Culper Research

Disclaimer

By downloading from or viewing material on this website you agree to the following Terms of Service. Use of Culper Research's ("Culper") research is at your own risk. In no event should Culper or any affiliated party be liable for any direct or indirect trading losses caused by any information on this site. You further agree to do your own research and due diligence, consult your own financial, legal, and tax advisors before making any investment decision with respect to transacting in any securities covered herein. You should assume that Culper (possibly along with or through our members, partners, affiliates, employees, and/or consultants) along with our clients and/or investors has a position in any securities covered herein. You should assume that following publication of any research, we are likely to immediately transact in these securities (by increasing and/or decreasing positions and/or risk exposure), continue to trade in these securities for an undefined time period thereafter, and be long, short, or neutral at any time hereafter regardless of our initial recommendation, conclusions, or opinions. We trade securities in conjunction with risk tolerances and management practices, and such trading may result in the derisking of some or all of the positions in the securities covered herein, at any time following publication of any report, depending on security-specific, market, portfolio, or other relevant conditions. Culper does not undertake to update or supplement this report to reflect changes in its position. Research may contain estimated fair values of securities, utilizing various valuation methods. Estimated fair values are not price targets, and Culper does not commit to hold securities until such time as the estimated fair values are reached. Culper may change its estimates of fair values at any time hereafter without updating its research or otherwise disclosing updated fair values publicly. We may transact in the covered securities for various reasons, none of which may relate to Culper's estimates of fair value. Research is not investment advice nor a recommendation or solicitation to buy securities. To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the securities covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. However, such information is presented "as is," without warranty of any kind – whether express or implied. Culper makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use. Research may contain forward-looking statements, estimates, projections, and opinions with respect to among other things, certain accounting, legal, and regulatory issues the issuer faces and the potential impact of those issues on its future business, financial condition and results of operations, as well as more generally, the issuer's anticipated operating performance, access to capital markets, market conditions, assets and liabilities. Such statements, estimates, projections and opinions may prove to be substantially inaccurate and are inherently subject to significant risks and uncertainties beyond Culper's control. All expressions of opinion are subject to change without notice, and Culper does not undertake to update or supplement this report or any of the information contained herein. You agree that the information on this website is copyrighted, and you therefore agree not to distribute this information (whether the downloaded file, copies / images / reproductions, or the link to these files) in any manner other than by providing the following link — http://www.culperresearch.com The failure of Culper to exercise or enforce any right or provision of these Terms of Service shall not constitute a waiver of this right or provision. If any provision of these Terms of Service is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision and rule that the other provisions of these Terms of Service remain in full force and effect, in particular as to this governing law and jurisdiction provision. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of this website or the material herein must be filed within one (1) year after such claim or cause of action arose or be forever barred.

A quick note from Culper Research,

Since our founding, I have always sought to push our process forward to the fullest extent possible. AppLovin was not an exception. Over the past several months, our research into AppLovin encompassed a decompiling and forensic review of AppLovin and partner app code, app download data, consultations with a renowned ad fraud researcher, interviews with former employees, customers across both mobile gaming and e-commerce, competitors, and industry experts, as well as extensive reviews of AppLovin filings and disclosures, public announcements, social media comments, AppLovin employee profiles, and more. We also spoke with current, former, and potential investors. In the course of this process, we realized that Fuzzy Panda Research ("FPR") was also investigating the Company. As such, FPR and Culper opted to share some of our views and research with one another, with the idea that "iron sharpens iron." FPR and Culper also agreed that we ought to each present our own unique views of the Company. We reiterate that the views we express in this report are entirely our own, based on research that is entirely our own. We hope that investors evaluate our work, as always, on its merit.

Happy reading,

Christian Lamarco
Founder, Culper Research

AppLovin Corporation (NADSAQ:APP): Force-Feeding Users with Silent Backdoor Installs and Copying Meta's Homework. Straight to the Principal's Office, Please

Source: YouTube[1]

We are short AppLovin ("APP", "the Company"), an AdTech platform for mobile gaming apps. APP shares have risen over 500% in the past 12 months, owing to investor enthusiasm for the Company's supposed breakthrough "AI" technology, AXON 2.0. AppLovin consistently credits AXON 2.0 for the turnaround in its mobile gaming business over the past 2 years, and has now doubled down on its promotion of AXON 2.0 in its claims to soon revolutionize e-commerce advertising, too. AppLovin wants investors to believe that AXON 2.0 is, in the words of CEO Adam Foroughi, "a black box" – irreplicable, inscrutable, and ingenious. We believe, however, that AppLovin has employed AXON 2.0 largely as a promotional tool – a smokescreen to hide the true drivers of its mobile gaming and e-commerce initiatives, neither of which have much to do with AI.

