or SMS related permissions.

## Location Permissions

[Device location](#) is regarded as personal and sensitive user data subject to the [Personal and Sensitive Information](#) policy and the following requirements:

- Apps may not access data protected by location permissions (e.g., `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`) after it is no longer necessary to deliver current features or services in your app.
- You should never request location permissions from users for the sole purpose of advertising or analytics. Apps that extend permitted usage of this data for serving advertising must be in compliance with our [Ads Policy](#).
- Apps should request the minimum scope necessary (i.e., coarse instead of fine, and foreground instead of background) to provide the current feature or service requiring location and users should reasonably expect that the feature or service needs the level of location requested. For example, we may reject apps that request or access background location without compelling justification.
- Background location may only be used to provide features beneficial to the user and relevant to the core functionality of the app.

Apps are allowed to access location using foreground service (when the app only has foreground access e.g.: "while in use") permission if the use:

- has been initiated as a continuation of an in-app user-initiated action, and
- is terminated immediately after the intended use case of the user-initiated action is completed by the application.

Apps designed specifically for children must comply with the [Designed for Families](#) policy.

## All Files Access Permission

Files and directory attributes on a user's device are regarded as personal and sensitive user data subject to the [Personal and Sensitive Information](#) policy and the following requirements:

- Apps should only request access to device storage which is critical for the app to function, and may not request access to device storage on behalf of any third-party for any purpose that is unrelated to critical user-facing app functionality.
- Android devices running R (Android 11, API Level 30) or later, will require the `MANAGE_EXTERNAL_STORAGE` permission in order to manage access in shared storage. All apps that target R and request broad access to shared storage ("All files access") must successfully pass an appropriate access review prior to publishing. Apps allowed to use this permission must clearly prompt users to enable "All files access" for their app under "Special app access" settings. For more information on the R requirements, please see this [help article](#).

## Device and Network Abuse

We don't allow apps that interfere with, disrupt, damage, or access in an unauthorized manner the user's device, other devices or computers, servers, networks, application programming interfaces (APIs), or services, including but not limited to other apps on the device, any Google service, or an authorized carrier's network.

Apps on Google Play must comply with the default Android system optimization requirements documented in the [Core App Quality guidelines for Google Play](#).

An app distributed via Google Play may not modify, replace, or update itself using any method other than Google Play's update mechanism. Likewise, an app may not download executable code (e.g. dex, JAR, .so files) from a source other than Google Play. This restriction does not apply to code that runs in a virtual machine and has limited access to Android APIs (such as JavaScript in a webview or browser).



We don't allow code that introduces or exploits security vulnerabilities. Check out the [App Security Improvement Program](#) to find out about the most recent security issues flagged to developers.

Here are some examples of common violations:

- Apps that block or interfere with another app displaying ads.
- Game-cheating apps that affect the gameplay of other apps.
- Apps that facilitate or provide instructions on how to hack services, software or hardware, or circumvent security protections.
- Apps that access or use a service or API in a manner that violates its terms of service.
- Apps that are not [eligible for whitelisting](#) and attempt to bypass [system power management](#).
- Apps that facilitate proxy services to third parties may only do so in apps where that is the primary, user-facing core purpose of the app.
- Apps or third party code (e.g., SDKs) that download executable code, such as dex files or native code, from a source other than Google Play.
- Apps that install other apps on a device without the user's prior consent.
- Apps that link to or facilitate the distribution or installation of malicious software.

## Deceptive Behavior

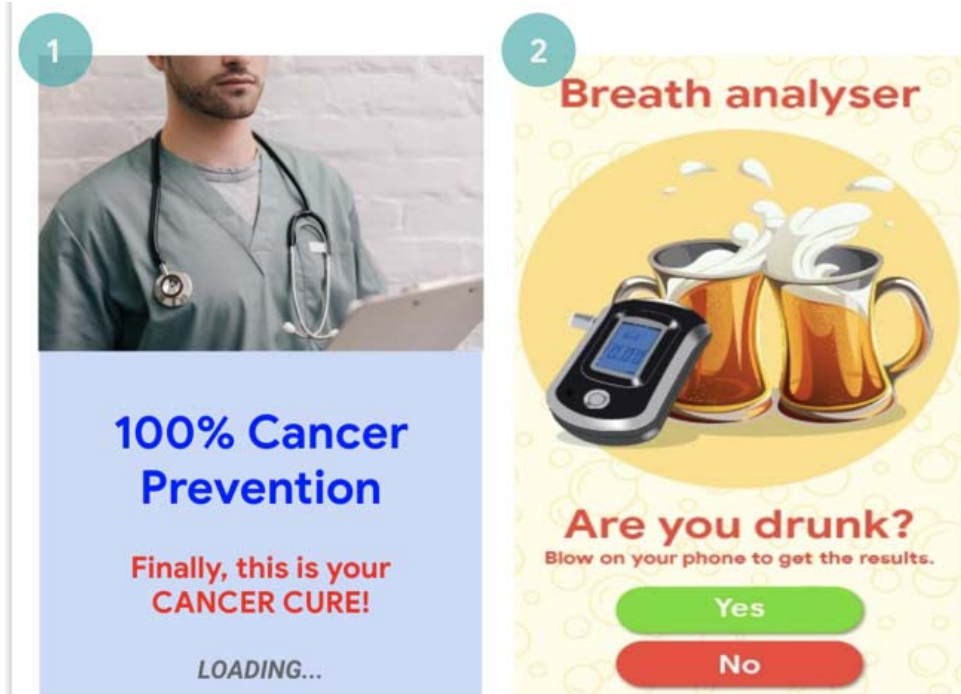
We don't allow apps that attempt to deceive users or enable dishonest behavior including but not limited to apps which are determined to be functionally impossible. Apps must provide an accurate disclosure, description and images/video of their functionality in all parts of the metadata. Apps must not attempt to mimic functionality or warnings from the operating system or other apps. Any changes to device settings must be made with the user's knowledge and consent and be reversible by the user.

## Misleading Claims

We don't allow apps that contain false or misleading information or claims, including in the description, title, icon, and screenshots.

Here are some examples of common violations:

- Apps that misrepresent or do not accurately and clearly describe their functionality:
  - An app that claims to be a racing game in its description and screenshots, but is actually a puzzle block game using a picture of a car.
  - An app that claims to be an antivirus app, but only contains a text guide explaining how to remove viruses.
- Developer or app names that misrepresent their current status or performance on Play. (E.g. "Editor's Choice," "Number 1 App," "Top Paid").
- Apps that feature medical or health-related content or functionalities that are misleading or potentially harmful.
- Apps that claim functionalities that are not possible to implement (e.g. insect repellent apps), even if it is represented as a prank, fake, joke, etc.
- Apps that are improperly categorized, including but not limited to the app rating or app category.
- Demonstrably deceptive content that may interfere with voting processes.
- Apps that falsely claim affiliation with a government entity or to provide or facilitate government services for which they are not properly authorized.
- Apps that falsely claim to be the official app of an established entity. Titles like "Justin Bieber Official" are not allowed without the necessary permissions or rights.



(1) This app features medical or health-related claims (Cure Cancer) that is misleading

(2) This apps claim functionalities that are not possible to implement (using your phone as a breathalyzer)

## Deceptive Device Settings Changes

We don't allow apps that make changes to the user's device settings or features outside of the app without the user's knowledge and consent. Device settings and features include system and browser settings, bookmarks, shortcuts, icons, widgets, and the presentation of apps on the homescreen.

Additionally, we do not allow:

- Apps that modify device settings or features with the user's consent but do so in a way that is not easily reversible.
- Apps or ads that modify device settings or features as a service to third parties or for advertising purposes.
- Apps that mislead users into removing or disabling third-party apps or modifying device settings or features.
- Apps that encourage or incentivize users into removing or disabling third-party apps or modifying device settings or features unless it is part of a verifiable security service.

## Enabling Dishonest Behavior

We don't allow apps that help users to mislead others or are functionally deceptive in any way, including, but not limited to: apps that generate or facilitate the generation of ID cards, social security numbers, passports, diplomas, credit cards and driver's licenses. Apps must provide accurate disclosures, titles, descriptions and images/video regarding the app's functionality and/or content and should perform as reasonably and accurately expected by the user.

Additional app resources (for example, game assets) may only be downloaded if they are necessary for the users' use of the app. Downloaded resources must be compliant with all Google Play policies, and before beginning the download, the app should prompt users and clearly disclose the download size.

Any claim that an app is a "prank", "for entertainment purposes" (or other synonym) does not exempt an app from application of our policies.

Here are some examples of common violations:

- Apps that mimic other apps or websites to trick users into disclosing personal or authentication information.
- Apps that depict or display unverified or real world phone numbers, contacts, addresses, or personally identifiable information of non-consenting individuals or entities.
- Apps with different core functionality based on a user's geography, device parameters, or other user-dependent data where those differences are not prominently advertised to the user in the store listing.
- Apps that change significantly between versions without alerting the user (e.g., ['what's new' section](#)) and updating the store listing.
- Apps that attempt to modify or obfuscate behavior during review.



- Apps with content delivery network (CDN) facilitated downloads that fail to prompt the user and disclose the download size prior to downloading.

## Manipulated Media

We don't allow apps that promote or help create false or misleading information or claims conveyed through imagery, videos and/or text. We disallow apps determined to promote or perpetuate demonstrably misleading or deceptive imagery, videos and/or text, which may cause harm pertaining to a sensitive event, politics, social issues, or other matters of public concern.

Apps that manipulate or alter media, beyond conventional and editorially acceptable adjustments for clarity or quality, must prominently disclose or watermark altered media when it may not be clear to the average person that the media has been altered. Exceptions may be provided for public interest or obvious satire or parody.

Here are some examples of common violations:

- Apps adding a public figure to a demonstration during a politically sensitive event.
- Apps using public figures or media from a sensitive event to advertise media altering capability within an app's store listing.
- Apps that alter media clips to mimic a news broadcast.



(1) This app provides functionality to alter media clips to mimic a news broadcast, and add famous or public figures to the clip without a watermark.

## Misrepresentation

We do not allow apps or developer accounts that impersonate any person or organization, or that misrepresent or conceal their ownership or primary purpose. We do not allow apps or developer accounts that engage in coordinated activity to mislead users. This includes, but isn't limited to, apps or developer accounts that misrepresent or conceal their country of origin and that direct content at users in another country.

## Malware

Malware is any code that could put a user, a user's data, or a device at risk. Malware includes, but is not limited to, Potentially Harmful Applications (PHAs), binaries, or framework modifications, consisting of categories such as trojans, phishing, and spyware apps, and we are continuously updating and adding new categories.

## Malware

Our Malware policy is simple, the Android ecosystem including the Google Play Store, and user devices should be free from malicious behaviors (i.e. malware). Through this fundamental principle we strive to provide a safe Android ecosystem for our users and their Android devices.

Though varied in type and capabilities, malware usually has one of the following objectives:

- Compromise the integrity of the user's device.
- Gain control over a user's device.
- Enable remote-controlled operations for an attacker to access, use, or otherwise exploit an infected device.
- Transmit personal data or credentials off the device without adequate disclosure and consent.
- Disseminate spam or commands from the infected device to affect other devices or networks.
- Defraud the user.

An app, binary, or framework modification can be Potentially Harmful, and therefore can generate malicious behavior, even if wasn't intended to be harmful. This is because apps, binaries, or framework modifications can function differently depending on a variety of variables. Therefore, what is harmful to one Android device might not pose a risk at all to another Android device. For example, a device running the latest version of Android is not affected by harmful apps which use deprecated APIs to perform malicious behavior but a device that is still running a very early version of Android might be at risk. Apps, binaries, or framework modifications are flagged as malware or PHA if they clearly pose a risk to some or all Android devices and users.

The malware categories, below, reflect our foundational belief that users should understand how their device is being leveraged and promote a secure ecosystem that enables robust innovation and a trusted user experience.

Visit [Google Play Protect](#) for more information.

## Backdoors

Code that allows the execution of unwanted, potentially harmful, remote-controlled operations on a device.

These operations may include behavior that would place the app, binary, or framework modification into one of the other malware categories if executed automatically. In general, backdoor is a description of how a potentially harmful operation can occur on a device and is therefore not completely aligned with categories like billing fraud or commercial spyware. As a result, a subset of backdoors, under some circumstances, are treated by Google Play Protect as a vulnerability.

## Billing Fraud

Code that automatically charges the user in an intentionally deceptive way.

Mobile billing fraud is divided into SMS fraud, Call fraud, and Toll fraud.

### *SMS Fraud*

Code that charges users to send premium SMS without consent, or tries to disguise its SMS activities by hiding disclosure agreements or SMS messages from the mobile operator notifying the user of charges or confirming subscriptions.

Some code, even though they technically disclose SMS sending behavior, introduce additional behavior that accommodates SMS fraud. Examples include hiding parts of a disclosure agreement from the user, making them unreadable, and conditionally suppressing SMS messages from the mobile operator informing the user of charges or confirming a subscription.

### *Call Fraud*

Code that charges users by making calls to premium numbers without user consent.

### *Toll Fraud*

Code that tricks users into subscribing to or purchasing content via their mobile phone bill.

Toll Fraud includes any type of billing except premium SMS and premium calls. Examples of this include direct carrier billing, wireless access point (WAP), and mobile airtime transfer. WAP fraud is one of the most prevalent types of Toll fraud. WAP fraud can include tricking users to click a button on a silently loaded, transparent WebView. Upon performing the action, a recurring subscription is initiated, and the confirmation SMS or email is often hijacked to prevent users from noticing the financial transaction.

## Stalkerware

Code that transmits personal information off the device without adequate notice or consent and doesn't display a persistent notification that this is happening.

Stalkerware apps transmit data to a party other than the PHA provider. Legitimate forms of these apps cannot be used by parents to track their children. However, these apps can be used to track a person (a spouse, for example) without their knowledge or permission unless a persistent notification is displayed while the data is being transmitted.

Only policy compliant apps exclusively designed and marketed for parental (including family) monitoring or enterprise management may distribute on the Play Store with tracking and reporting features, provided they fully comply with the requirements described below.

Apps distributed on the Play Store that monitor or track a user's behavior on a device must comply with these requirements:

- Apps must not present themselves as a spying or secret surveillance solution.
- Apps must not hide or cloak tracking behavior or attempt to mislead users about such functionality.
- Present users with a persistent notification and unique icon that clearly identifies the app.
- Apps and app listings on Google Play must not provide any means to activate or access functionality that violate these terms, such as linking to a non-compliant APK hosted outside Google Play.
- You are solely responsible for determining the legality of your app in its targeted locale. Apps determined to be unlawful in locations where they are published will be removed.

## Denial of Service (DoS)

Code that, without the knowledge of the user, executes a denial-of-service (DoS) attack or is a part of a distributed DoS attack against other systems and resources.

For example, this can happen by sending a high volume of HTTP requests to produce excessive load on remote servers.

## Hostile Downloaders

Code that isn't in itself potentially harmful, but downloads other PHAs.

Code may be a hostile downloader if:

- There is reason to believe it was created to spread PHAs and it has downloaded PHAs or contains code that could download and install apps; or
- At least 5% of apps downloaded by it are PHAs with a minimum threshold of 500 observed app downloads (25 observed PHA downloads).

Major browsers and file-sharing apps aren't considered hostile downloaders as long as:

- They don't drive downloads without user interaction; and
- All PHA downloads are initiated by consenting users.

## Non-Android Threat

Code that contains non-Android threats.

These apps can't cause harm to the Android user or device, but contain components that are potentially harmful to other platforms.

## Phishing

Code that pretends to come from a trustworthy source, requests a user's authentication credentials or billing information, and sends the data to a third-party. This category also applies to code that intercept the transmission of user credentials in transit.

Common targets of phishing include banking credentials, credit card numbers, and online account credentials for social networks and games.

## Elevated Privilege Abuse

Code that compromises the integrity of the system by breaking the app sandbox, gaining elevated privileges, or changing or disabling access to core security-related functions.

Examples include:

- An app that violates the Android permissions model, or steals credentials (such as OAuth tokens) from other apps.

- Apps that abuse features to prevent them from being uninstalled or stopped.
- An app that disables SELinux.

Privilege escalation apps that root devices without user permission are classified as rooting apps.

## Ransomware

Code that takes partial or extensive control of a device or data on a device and demands that the user make a payment or perform an action to release control.

Some ransomware encrypts data on the device and demands payment to decrypt the data and/or leverage the device admin features so that it can't be removed by a typical user. Examples include:

- Locking a user out of their device and demanding money to restore user control.
- Encrypting data on the device and demanding payment, ostensibly to decrypt the data.
- Leveraging device policy manager features and blocking removal by the user.

Code distributed with the device whose primary purpose is for subsidized device management may be excluded from the ransomware category provided they successfully meet requirements for secure lock and management, and adequate user disclosure and consent requirements.

## Rooting

Code that roots the device.

There's a difference between non-malicious and malicious rooting code. For example, non-malicious rooting apps let the user know in advance that they're going to root the device and they don't execute other potentially harmful actions that apply to other PHA categories.

Malicious rooting apps don't inform the user that they're going to root the device, or they inform the user about the rooting in advance but also execute other actions that apply to other PHA categories.

## Spam

Code that sends unsolicited messages to the user's contacts or uses the device as an email spam relay.

## Spyware

Code that transmits personal data off the device without adequate notice or consent.

For example, transmitting any of the following information without disclosures or in a manner that is unexpected to the user is sufficient to be considered spyware:

- Contact list
- Photos or other files from the SD card or that aren't owned by the app
- Content from user email
- Call log
- SMS log
- Web history or browser bookmarks of the default browser
- Information from the /data/ directories of other apps.

Behaviors that can be considered as spying on the user can also be flagged as spyware. For example, recording audio or recording calls made to the phone, or stealing app data.

## Trojan

Code that appears to be benign, such as a game that claims only to be a game, but that performs undesirable actions against the user.

This classification is usually used in combination with other PHA categories. A trojan has an innocuous component and a hidden harmful component. For example, a game that sends premium SMS messages from the user's device in the background and without the user's knowledge.

## A Note on Uncommon Apps

New and rare apps can be classified as uncommon if Google Play Protect doesn't have enough information to clear them as safe. This doesn't mean the app is necessarily harmful, but without further review it can't be cleared as safe either.

## A Note on the Backdoor Category

The backdoor malware category classification relies on how the code acts. A necessary condition for any code to be classified as a backdoor is that it enables behavior that would place the code into one of the other malware categories if executed automatically. For example, if an app allows dynamic code loading and the dynamically loaded code is extracting text messages, it will be classified as a backdoor malware.

However, if an app allows arbitrary code execution and we don't have any reason to believe that this code execution was added to perform a malicious behaviour then the app will be treated as having a vulnerability, rather than being backdoor malware, and the developer will be asked to patch it.

## Mobile Unwanted Software

This policy builds on the Google Unwanted Software Policy by outlining principles for the [Android ecosystem](#) and the Google Play Store. Software that violates these principles is potentially harmful to the user experience, and we will take steps to protect users from it.

### Mobile Unwanted Software

At Google, we believe that if we focus on the user, all else will follow. In our [Software Principles](#) and the [Unwanted Software Policy](#), we provide general recommendations for software that delivers a great user experience. This policy builds on the Google Unwanted Software Policy by outlining principles for the [Android ecosystem](#) and the Google Play Store. Software that violates these principles is potentially harmful to the user experience, and we will take steps to protect users from it.

As mentioned in the [Unwanted Software Policy](#), we've found that most unwanted software displays one or more of the same basic characteristics:

- It is deceptive, promising a value proposition that it does not meet.
- It tries to trick users into installing it or it piggybacks on the installation of another program.
- It doesn't tell the user about all of its principal and significant functions.
- It affects the user's system in unexpected ways.
- It collects or transmits private information without users' knowledge.
- It collects or transmits private information without a secure handling (e.g., transmission over HTTPS)
- It is bundled with other software and its presence is not disclosed.

On mobile devices, software is code in the form of an app, binary, framework modification, etc. In order to prevent software that is harmful to the software ecosystem or disruptive to the user experience we will take action on code that violates these principles.

Below, we build on the Unwanted Software Policy to extend its applicability to mobile software. As with that policy, we will continue to refine this Mobile Unwanted Software policy to address new types of abuse.

### Transparent behavior and clear disclosures

*All code should deliver on promises made to the user. Apps should provide all communicated functionality. Apps should not confuse users.*

- Apps should be clear about the functionality and objectives.
- Explicitly and clearly explain to the user what system changes will be made by the app. Allow users to review and approve all significant installation options and changes.
- Software should not misrepresent the state of the user's device to the user, for example by claiming the system is in a critical security state or infected with viruses.
- Don't utilize invalid activity designed to increase ad traffic and/or conversions.
- We don't allow apps that mislead users by impersonating someone else (e.g. another developer, company, entity) or another app. Don't imply that your app is related to or authorized by someone that it isn't.

Example violations:

- Ad fraud
- Impersonation

### Protect user data

*Be clear and transparent about the access, use, collection, and sharing of personal and sensitive user data. Uses of user data in must adhere to all relevant User Data Policies, where applicable, and take all precautions to protect the data.*



- Provide users an opportunity to agree to the collection of their data before you start collecting and sending it from the device, including data about third-party accounts, email, phone number, installed apps, files, location, and any other personal and sensitive data that the user would not expect to be collected.
- Personal and sensitive user data collected should be handled securely, including being transmitted using modern cryptography (for example, over HTTPS).
- Software, including mobile apps, must only transmit personal and sensitive user data to servers as it is related to the functionality of the app.

Example violations:

- Data Collection (cf [Spyware](#))
- Restricted Permissions abuse

Example User Data Policies:

- [Google Play User Data Policy](#)
- [GMS Requirements User Data Policy](#)
- [Google API Service User Data Policy](#)

#### Do not harm the mobile experience

*The user experience should be straightforward, easy-to-understand, and based on clear choices made by the user. It should present a clear value proposition to the user and not disrupt the advertised or desired user experience.*

- Don't show ads that are displayed to users in unexpected ways including impairing or interfering with the usability of device functions, or displaying outside the triggering app's environment without being easily dismissable and adequate consent and attribution.
- Apps should not interfere with other apps or the usability of the device
- Uninstall, where applicable, should be clear.
- Mobile software should not mimic prompts from the device OS or other apps. Do not suppress alerts to the user from other apps or from the operating system, notably those which inform the user of changes to their OS.