Having peaked at a market capitalization of $173 billion, we believe AppLovin could go down as the single largest US stock promotion unraveling since at least the GFC. We are short for two reasons.

- First, we believe AppLovin's recent success in mobile gaming stems from the systematic exploitation of app permissions that enable *advertisements themselves* to force-feed silent, backdoor app installations directly onto users' phones, with just a single click – an event that is often inadvertent thanks to the Company's notorious UX gimmicks. **This is AdTech's version of *"the truck rolling down the hill."*** As AppLovin is paid largely on a per-install basis, each illicit install translates directly to profit.

- Second, we believe AppLovin's nascent e-commerce initiative is a smoke and mirrors game that the Company has rigged in its favor from the start. AppLovin must maintain a tight rein on advertisers it allows onto the platform, lest the narrative slip. To that end, the Company requires advertisers first demonstrate proof of $600,000 per month on Meta, so that AppLovin – through its MAX mediation platform – can "see" ads shown to Meta users in order to insert itself into the process and take credit for the sale. AppLovin then cajoles advertisers into spreading the news of their success, drumming up excitement. The Company has parlayed this excitement into a waitlist, where sources say the Company is now again stacking the deck with advertisers with low SKU counts, those without robust data science

[1] This is a clipping from an episode of a British television sitcom, and should be evaluated solely as such.

teams (who can more easily call bullshit), or those who are willing to use Adjust, AppLovin's own attribution platform that allows the Company to "grade their own homework."

The Mechanics of AppLovin's Backdoor Installation Scheme: Unwanted Apps Force-Fed to Users Directly from Ads. Pure Profit to AppLovin

In late 2022, AppLovin introduced Array, which partners with OEMs and carriers to install new applications on users' phones at the time of unboxing. As such, Array's "AppHub" – a system-level app – is granted powerful "direct download" permissions that allow AppHub to install apps outside of the Google Play store. Tellingly, AppLovin stopped disclosing new partnerships in late 2023, but based on our decompiling of AppHub's code, we believe AppLovin has quietly achieved large-scale distribution of AppHub through partnerships with several major OEMs and carriers distributing hundreds of millions of phones across the world. Indeed, AppLovin proudly touts its ability to reach 1.4 billion daily active users across thousands of apps worldwide, and AppLovin employees publicly brag about how the program was deployed to 20 million T-Mobile phones in 6 months alone.

From late 2022 through at least late 2024, AppLovin simultaneously smuggled a single permission into thousands of their own advertising customers apps via MAX SDK updates. The permission allows the apps to "bind" to AppHub, effectively borrowing or inheriting AppHub's one-click direct install permissions as their own. This permission is presently embedded within many of the most popular free-to-play games in the world, including Subway Surfers, 8 Ball Pool, Wordscapes, and Angry Birds 2.

Finally, AppLovin ads within these games then hijack these permissions to force-feed direct installations to users.[2] Others – including Fuzzy Panda Research – have written extensively on what we can only refer to, if we're being generous, as AppLovin's multitude of UX gimmicks. We believe these gimmicks are now unquestionably malicious, and the Company's backdooring of direct installations into partners' apps is tantamount to malware and in clear violation of Google Play's Device and Network Abuse policy, which explicitly forbids *"apps that install other apps without the user's prior consent"*. Accordingly, we intend to write an open letter to Google Play and Google Play creators, addressing concerns regarding policy violations and risks that could potentially affect up to the 1.4 billion daily active users that AppLovin's ads currently reach.[3]

We provide a case study that encapsulates many aspects of the problematic practices and self-perpetuating feedback loops that have driven AppLovin's recent performance.

- First, we uncovered complaints alleging that one mobile game, Animal Restaurant (10M+ installations) had *"automatically installed an app"* named "Bricks n Balls. (10M+ installations). The user reported that they *"only realized it happened because I got a notification that said 'click to launch."*

- Our review of Animal Restaurant's APK confirms that the app contains the "Bind to AppHub" permission, allowing the ads in that game to initiate direct installations.

- The app that was allegedly illicitly installed, Bricks n Balls, was then-owned by AppLovin's own studio, PeopleFun. **Reviews for Bricks n Balls then allege that very same app will also *"automatically install [additional apps] without your consent."*[4]** Finally, third-party install data for Bricks n Balls reveals what we view as an otherwise highly anomalous pattern, with two massive spikes in installations, concentrated among Android users in Brazil in May 2023 and in India in September 2023 – almost immediately following new Array partnerships (Samsung and OPPO, respectively) in those regions.

[2] We also engaged Dr. Ben Edelman – renowned ad fraud researcher, previous HBS faculty member, and later a Chief Economist at Microsoft – who confirmed that we had come to the correct understanding of the code's abilities and practical functioning.

[3] We also note that Android users may simply disable AppHub in their Android phone's settings or list of apps if they wish to do so, as disclosed in Array's terms of service.