Example violations:

- Disruptive ads
- Unauthorized Use or Imitation of System Functionality

## Ad Fraud

Ad fraud is strictly prohibited. Ad interactions generated for the purpose of tricking an ad network into believing traffic is from authentic user interest is ad fraud, which is a form of [invalid traffic](#). Ad fraud may be the byproduct of developers implementing ads in disallowed ways, such as showing hidden ads, automatically clicking ads, altering or modifying information and otherwise leveraging non-human actions (spiders, bots, etc.) or human activity designed to produce invalid ad traffic. Invalid traffic and ad fraud is harmful to advertisers, developers, and users, and leads to long-term loss of trust in the mobile Ads ecosystem..

Here are some examples of common violations:

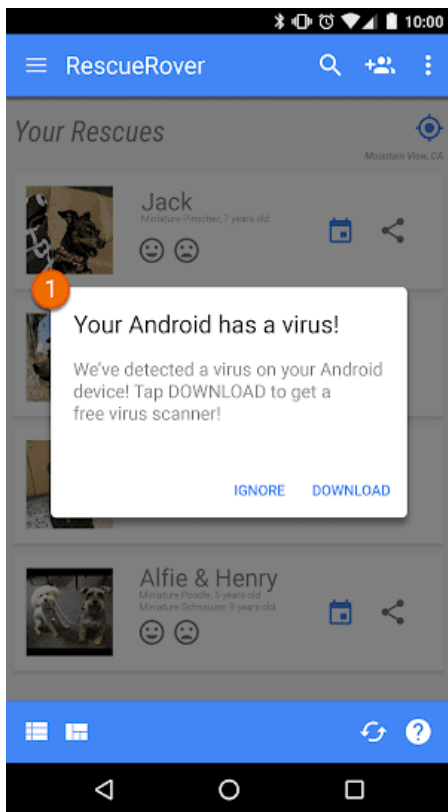
- An app that renders ads that are not visible to the user.
- An app that automatically generates clicks on ads without the user's intention or that produces equivalent network traffic to fraudulently give click credits.
- An app sending fake installation attribution clicks to get paid for installations that did not originate from the sender's network.
- An app that pops up ads when the user is not within the app interface.
- False representations of the ad inventory by an app, e.g. an app that communicates to ad networks that it is running on an iOS device when it is in fact running on an Android device; an app that misrepresents the package name that is being monetized.

## Unauthorized Use or Imitation of System Functionality

We don't allow apps or ads that mimic or interfere with system functionality, such as notifications or warnings. System level notifications may only be used for an app's integral features, such as an airline app that notifies users of special deals, or a game that notifies users of in-game promotions.

Here are some examples of common violations:

- Apps or ads that are delivered through a system notification or alert:



① The system notification shown in this app is being used to serve an ad.

For additional examples involving ads, please refer to the [Ads policy](#).

## Impersonation

When developers impersonate others or their apps, it misleads users and hurts the developer community. We prohibit apps that mislead users by impersonating someone else.

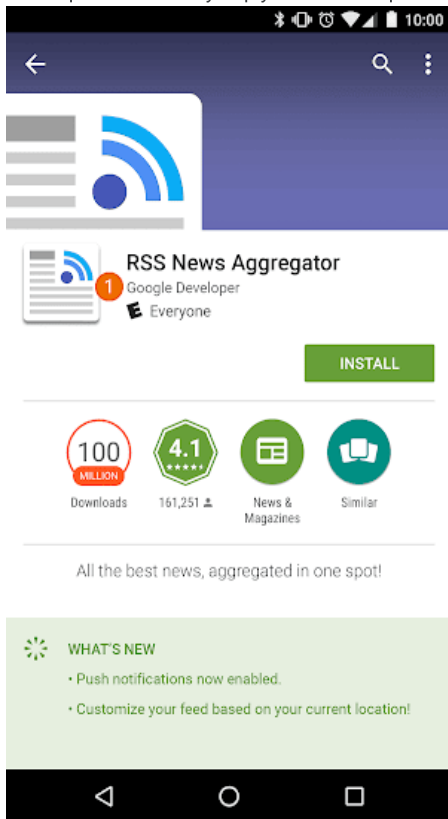
### Impersonation

We don't allow apps that mislead users by impersonating someone else (e.g. another developer, company, entity) or another app. Don't imply that your app is related to or authorized by someone that it isn't. Be careful not to use app icons, descriptions, titles, or in-app elements that could mislead users about your app's relationship to someone else or another app.

Here are some examples of common violations:



- Developers that falsely imply a relationship to another company / developer:



① The developer name listed for this app suggests an official relationship with Google, even though such a relationship doesn't exist.

- App titles and icons that are so similar to those of existing products or services that users may be misled:

✓	 Google Maps	 Google+	 YouTube	 Twitter
✗	 Google Maps Navigator	 Google+ Sharify	 YouTube Aggregator	 TwitterPro

## Monetization and Ads

Google Play supports a variety of monetization strategies to benefit developers and users, including paid distribution, in-app products, subscriptions, and ad-based models. To ensure the best user experience, we require you to comply with these policies.

## Payments

Apps that employ in-store or in-app purchases must comply with the following guidelines:

**In-store purchases:** Developers charging for apps and downloads from Google Play must use Google Play's payment system.

**In-app purchases:**

- Developers offering products within a game downloaded on Google Play or providing access to game content must use [Google Play In-app Billing](#) as the method of payment.
- Developers offering products within another category of app downloaded on Google Play must use [Google Play In-app Billing](#) as the method of payment, except for the following cases:
  - Payment is solely for physical products

- Payment is for digital content that may be consumed outside of the app itself (e.g. songs that can be played on other music players).
- In-app virtual currencies must only be used within the app or game title for which they were purchased.
- Developers must not mislead users about the apps they are selling nor about any in-app services, goods, content, or functionality offered for purchase. If your product description on Google Play refers to in-app features that may require a specific or additional charge, your description must clearly notify users that payment is required to access those features.
- Apps offering mechanisms to receive randomized virtual items from a purchase (i.e. "loot boxes") must clearly disclose the odds of receiving those items in advance of purchase.

**Here are some examples of products supported by Google Play In-app Billing:**

- **Virtual game products**, including coins, gems, extra lives or turns, special items or equipment, characters or avatars, additional levels or playtime.
- **App functionality or content**, such as an ad-free version of an app or new features not available in the free version.
- **Subscription services**, such as streaming music, video, book, or other media services; digital publications, including when bundled with a physical edition; and social networking services.
- **Cloud software products**, including data storage services, business productivity software, and financial management software.

**Here are some examples of products not currently supported by Google Play In-app Billing:**

- **Retail merchandise**, such as groceries, clothing, housewares, and electronics.
- **Service fees**, including taxi and transportation services, cleaning services, food delivery, airfare, and event tickets.
- **One-time membership fees or recurring dues**, including gym memberships, loyalty programs, or clubs offering accessories, clothing, or other physical products.
- **One time-payments**, including peer-to-peer payments, online auctions, and donations.
- **Electronic bill payment**, including credit card bills, utilities, and cable or telecommunications services.

Note that we offer the Google Pay API for apps selling physical products and services. For more information, please visit our [Google Pay developer page](#).

## Subscriptions

You, as a developer, must not mislead users about any subscription services or content you offer within your app. It is critical to communicate clearly in any in-app promotions or splash screens.

**In your app:** You must be transparent about your offer. This includes being explicit about your offer terms, the cost of your subscription, the frequency of your billing cycle, and whether a subscription is required to use the app. Users should not have to perform any additional action to review the information.

**Here are some examples of common violations:**

- Monthly subscriptions that do not inform users they will be automatically renewed and charged every month.
- Annual subscriptions that most prominently display their pricing in terms of monthly cost.
- Subscription pricing and terms that are incompletely localized.
- In-app promotions that do not clearly demonstrate that a user can access content without a subscription (when available).
- SKU names that do not accurately convey the nature of the subscription, such as "Free Trial" for a subscription with an auto-recurring charge.

**Get AnalyzeAPP Premium**

16 issues found in your data!  
Subscribe to see how we can help

12 months	6 months	1 month
\$9.16/mo Save 35%	\$12.50/mo Save 11% MOST POPULAR PLAN	\$14.00/mo

3 Try for \$12.50!

4 Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

- ① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.
- ② Offer only displays pricing in terms of monthly cost and users may not understand that they will be charged a six month price at the time they subscribe.
- ③ Offer only shows the introductory price and users may not understand what they will automatically be charged at the end of the introductory period.
- ④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

## Free Trials & Introductory Offers

**Before a user is enrolled in your subscription:** You must clearly and accurately describe the terms of your offer, including the duration, pricing, and description of accessible content or services. Be sure to let your users know how and when a free trial will convert to a paid subscription, how much the paid subscription will cost, and that a user can cancel if they do not want to convert to a paid subscription.

Here are some examples of common violations:

- Offers that do not clearly explain how long the free trial or introductory pricing will last.
- Offers that do not clearly explain that the user will be automatically enrolled in a paid subscription at the end of the offer period.
- Offers that do not clearly demonstrate that a user can access content without a trial (when available).
- Offer pricing and terms that are incompletely localized.



① Dismiss button is not clearly visible and users may not understand that they can access functionality without signing up for the free trial.

② Offer emphasizes the free trial and users may not understand that they will automatically be charged at the end of the trial.

③ Offer does not state a trial period and users may not understand how long their free access to subscription content will last.

④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

## Subscriptions Management & Cancellation

As a developer, you must ensure that your app clearly disclose how a user can manage or cancel their subscription.

It is your responsibility to notify your users of any changes to your subscription, cancellation and refund policies and ensure that the policies comply with applicable law.

## Ads

We don't allow apps that contain deceptive or disruptive ads. Ads must only be displayed within the app serving them. We consider ads served in your app as part of your app. The ads shown in your app must be compliant with all our policies. For policies on gambling ads, please click [here](#).

## Use of Location Data for Ads

Apps that extend usage of permission based device location data for serving ads are subject to the [Personal and Sensitive Information](#) policy, and must also comply with the following requirements:

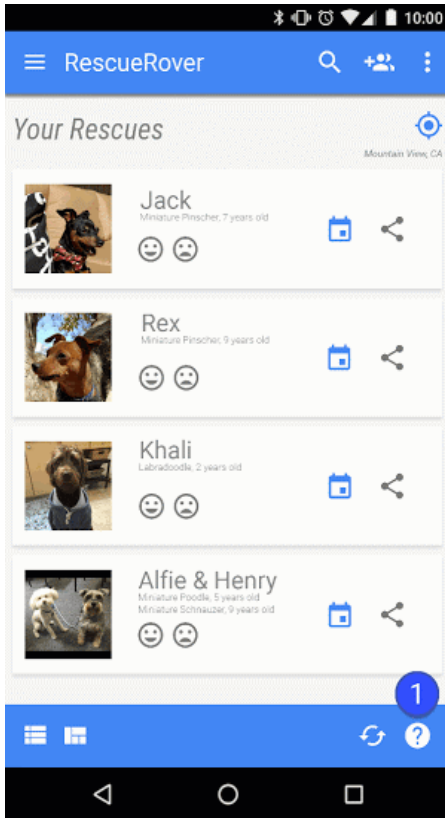
- Use or collection of permission based device location data for advertising purposes must be clear to the user and documented in the app's mandatory privacy policy, including linking to any relevant ad network privacy policies addressing location data use.
- In accordance with [Location Permissions](#) requirements, location permissions may only be requested to implement current features or services within your app, and may not request device location permissions solely for the use of ads.

## Deceptive Ads

Ads must not simulate or impersonate the user interface of any app, notification, or warning elements of an operating system. It must be clear to the user which app is serving each ad.

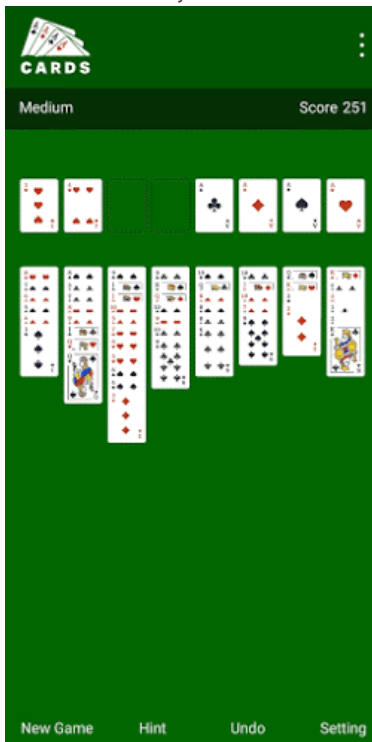
Here are some examples of common violations:

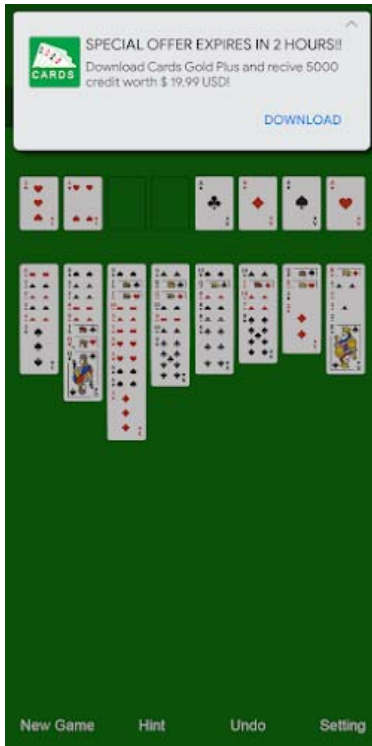
- Ads that mimic an app's UI:



① The question mark icon in this app is an ad that takes the user to an external landing page.

- Ads that mimic a system notification:





The examples above illustrate ads mimicking various system notifications.

## Lockscreen Monetization

Unless the exclusive purpose of the app is that of a lockscreen, apps may not introduce ads or features that monetize the locked display of a device.

## Disruptive Ads

Disruptive ads are ads that are displayed to users in unexpected ways, that may result in inadvertent clicks, or impairing or interfering with the usability of device functions.

Your app cannot force a user to click an ad or submit personal information for advertising purposes before they can fully use an app. Interstitial ads may only be displayed inside of the app serving them. If your app displays interstitial ads or other ads that interfere with normal use, they must be easily dismissible without penalty.

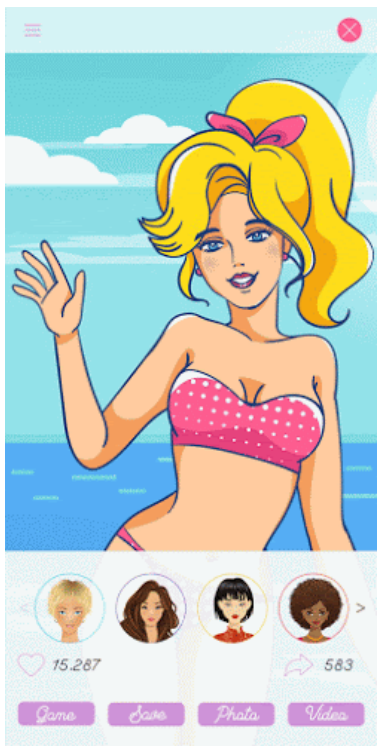
Here are some examples of common violations:

- Ads that take up the entire screen or interfere with normal use and do not provide a clear means to dismiss the ad:



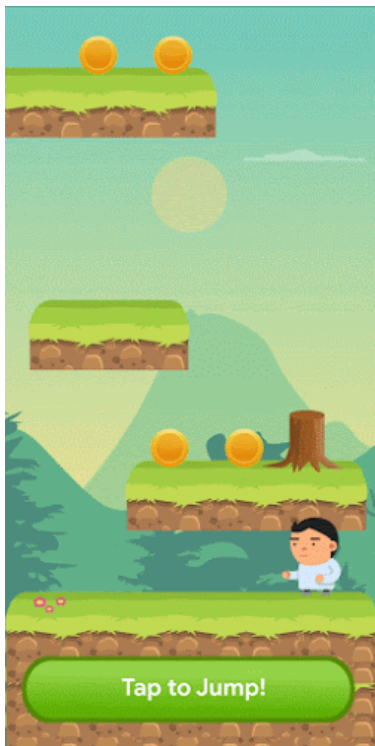
① This ad does not have a dismiss button.

- Ads that force the user to click-through by using a false dismiss button, or by making ads suddenly appear in areas of the app whether the user usually taps for another function.



An ad that is using a false dismiss button





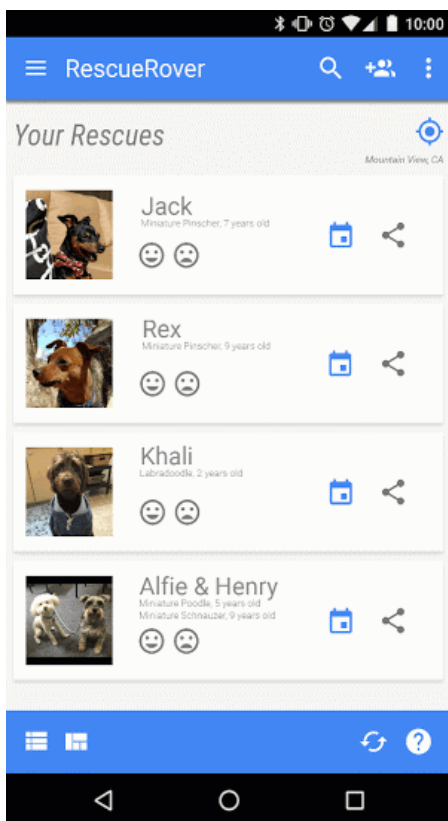
An ad that suddenly appears in an area where the user is used to tapping for in-app functions

### Interfering with Apps, Third-party Ads, or Device Functionality

Ads associated with your app must not interfere with other apps, ads, or the operation of the device, including system or device buttons and ports. This includes overlays, companion functionality, and widgetized ad units. Ads must only be displayed within the app serving them.

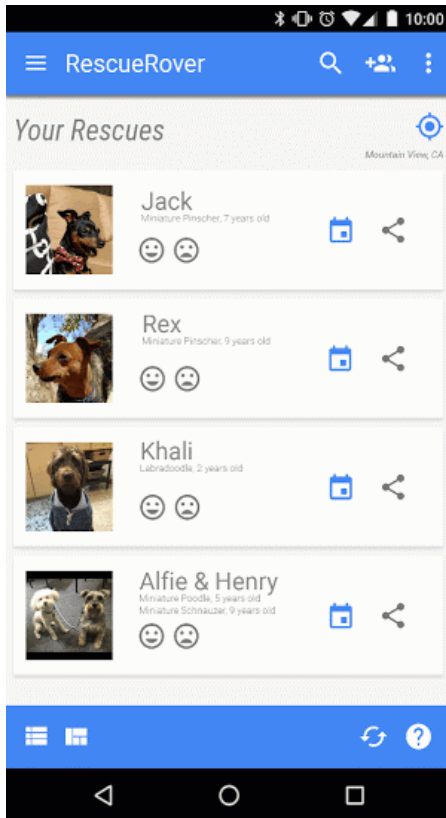
Here are some examples of common violations:

- Ads that display outside of the app serving them:



Description: The user navigates to the home screen from this app, and suddenly an ad appears on the homescreen.

- Ads that are triggered by the home button or other features explicitly designed for exiting the app:

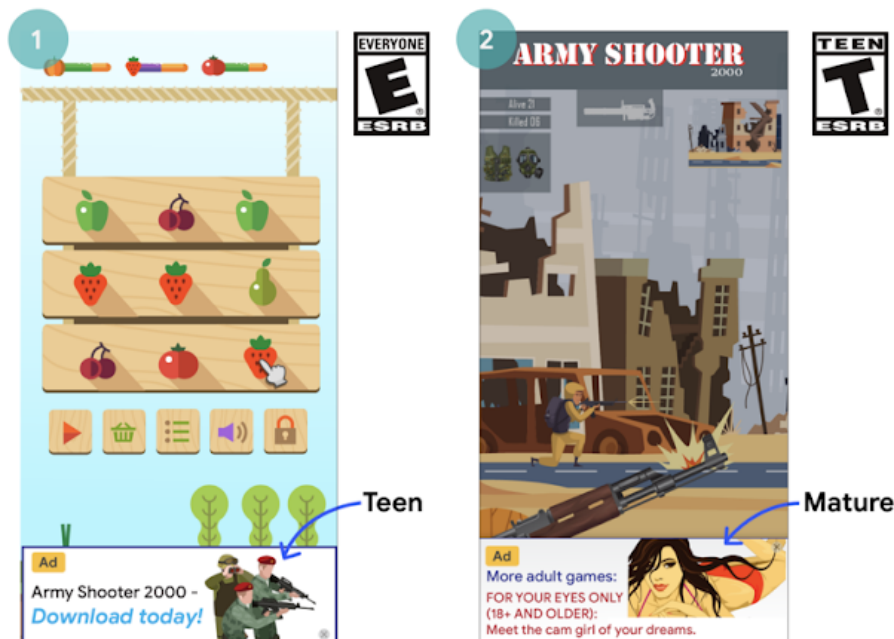


Description: The user attempts to exit the app and navigate to the home screen, but instead, the expected flow is interrupted by an ad.

## Inappropriate Ads

The ads shown within your app must be appropriate for the intended audience of your app, even if the content by itself is otherwise compliant with our policies.

Here is an example of a common violation:



- ① This ad is inappropriate (Teen) for the intended audience of the app (7+)
- ② This ad is inappropriate (Mature) for the intended audience of the app (12+)

## Usage of Android Advertising ID

Google Play Services version 4.0 introduced new APIs and an ID for use by advertising and analytics providers. Terms for the use of this ID are below.