[4] That particular review has 240 upvotes; these reviews are rampant.

One AdTech industry executive told us:

> *"**I'm almost certain that what they're doing is a Ponzi scheme...** It's junk inventory, junk apps... They've changed recently... It's kicked you out of the app and forced you to download the other app via the ad. Then when you log back in, it counts you again, so it shows you as a repeating user, but in reality it's a really poor experience. It's dirty metrics."* – AdTech Industry Executive

We believe these silent, backdoor installations are happening on an unprecedented scale.

- Don't just take our word for it. Multiple current and former AppLovin employees are bragging about the massive success of the program in plain sight. **AppLovin's former Head of Product for Array publicly and explicitly refers to *"the ad product for Direct Download"* as *"the company's top revenue driver."*** AppLovin's current Senior Director of Strategic Partnerships describes an agreement with Samsung *"to expand app recommendation and direct download services...valued at $1 billion over 4 years..."* He also publicly confirmed the ability to *"install mobile applications directly without the need for an app store."* Finally AppLovin's technical lead for Array calls out *"direct downloads for instant access to games from ads"* as a key functionality.

- User complaints are widespread. Our report details a litany of grievances: *"my phone just started installing random apps to my secure folder"; "the games automatically download to the device when the ads are tapped... WITHOUT YOUR CONSENT"; "three times now I've gotten that ad for Tower War and any 30 seconds after the ad is over I get a push notification that Tower War has finished installing..."* Others simply refer to AppHub as *"pure cancer."*

- We also find it puzzling that in June 2024, Array updated its privacy policy to include a new section on "Direct Download Services." This is the only material change that we see from the previous April 2023 version, and yet if this feature was always inherent to Array's existence, why the update?

We Believe AppLovin's e-Commerce Push is a Smoke and Mirrors Game, Rigged from the Start, and Likely to Collapse Under Meta-Related or Expansion-Related Scrutiny

AppLovin has now attempted to parlay its mobile gaming promotion into e-commerce. Yet here we also believe the true drivers of AppLovin's claims to outperformance have resulted from the Company having effectively "rigged the game" in their favor to wildly overstate true results to advertisers.

AppLovin CEO Adam Foroughi: Advertising God? A Different "G-Word" Comes to Mind

AppLovin bulls have arrived at the mistaken conclusion that AppLovin CEO Adam Foroughi is something akin to an AdTech God. We'd use a different "G-word" to better describe his now 20+ years of AdTech-related exploits.

- From March 2004 to July 2004, Foroughi worked at Claria Corporation, previously known as Gator Corporation. Gator created a software that was *"notorious as **one of the first widespread spyware applications."*** Spyware displays and/or silently downloaded advertising to a users' personal computer. According to a 2005 Adweek article, Gator's distribution of this adware was spearheaded by Mitchell Weisman, who was Foroughi's direct boss and mentor at Gator/Claria, according to Foroughi himself.

- Foroughi left alongside Weisman and ousted Gator CEO Jeff McFadden, the group then founding LifeStreet Media, where Wiesman remains chairman today.

- In 2008, Foroughi left LifeStreet to create an ad-serving company called Social Hour, alongside eventual AppLovin co-founder Andrew Karam. Foroughi served as CEO of Social Hour from August 2008 to July 2010. **In June 2009, Facebook banned Social Hour from advertising on its platform entirely, citing "deceptive content" that "posed a potential threat"** to their users' experience.

At AppLovin, Foroughi has now stacked the deck with former colleagues.

- AppLovin co-founder and VP of Product Andrew Karam worked at Lifestreet, Style Page, and Social Hour, all founded by Foroughi. Karam was also a manager of Mingle Media Corp, Foroughi's failed attempt at a dating service business.

- Current AppLovin Director Eduardo Vivas co-founded Social Hour, while AppLovin's co-founder, former CTO, and major shareholder John Krystynak was formerly the CTO of Social Hour.

- AppLovin's GM of New Initiatives Rafael Vivas was Director of Business Development at Social Hour. He is also the brother of Eduardo Vivas.

- Current Applovin Finance and Accounting executive Patrick McNenny previously served as VP of Finance at Lifestreet for 10+ years.

In the LTM, insiders have sold nearly $2.0 billion in stock, while KKR has dumped the entirety of its remaining $7.3 billion stake. We are short AppLovin and believe shares are headed lower.