- **Usage.** The Android advertising identifier must only be used for advertising and user analytics. The status of the “Opt out of Interest-based Advertising” or “Opt out of Ads Personalization” setting must be verified on each access of the ID.
- **Association with personally-identifiable information or other identifiers**
  - Advertising use: The advertising identifier may not be connected to persistent device Identifiers (for example: SSAID, MAC address, IMEI, etc.) for any advertising purpose. The advertising identifier may only be connected to personally-identifiable information with the explicit consent of the user.
  - Analytics use: The advertising identifier may only be connected to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) with the explicit consent of the user.
- **Respecting users' selections.** If reset, a new advertising identifier must not be connected to a previous advertising identifier or data derived from a previous advertising identifier without the explicit consent of the user. Also, you must abide by a user's “Opt out of Interest-based Advertising” or “Opt out of Ads Personalization” setting. If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection.
- **Transparency to users.** The collection and use of the advertising identifier and commitment to these terms must be disclosed to users in a legally adequate privacy notification. To learn more about our privacy standards, please review our [User Data](#) policy.
- **Abiding by the terms of use.** The advertising identifier may only be used in accordance with these terms, including by any party that you may share it with in the course of your business. All apps uploaded or published to Google Play must use the advertising ID (when available on a device) in lieu of any other device identifiers for any advertising purposes.

## Families Ads Program

If you serve ads in your app, and the target audience for your app only includes children as described in the [Families Policy](#), then you must use ad SDKs that have self-certified compliance with Google Play policies, including the Ad SDK certification requirements below. If the target audience for your app includes both children and older users, you must implement age screening measures and make sure that ads shown to children come exclusively from one of these self-certified ad SDKs. Apps in the Designed for Families program are required to only use self-certified ad SDKs.

The use of Google Play certified ad SDKs is only required if you are using ad SDKs to serve ads to children. The following are permitted without an ad SDK's self-certification with Google Play, however, you are still responsible for ensuring your

ad content and data collection practices are compliant with Play's [User Data Policy](#) and [Families Policy](#):

- In-House Advertising whereby you use SDKs to manage cross promotion of your apps or other owned media and merchandising
- Entering into direct deals with advertisers whereby you use SDKs for inventory management

#### Ad SDK Certification Requirements

- Define what are objectionable ad content and behaviors and prohibit them in the ad SDK's terms or policies. The definitions should comply with Play's Developer Program Policies.
- Create a method to rate your ad creatives according to age appropriate groups. Age appropriate groups must at least include groups for Everyone and Mature. The rating methodology must align with the methodology that Google supplies to SDKs once they have filled out the interest form below.
- Allow publishers, on a per-request or per-app basis, to request child-directed treatment for ad serving. Such treatment must be in compliance with applicable laws and regulations, such as the [US Children's Online Privacy and Protection Act \(COPPA\)](#) and the EU [General Data Protection Regulation \(GDPR\)](#). Google Play requires ad SDKs to disable personalized ads, interest based advertising, and remarketing as part of the child-directed treatment.
- Allow publishers to select ad formats that are compliant with [Play's Families Ads and Monetization policy](#), and meet the requirement of the [Teacher Approved program](#).
- Ensure that when real-time bidding is used to serve ads to children, the creatives have been reviewed and privacy indicators are propagated to the bidders.
- Provide Google with sufficient information, such as information indicated in the [interest form](#) below, to verify the ad SDK's compliance with all certification requirements, and respond in a timely manner to any subsequent requests for information.

*Note: Ad SDKs must support ad serving that complies with all relevant statutes and regulations concerning children that may apply to their publishers.*

Mediation requirements for serving platforms when serving ads to children:

- Only use Play certified ad SDKs or implement safeguards necessary to ensure that all ads served from mediation comply with these requirements; and
- Pass information necessary to mediation platforms to indicate the ad content rating and any applicable child-directed treatment.

Developers can find a [list of self-certified ad SDKs](#) here.

Also, developers can share this [interest form](#) with ad SDKs who wish to become self-certified.

## Store Listing and Promotion

The promotion and visibility of your app dramatically affects store quality. Avoid spammy store listings, low quality promotion, and efforts to artificially boost app visibility on Google Play.

### App Promotion

We don't allow apps that directly or indirectly engage in or benefit from promotion practices that are deceptive or harmful to users or the developer ecosystem. This includes apps that engage in the following behavior:

- Using deceptive ads on websites, apps, or other properties, including notifications that are similar to system notifications and alerts.
- Promotion or installation tactics that redirect users to Google Play or download apps without informed user action.
- Unsolicited promotion via SMS services.

It is your responsibility to ensure that any ad networks or affiliates associated with your app comply with these policies and do not employ any prohibited promotion practices.

### Metadata

We don't allow apps with misleading, improperly formatted, non-descriptive, irrelevant, excessive, or inappropriate metadata, including but not limited to the app's description, developer name, title, icon, screenshots, and promotional images. Developers must provide a clear and well-written description of their app. We also don't allow unattributed or anonymous user testimonials in the app's description.

In addition to the requirements noted here, specific Play Developer Policies may require you to provide additional metadata information.

Here are some examples of common violations:



- ① Unattributed or Anonymous User testimonials
- ② Data comparison of apps or brands
- ③ Word blocks and vertical/horizontal word lists

Here are some examples of inappropriate text, images, or videos within your listing:

- Imagery or videos with sexually suggestive content. Avoid suggestive imagery containing breasts, buttocks, genitalia, or other fetishized anatomy or content, whether illustrated or real.
- Using profane, vulgar, or other language that is inappropriate for a general audience in your app's Store listing.
- Graphic violence prominently depicted in app icons, promotional images, or videos.
- Depictions of the illicit usage of drugs. Even EDSA (Educational, Documentary, Scientific, or Artistic) content must be suitable for all audiences within the store listing.

Here are a few best practices:

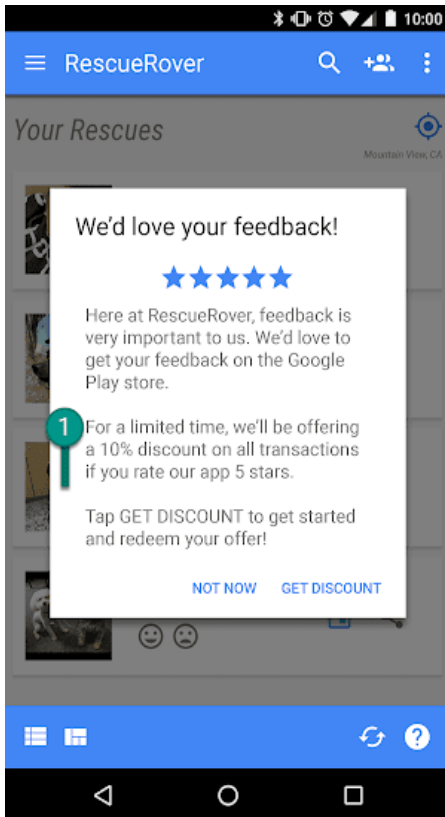
- Highlight what's great about your app. Share interesting and exciting facts about your app to help users understand what makes your app special.
- Make sure that your app's title and description accurately describe your app's functionality.
- Avoid using repetitive or unrelated keywords or references.
- Keep your app's description succinct and straightforward. Shorter descriptions tend to result in a better user experience, especially on devices with smaller displays. Excessive length, detail, improper formatting, or repetition can result in a violation of this policy.
- Remember that your listing should be suitable for a general audience. Avoid using inappropriate text, images or videos in your listing and adhere to the guidelines above.

## User Ratings, Reviews, and Installs

Developers must not attempt to manipulate the placement of any apps in Google Play. This includes, but is not limited to, inflating product ratings, reviews, or install counts by illegitimate means, such as fraudulent or incentivized installs, reviews and ratings.

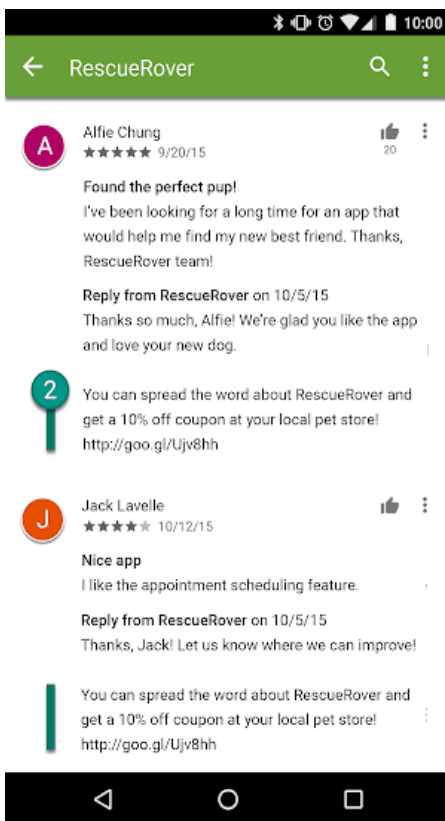
Here are some examples of common violations:

- Asking users to rate your app while offering an incentive:



① This notification offers users a discount in exchange for a high rating.

- Repeatedly submitting ratings to influence the app's placement on Google Play.
- Submitting or encouraging users to submit reviews containing inappropriate content, including affiliates, coupons, game codes, email addresses, or links to websites or other apps:



② This review encourages users to promote the RescueRover app by making a coupon offer.



Ratings and reviews are benchmarks of app quality. Users depend on them to be authentic and relevant. Here are some best practices when responding to user reviews:

- Keep your reply focused on the issues raised in the user's comments and don't ask for a higher rating.
- Include references to helpful resources such as a support address or FAQ page.

## Content Ratings

Content ratings on Google Play are provided by the International Age Rating Coalition (IARC) and are designed to help developers communicate locally relevant content ratings to users. Regional IARC authorities maintain guidelines which are used to determine the maturity level of the content in an app. We don't allow apps without a content rating on Google Play.

### How content ratings are used

Content ratings are used to inform consumers, especially parents, of potentially objectionable content that exists within an app. They also help filter or block your content in certain territories or to specific users where required by law, and determine your app's eligibility for special developer programs.

### How content ratings are assigned

To receive a content rating, you must fill out a [rating questionnaire on the Play Console](#) that asks about the nature of your apps' content. Your app will be assigned a content rating from multiple rating authorities based on your questionnaire responses. Misrepresentation of your app's content may result in removal or suspension, so it is important to provide accurate responses to the content rating questionnaire.

To prevent your app from being listed as "Unrated", you must complete the content rating questionnaire for each new app submitted to the Play Console, as well as for all existing apps that are active on Google Play.

If you make changes to your app content or features that affect the responses to the rating questionnaire, you must submit a new content rating questionnaire in the Play Console.

Visit the [Help Center](#) to find more information on the different [rating authorities](#) and how to complete the content rating questionnaire.

### Rating appeals

If you do not agree with the rating assigned to your app, you can appeal directly to the IARC rating authority using the link provided in your certificate email.

## News

Apps that select the 'News' category but exhibit content that does not meet these requirements are not permitted in the News category of the Play Store. News apps that require a user to purchase a membership must provide a content preview for users prior to purchase.

News apps MUST:

- provide adequate information about the news publisher and its contributors including clear ownership, and
- have a website or in-app page that provides valid contact information for the news publisher.

News apps MUST NOT:

- contain significant spelling & grammar errors,
- contain only static content, and
- have affiliate marketing or ad revenue as its primary purpose.

News aggregator apps must be transparent about the publishing source of the content in the app and each of the sources must meet News policy requirements.

## Spam and Minimum Functionality

At a minimum, apps should provide users with a basic degree of functionality and a respectful user experience. Apps that crash, exhibit other behavior that is not consistent with a functional user experience, or that serve only to spam users or Google Play are not apps that expand the catalog in a meaningful way.



## Spam

We don't allow apps that spam users or Google Play, such as apps that send users unsolicited messages or apps that are repetitive or low-quality.

## Message Spam

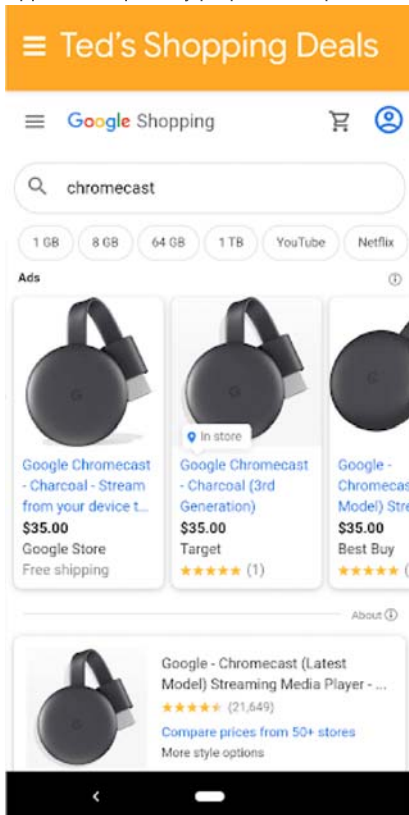
We don't allow apps that send SMS, email, or other messages on behalf of the user without giving the user the ability to confirm the content and intended recipients.

## Webviews and Affiliate Spam

We don't allow apps whose primary purpose is to drive affiliate traffic to a website or provide a webview of a website without permission from the website owner or administrator.

Here are some examples of common violations:

- An app whose primary purpose is to drive referral traffic to a website to receive credit for user sign-ups or purchases on that website.
- Apps whose primary purpose is to provide a webview of a website without permission:



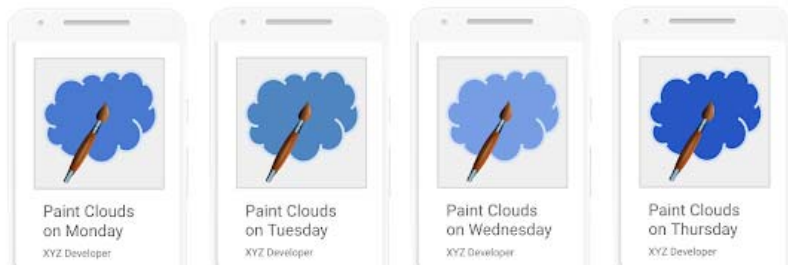
This app is called "Ted's Shopping Deals" and it simply provides a webview of Google Shopping.

## Repetitive Content

We don't allow apps that merely provide the same experience as other apps already on Google Play. Apps should provide value to users through the creation of unique content or services.

Here are some examples of common violations:

- Copying content from other apps without adding any original content or value.
- Creating multiple apps with highly similar functionality, content, and user experience. If these apps are each small in content volume, developers should consider creating a single app that aggregates all the content.



## Made for Ads

We do not allow apps whose primary purpose is to serve ads.

Here are some examples of common violations:

- Apps where interstitial ads are placed after every user action, including but not limited to clicks, swipes, etc.

## Minimum Functionality

Ensure your app provides a stable, engaging, responsive user experience.

Here are some examples of common violations:

- Apps that are designed to do nothing or have no function

## Broken Functionality

We don't allow apps that crash, force close, freeze, or otherwise function abnormally.

Here are some examples of common violations:

- Apps that don't install
- Apps that install, but don't load
- Apps that load, but are not responsive

## Other Programs

In addition to compliance with the content policies set out elsewhere in this Policy Center, apps that are designed for other Android experiences and distributed via Google Play may also be subject to program-specific policy requirements. Be sure to review the list below to determine if any of these policies apply to your app.

## Android Instant Apps

Our goal with Android Instant Apps is to create delightful, frictionless user experiences while also adhering to the highest standards of privacy and security. Our policies are designed to support that goal.

Developers choosing to distribute Android Instant Apps through Google Play must adhere to the following policies, in addition to all other [Google Play Developer Program Policies](#).

## Identity

For instant apps that include login functionality, developers must integrate [Smart Lock for Passwords](#).

## Link Support

Android Instant Apps developers are required to properly support links for other apps. If the developer's instant app or installed app contains links that have the potential to resolve to an instant app, the developer must send users to that instant app, rather than, for example, capturing the links in a [WebView](#).

## Technical Specifications

Developers must comply with the Android Instant Apps technical specifications and requirements provided by Google, as may be amended from time to time, including those listed in [our public documentation](#).

## Offering App Installation

The instant app may offer the user the installable app, but this must not be the instant app's primary purpose. When offering installation, developers must:

- Use the [Material Design "get app" icon](#) and the label "install" for the installation button.
- Not have more than 2-3 implicit installation prompts in their instant app.
- Not use a banner or other ad-like technique for presenting an installation prompt to users.

Additional instant app details and UX guidelines can be found in the [Best Practices for User Experience](#).

## Changing Device State

Instant apps must not make changes to the user's device that persist longer than the instant app session. For example, instant apps may not change the user's wallpaper or create a homescreen widget.

## App Visibility

Developers must ensure that instant apps are visible to the user, such that the user is aware at all times that the instant app is running on their device.

## Device Identifiers

Instant apps are prohibited from accessing device identifiers that both (1) persist after the instant app stops running and (2) are not resettable by the user. Examples include, but are not limited to:

- Build Serial
- Mac Addresses of any networking chips
- IMEI, IMSI

Instant apps may access phone number if obtained using the runtime permission. The developer must not attempt to fingerprint the user using these identifiers or any other means.

## Network traffic

Network traffic from inside the instant app must be encrypted using a TLS protocol like HTTPS.

## Families

Google Play offers a rich platform for developers to showcase their high-quality, age appropriate content for the whole family. Before submitting an app to the Designed for Families program or submitting an app that targets children to the Google Play Store, you are responsible for ensuring your app is appropriate for children and compliant with all relevant laws.

Learn about the families process and review the interactive checklist at [Academy for App Success](#).

## Designing Apps for Children and Families

The use of technology as a tool for enriching families' lives continues to grow, and parents are looking for safe, high-quality content to share with their children. You may be designing your apps specifically for children or your app may just attract their attention. Google Play wants to help you make sure your app is safe for all users, including families.

The word "children" can mean different things in different locales and in different contexts. It is important that you consult with your legal counsel to help determine what obligations and/or age-based restrictions may apply to your app. You know best how your app works so we are relying on you to help us make sure apps on Google Play are safe for families.

Apps designed specifically for children must participate in the Designed for Families program. If your app targets both children and older audiences, you may still participate in the Designed for Families program. All apps that opt in to the Designed for Families program will be eligible to be rated for the [Teacher Approved program](#), but we cannot guarantee that your app will be included in the Teacher Approved program. If you decide not to participate in the Designed for Families program, you still must comply with the Google Play Families Policy requirements below, as well as all other [Google Play Developer Program Policies](#) and the [Developer Distribution Agreement](#).

## Play Console Requirements

### [Target Audience and Content](#)

In the [Target Audience and Content](#) section of the Google Play Console you must indicate the target audience for your app, prior to publishing, by selecting from the list of age groups provided. Regardless of what you identify in the Google

Play Console, if you choose to include imagery and terminology in your app that could be considered targeting children, this may impact Google Play's assessment of your declared target audience. Google Play reserves the right to conduct its own review of the app information that you provide to determine whether the target audience that you disclose is accurate.

If you select a target audience that only includes adults, but Google determines that this is inaccurate because your app is targeting both children and adults, you will have the option to make clear to users that your app is not targeting children by agreeing to carry a warning label.

You should only select more than one age group for your app's target audience if you have designed your app for and ensured that your app is appropriate for users within the selected age group. For example, apps designed for babies, toddlers, and preschool children should only have the age group "Ages 5 & Under" selected as the age group target for those apps. If your app is designed for a specific level of school, choose the age group that best represents that school level. You should only select age groups that include both adults and children if you truly have designed your app for all ages.

#### Updates to Target Audience and Content Section

You can always update your app's information in the Target Audience and Content section in the Google Play Console. An [app update](#) is required before this information will be reflected on the Google Play store. However, any changes you make in this section of the Google Play Console may be reviewed for policy compliance even before an app update is submitted.

We strongly recommend that you let your existing users know if you change the target age group for your app or start using ads or in-app purchases, either by using the "What's New" section of your app's store listing page or through in-app notifications.

#### Misrepresentation in Play Console

Misrepresentation of any information about your app in the Play Console, including in the Target Audience and Content section, may result in removal or suspension of your app, so it is important to provide accurate information.

## Families Policy Requirements

If one of the target audiences for your app is children, you must comply with the following requirements. Failure to satisfy these requirements may result in app removal or suspension.

1. **App content:** Your app's content that is accessible to children must be appropriate for children.
2. **Google Play Console Answers:** You must accurately answer the questions in the Google Play Console regarding your app and update those answers to accurately reflect any changes to your app.
3. **Ads:** If your app displays ads to children or to users of unknown age, you must:
  - only use [Google Play certified ad SDKs](#) to display ads to those users;
  - ensure ads displayed to those users do not involve interest-based advertising (advertising targeted at individual users who have certain characteristics based on their online browsing behavior) or remarketing (advertising targeted at individual users based on previous interaction with an app or website);
  - ensure ads displayed to those users present content that is appropriate for children;
  - ensure ads displayed to those users follow the Families ad format requirements; and
  - ensure compliance with all applicable legal regulations and industry standards relating to advertising to children.
4. **Data Collection:** You must disclose the collection of any [personal and sensitive information](#) from children in your app, including through APIs and SDKs called or used in your app. Sensitive information from children includes, but is not limited to, authentication information, microphone and camera sensor data, device data, Android ID, ad usage data, and advertising ID.
5. **APIs and SDKs:** You must ensure that your app properly implements any APIs and SDKs.
  - Apps that solely target children must not contain any APIs or SDKs that are not approved for use in child-directed services. This includes, Google Sign-In (or any other Google API Service that accesses data associated with a Google Account), Google Play Games Services, and any other API Service using OAuth technology for authentication and authorization.
  - Apps that target both children and older audiences must not implement APIs or SDKs that are not approved for use in child-directed services unless they are used behind a [neutral age screen](#) or implemented in a way that does not result in the collection of data from children (e.g., providing Google Sign-in as an optional feature). Apps that target both children and older audiences must not require users to sign-in or access app content through an API or SDK that is not approved for use in child-directed services.
6. **Privacy policy:** You must provide a link to your app's privacy policy on your app's store listing page. This link must be maintained at all times while the app is available on the Store, and it must link to a privacy policy that, among other things, accurately describes your app's data collection and use.

**7. Special restrictions:**

- If your app uses Augmented Reality, you must include a safety warning immediately upon launch of the AR section. The warning should contain the following:
  - An appropriate message about the importance of parental supervision.
  - A reminder to be aware of physical hazards in the real world (e.g., be aware of your surroundings).
- Your app must not require the usage of a device that is advised not to be used by children. (e.g. Daydream, Oculus)

**8. Legal Compliance:** You must ensure that your app, including any APIs or SDKs that your app calls or uses, is compliant with the [U.S. Children's Online Privacy and Protection Act \(COPPA\)](#), [E.U. General Data Protection Regulation \(GDPR\)](#), and any other applicable laws or regulations.

**Here are some examples of common violations:**

- Apps that promote play for children in their store-listing but the app content is only appropriate for adults.
- Apps that implement APIs with terms of service that prohibit their use in child-directed apps.
- Apps that glamorize the use of alcohol, tobacco or controlled substances.
- Apps that include real or simulated gambling.
- Apps that include violence, gore, or shocking content not appropriate for children.
- Apps that provide dating services or offer sexual or marital advice.
- Apps that contain links to websites that present content that violates Google Play's [Developer Program policies](#).
- Apps that show mature ads (e.g. violent content, sexual content, gambling content) to children. Please see the [Families Ads and Monetization policies](#) for more information on Google Play's policies on advertising, in-app purchase, and commercial content for children.

## Designed for Families Program

Apps designed specifically for children must participate in the Designed for Families program. If your app is designed for everyone, including children and families, you too can apply to participate in the program.

Before being accepted into the program your app must meet all of the Families Policy requirements and Designed for Families eligibility requirements, in addition to those outlined in the [Google Play Developer Program Policies](#) and [Developer Distribution Agreement](#).

For more information on the process for submitting your app for inclusion in the program, click [here](#).

**Program Eligibility**

All apps participating in the Designed for Families program must have both app and ad content that are relevant and appropriate for children and must satisfy all of the requirements below. Apps accepted into the Designed for Families program must remain compliant with all program requirements. Google Play may reject, remove, or suspend any app determined to be inappropriate for the Designed for Families program.

**Designed for Families Requirements**

1. Apps must be rated ESRB Everyone or Everyone 10+, or equivalent.
2. You must accurately disclose the app's interactive elements on the Content Rating Questionnaire in the Google Play Console, including whether:
  - users can interact or exchange information;
  - your app shares user-provided personal information with third parties; and
  - your app shares the user's physical location with other users.
3. If your app uses the [Android Speech API](#), your app's RecognizerIntent.EXTRA\_CALLING\_PACKAGE must be set to its PackageName.
4. Apps must only use [Google Play certified ad SDKs](#).
5. Apps designed specifically for children cannot request location permissions.
6. Apps must use the [Companion Device Manager\(CDM\)](#) when requesting Bluetooth, unless your app is only targeting device Operating System(OS) versions that are not compatible with CDM.

**Here are some examples of common apps that are ineligible for the program:**

- Apps that are rated ESRB Everyone but contain ads for gambling content
- Apps for parents or care-givers (e.g., breastfeeding tracker, developmental guide)
- Parent guides or device management apps that are only intended for use by parents or care-givers
- Apps that use an app icon or a launcher icon that is inappropriate for children

**Categories**

If you are accepted to participate in the Designed for Families program, you can choose a second Families-specific category that describes your app. Here are the categories available for apps participating in the Designed for Families program:

**Action & Adventure:** Action-oriented apps/games, including everything from simplistic racing games to fairy tale adventures, to other apps and games that are designed to generate excitement.

**Brain Games:** Games that make the user think, including puzzles, matching games, quizzes, and other games that challenge the memory, intelligence or logic.

**Creativity:** Apps and games that encourage creativity, including drawing apps, painting apps, coding apps, and other apps and games where you can build and make things.

**Education:** Apps and games designed with input from learning experts (e.g., educators, learning specialists, researchers) to promote learning, including academic, social-emotional, physical, and creative learning, as well as learning related to basic life skills, critical thinking, and problem solving.

**Music and Video:** Apps and games with a musical or video component, including everything from instrument simulation apps to apps that provide video and musical audio content.

**Pretend Play:** Apps and games where the user can pretend to take on a role, for example, pretending to be a chef, caregiver, prince/princess, firefighter, police person or fictional character.

## Ads and Monetization

The policies below apply to all advertising in your app, including ads for your apps and third party apps, offers for in-app purchase, or any other commercial content (such as paid product placement) that is served to users of apps that are subject to the Families Policy Requirements and/or the Designed for Families Requirements. All advertising, offers for in-app purchase, and commercial content in these apps must comply with all applicable laws and regulations (including any relevant self-regulatory or industry guidelines).

Google Play reserves the right to reject, remove or suspend apps for overly aggressive commercial tactics.

### Ad format requirements

Ads and offers for in-app purchases must not have deceptive content or be designed in a way that will result in inadvertent clicks from child users. The following are prohibited:

- Disruptive ads, including ads that take up the entire screen or interfere with normal use and do not provide a clear means to dismiss the ad (e.g. [Ad walls](#))
- Ads that interfere with normal app use or game play that are not closeable after 5 seconds. Ads that do not interfere with normal app use or game play may persist for more than 5 seconds (e.g. video content with integrated ads).
- Interstitial ads or offers for in-app purchase displayed immediately upon app launch
- Multiple ad placements on a page (e.g. banner ads that show multiple offers in one placement or displaying more than one banner or video ad is not allowed).
- Ads or offers for in-app purchases that are not clearly distinguishable from your app content
- Use of shocking or emotionally manipulative tactics to encourage ads viewing or in-app purchases
- Not providing a distinction between the use of virtual game coins versus real-life money to make in-app purchases

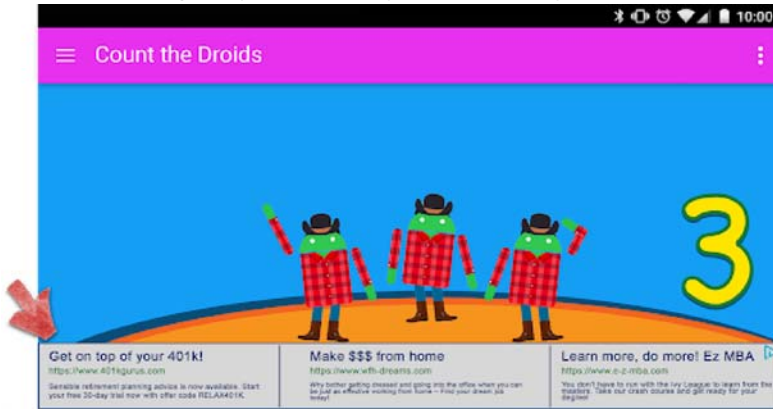
### Here are some examples of common ad format violations

- Ads that move away from a user's finger as the user tries to close it
- Ads that take up the majority or the device screen without providing the user a clear way to dismiss it, as depicted in the example below:

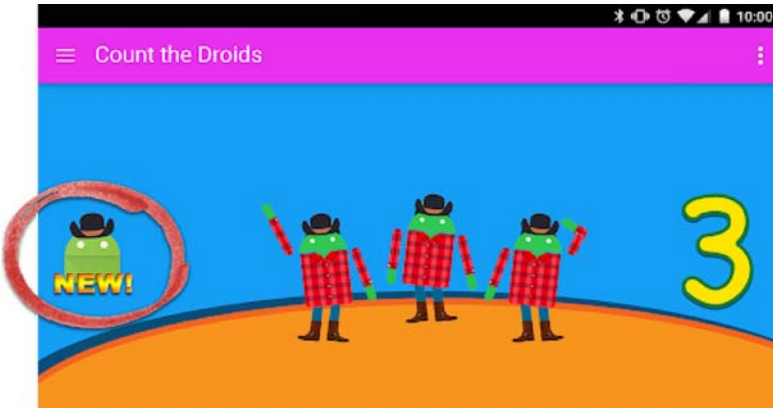




- Banner ads showing multiple offers, as depicted in the example below:

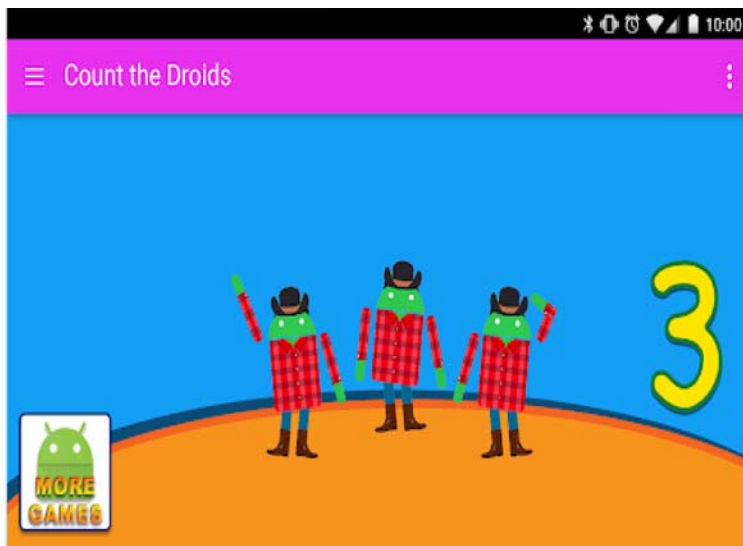


- Ads that could be mistaken by a user for app content, as depicted in the example below:



- Buttons or ads that promote your other Google Play store listings but that are indistinguishable from app content, as depicted in the example below:





Here are some examples of inappropriate ad content that should not be displayed to children.

- **Inappropriate Media Content:** Ads for TV shows, movies, music albums, or any other media outlet that are not appropriate for children.
- **Inappropriate Video Games & Downloadable Software:** Ads for downloadable software and electronic video games that are not appropriate for children.
- **Controlled or Harmful Substances:** Ads for alcohol, tobacco, controlled substances, or any other harmful substances.
- **Gambling:** Ads for simulated gambling, contests or sweepstakes promotions, even if free to enter.
- **Adult and Sexually Suggestive Content:** Ads with sexual, sexually suggestive and mature content.
- **Dating or Relationships:** Ads for dating or adult relationship sites.
- **Violent Content:** Ads with violent and graphic content that is not appropriate for children.

#### Ad SDKs

If you serve ads in your app and your target audience only includes children, then you must use [Google Play certified ad SDKs](#). If the target audience for your app includes both children and older users, you must implement age screening measures, such as a [neutral age screen](#), and make sure that ads shown to children come exclusively from Google Play certified ad SDKs. Apps in the Designed for Families program are required to only use self-certified ad SDKs.

Please refer to the [Families Ads Program policy](#) page for more details on these requirements and to see the current list of approved ad SDKs.

If you use AdMob, refer to the [AdMob Help Center](#) for more details on their products.

It is your responsibility to ensure your app satisfies all requirements concerning advertisements, in-app purchases, and commercial content. Contact your ad SDK provider to learn more about their content policies and advertising practices.

#### In-app purchases

Google Play will re-authenticate all users prior to any in-app purchases in apps participating in the Designed for Families program. This measure is to help ensure that the financially responsible party, and not children, are approving purchases.

## Enforcement

Avoiding a policy violation is always better than managing one, but when violations do occur, we're committed to ensuring developers understand how they can bring their app into compliance. Please let us know if you [see any violations](#) or have any questions about [managing a violation](#).

## Policy Coverage

Our policies apply to any content your app displays or links to, including any ads it shows to users and any user-generated content it hosts or links to. Further, they apply to any content from your developer account which is publicly displayed in Google Play, including your developer name and the landing page of your listed developer website.

We don't allow apps that let users install other apps to their devices. Apps that provide access to other apps, games, or software without installation, including features and experiences provided by third parties, must ensure that all the content they provide access to adheres to all [Google Play policies](#) and may also be subject to additional policy reviews.

Defined terms used in these policies have the same meaning as in the [Developer Distribution Agreement \(DDA\)](#). In addition to complying with these policies and the DDA, the content of your app must be rated in accordance with our [Content Rating Guidelines](#).

In assessing whether to include or remove apps from Google Play, we consider a number of factors including, but not limited to, a pattern of harmful behavior or high risk of abuse. We identify risk of abuse including, but not limited to, items such as previous violation history, user feedback, and use of popular brands, characters, and other assets.

## How Google Play Protect works

Google Play Protect checks apps when you install them. It also periodically scans your device. If it finds a potentially harmful app, it might:

- Send you a notification. To remove the app, tap the notification, then tap Uninstall.
- Disable the app until you uninstall it.
- Remove the app automatically. In most cases, if a harmful app has been detected, you will get a notification saying that the app was removed.

## How malware protection works

To protect you against malicious third-party software, URLs and other security issues, Google may receive information about:

- Your device's network connections
- Potentially harmful URLs
- Operating system, and apps installed on your device through Google Play or other sources.

You may get a warning from Google about an app or URL that may be unsafe. The app or URL may be removed or blocked from installation by Google if it is known to be harmful to devices, data or users.

You can choose to disable some of these protections in your device settings. But Google may continue to receive information about apps installed through Google Play, and apps installed on your device from other sources may continue to be checked for security issues without sending information to Google.

## How Privacy alerts work

Google Play Protect will alert you if an app is removed from the Google Play Store because the app may access your personal information and you'll have an option to uninstall the app.

## Enforcement Process

If your app violates any of our policies, we'll take appropriate action as outlined below. In addition, we'll provide you with relevant information about the action we've taken via email along with instructions on how to appeal if you believe we've taken action in error.

Please note that removal or administrative notices may not indicate each and every policy violation present in your app or broader app catalog. Developers are responsible for addressing any policy issue and conducting extra due diligence to ensure that the remainder of their app is fully policy compliant. Failure to address policy violations in all of your apps may result in additional enforcement actions.

Repeated or serious violations (such as malware, fraud, and apps that may cause user or device harm) of these policies or the [Developer Distribution Agreement \(DDA\)](#) will result in termination of individual or related Google Play Developer accounts.

## Enforcement Actions

Different enforcement actions can impact your app in different ways. The following section describes the various actions Google Play may take, and the impact to your app and / or your Google Play Developer account. This information is also explained in [this video](#).

## Rejection

- A new app or app update submitted for review will not be made available on Google Play.
- If an update to an existing app was rejected, the app version published prior to the update will remain available on Google Play.
- Rejections don't impact your access to a rejected app's existing user installs, statistics, and ratings.
- Rejections don't impact the standing of your Google Play Developer account.

Note: Do not attempt to resubmit a rejected app until you've fixed all the policy violations.

## Removal

- The app, along with any previous versions of that app, are removed from Google Play and will no longer be available for users to download.
- Because the app is removed, users will not be able to see the app's Store listing, user installs, statistics, and ratings. This information will be restored once you submit a policy-compliant update for the removed app.
- Users may not be able to make any in-app purchases, or utilize any in-app billing features in the app until a policy-compliant version is approved by Google Play.
- Removals don't immediately impact the standing of your Google Play Developer account, but multiple removals may result in a suspension.

Note: Don't attempt to republish a removed app until you've fixed all policy violation.

## Suspension

- The app, along with any previous versions of that app, are removed from Google Play and will no longer be available for users to download.
- Suspension can occur as the result of egregious or multiple policy violations, as well as repeated app rejections or removals.
- Because the app is suspended, users will not be able to see the app's Store listing, existing user installs, statistics, and ratings. This information will be restored once you submit a policy-compliant update for the removed app.
- You can no longer use a suspended app's APK or app bundle.
- Users will not be able to make any in-app purchases, or utilize any in-app billing features in the app until a policy-compliant version is approved by Google Play.
- Suspensions count as strikes against the good standing of your Google Play Developer account. Multiple strikes can result in the termination of individual and related Google Play Developer accounts.

Note: Don't attempt to republish a suspended app unless Google Play has explained that you may do so.

## Limited Visibility

- Your app's discoverability on Google Play is restricted. Your app will remain available on Google Play and can be accessed by users with a direct link to the app's Play store listing.
- Having your app placed in a Limited Visibility state doesn't impact the standing of your Google Play Developer account.
- Having your app placed in a Limited Visibility state doesn't impact users' ability to see the app's existing Store listing, user installs, statistics, and ratings.

## Account Termination

- When your developer account is terminated, all apps in your catalog will be removed from Google Play and you will no longer be able to publish new apps. This also means that any related Google Play developer accounts will also be permanently suspended.
- Multiple suspensions or suspensions for egregious policy violations may also result in the termination of your Play Console account.
- Because the apps within the terminated account are removed, users will not be able to see the apps' Store listing, existing user installs, statistics, and ratings.

Note: Any new account that you try to open will be terminated as well (without a refund of the developer registration fee), so please do not attempt to register for a new Play Console account while one of your other accounts are terminated.

## Managing and Reporting Policy Violations

How to handle a policy violation on Go...



## Appealing an Enforcement Action

We will reinstate applications if an error was made, and we find that your application does not violate the Google Play Program Policies and Developer Distribution Agreement. If you've reviewed the policies carefully and feel that our decision may have been in error, please follow the instructions provided to you in the enforcement email notification to appeal our decision.

## Additional Resources

If you need more information regarding an enforcement action or a rating/comment from a user, you may refer to some of the resources below or contact us through the [Google Play Help Center](#). We cannot, however, offer you legal advice. If you need legal advice, please consult your legal counsel.

- [App verification & appeals](#)
- [Report a policy violation](#)
- [Contact Google Play about an account termination or app removal](#)
- [Fair warnings](#)
- [Report inappropriate apps & comments](#)
- [My app has been removed from Google Play](#)
- [Understanding Google Play developer account terminations](#)

 Give feedback about this article

---

Was this helpful?

Yes

No

---

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

# **Exhibit I**

**Subject:** Re: Magazine subscription write up  
**From:** "Steve Jobs" <Confidential>  
**Received(Date):** Sun, 06 Feb 2011 21:19:57 +0000  
**To:** "Eddy Cue" <Confidential>  
**Cc:** "Philip Schiller" <Confidential>  
**Date:** Sun, 06 Feb 2011 21:19:57 +0000

---

I think this is all pretty simple - iBooks is going to be the only bookstore on iOS devices. We need to hold our heads high. One can read books bought elsewhere, just not buy/rent/subscribe from iOS without paying us, which we acknowledge is prohibitive for many things.

Sent from my iPad

On Feb 6, 2011, at 11:17 AM, Eddy Cue <Confidential> wrote:

> I am also looking forward to discussing whether we require in-app for books. At first this doesn't seem that bad not to require but the more I think about it, it will be very problematic. It will be difficult to limit this to books. What about Netflix, WSJ, MLB, Pandora, etc? They will all do it. Where do you draw the line? And many other would want it (e.g. magazines and games). The problem is many can afford 30% but others will say they can't. This is going to be a huge decision for us. We don't want to lose the apps from iOS and at the same time we don't want to compromise the app experience that we have (e.g. don't have to enter your info or payment everywhere).

>

> Eddy

>

> Sent from my iPhone

>

> On Feb 6, 2011, at 12:27 PM, Philip Schiller <Confidential> wrote:

>

>> One interesting point: magazines and newspapers argued that they don't like our offering because they want to get a lot of customer data (mostly name, email, address, phone number) but one of the big things they get by offering an app is a ton of customer data that they never had before - they can learn what stories customers read, how often and long they read, where they are (weather), what teams they follow (sports), when they were born (horoscopes), what companies they follow (stocks and business), what games they play (crosswords, suduko, etc), what ads they click on, etc. It is very impressive all they can learn about customers without forcing the customer to provide anything that they do not want to share.

>>

>>

>> On Feb 6, 2011, at 1:11 PM, Eddy Cue wrote:

>>

>>> I thought we should meet to go over the rules. We need to decide what we want to



do with books. I have asked Lanita for a meeting with Phil, you and I this week.

>>>

>>> The basic premise is if the publisher brings a subscriber we get nothing and if we bring the subscriber we get 70/30. Apps must offer our in-app subscription offer and can not link out to any other. Publisher can offer subscriptions through any of their mechanisms (e.g. print, web site).

>>>

>>> Here are the rules with all the fine details for subscriptions -

>>> • Only for magazine and newspaper apps

>>> • Offer can be weekly, monthly, bi-monthly, quarterly, bi-yearly or yearly (you can offer more than one)

>>> • Customer is automatically charged each time (e.g. weekly) until they indicate that they no longer wish to subscribe. At that point, they will receive any pending issues to the end of their paid subscription.

>>> • When customer buys a subscription, they will be asked if they want to share their name, email and zip code with the publisher. In addition, the publisher can offer a free incentive based on their offer (e.g. extra month for monthly or 2 weeks for weekly) if customer agrees to send the information.

>>> • Newspaper or magazine publisher sets the subscription pricing (can be free if they want to)

>>> • Subscription rates must be equal or less than other digital rate offered elsewhere

>>> • If publisher changes the subscription price, it applies to all existing subscribers at the time of renewal (if the price is higher than the customer was paying, they will be notified and will need to agree to the higher rate).

>>> • Revenue split is 70/30 for all subscription payments (Apple is not involved with any transaction that happens outside the store)

>>> • Subscription can include any other digital access (e.g. access to paid web site)

>>> • Subscription can not include any physical product (e.g. print)>>> • App can not require sign in or personal information at launch but can optionally ask the customer if they wish to register with their site (existing rule already)

>>> • In the app, you can make other product offerings (e.g. buy a calendar, sign up for an email list) transacted directly with the publisher

>>> • Newspaper or magazine publisher can give free access to existing print subscribers (publisher does authentication)

>>> • Newspaper or magazine publisher can sell digital subscriptions on their properties and Apple does not get any payments (publisher does authentication)

>>> • The app must have a subscription offer using Apple's recurring subscription (can not link out from the app to any subscription offering).

>>>

>>> This may sound complicated but it addresses their needs and bounds the box which we must do. Without it, some will try to do things that are not appropriate or fair.

>>>

>>> For books, it is less complicated except book stores will claim this model doesn't work because they pay 30% to the publisher already. For those with which this is the case, they would break even. They have other ways to make money using their own sites and cutting better deals. If I want to sell my Android book app on their new Android store I only get 20% so Amazon is getting a better deal!



>>>

>>> The book rules are -

>>> • App must include Apple in-app purchases for new books (can not link out to buy a book)

>>> • App may read books purchased outside the app.

>>>

>>> We will get you a draft of this by tomorrow.

>>>

>>> Eddy

>>>

>>>

>>> On Feb 6, 2011, at 10:38 AM, Steve Jobs wrote:

>>>

>>>> I have seen nothing yet. We need a few paragraphs clearly stating our philosophy, and how this directly translates into our new policies.

>>>>

>>>> Sent from my iPhone

>>>

>>

---