AppLovin Claims AI Has Fueled Its Turnaround, But Can't Explain How

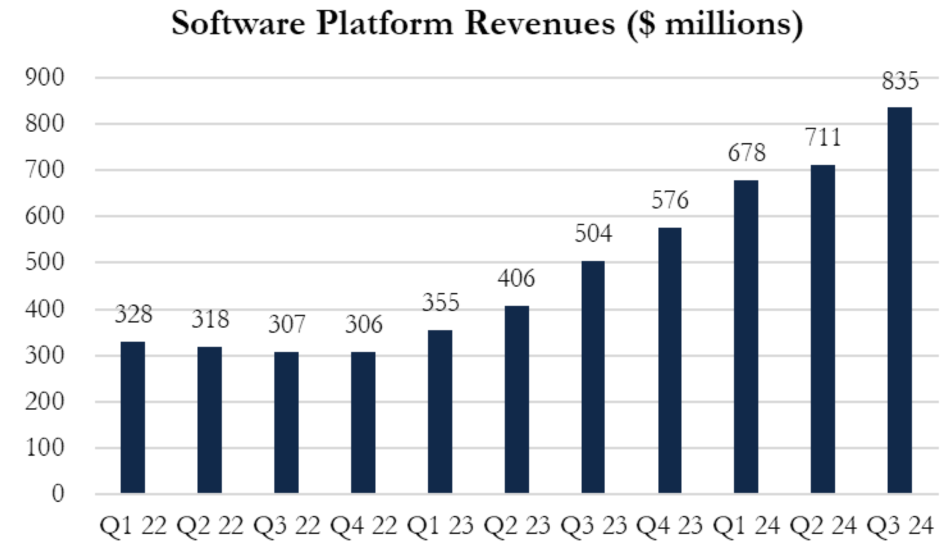
AppLovin was founded in 2012 as a mobile advertising technology business. The Company's core platform is AppDiscovery ("AD"), which contributed 67% of the Company's YTD revenues and now effectively represents the entire business after accounting for the Company's agreement to sell its Apps business earlier this month.

AppDiscovery works by *"matching advertiser demand with publisher supply through auctions at vast scale and at microsecond-level speeds."* AD connects app developers – who are good at making games but bad at getting people to play them – to new users by running programmatic advertising auctions. AppLovin generates revenues primarily on a per-installation basis; the Company reports percentage growth (but not standalone values) in both installations and revenues per installation each quarter.

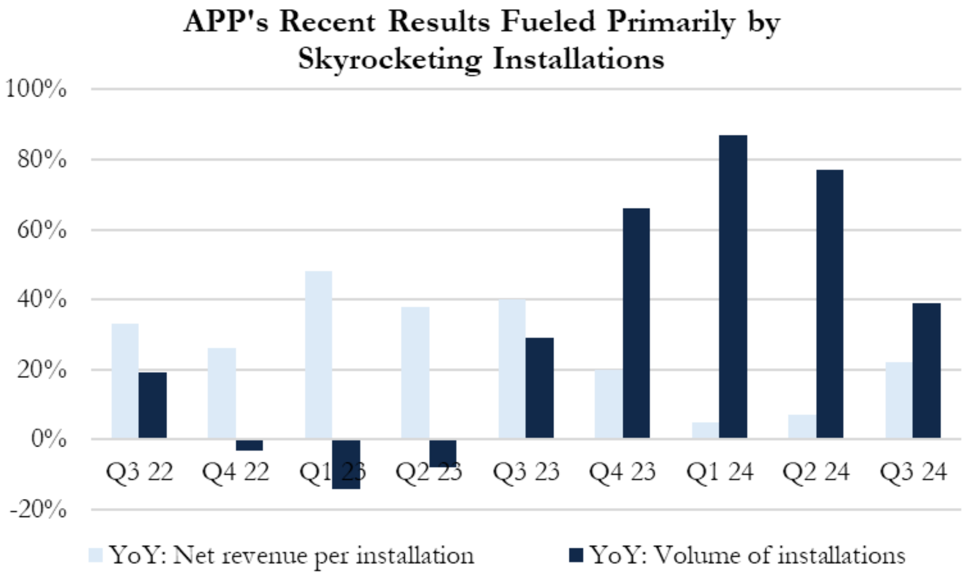
AppDiscovery has historically been shackled to the casual and hyper-casual mobile gaming ecosystem. Mobile game developers buy ad space *within other games* to drive installations of their own games. They then monetize these newly acquired users primarily by *re-selling* ad space within those games to yet another gaming operator. The shelf lives of these games are often extremely short – one studio described to us that they look to a 7-day user shelf life. Developers rest in the hope that their games eventually achieving organic virality, by which they bring in higher revenues through either in-app purchases or higher-valued advertising.

> *"95% of the advertisers are feeding it back into AppLovin... It's a pretty incestuous relationship."*
> – Former AppLovin Employee (1)
>
> *"Over 80% of the ads are spent on other mobile games... There are certainly a lot of losers in this casino."* – Former AppLovin Executive (3)

APP claims to have an edge in driving installs more effectively, leveraging years of accumulated data on buyers, sellers, and users, as well as insights from its other businesses. The Company refers to AppDiscovery's underlying technology as AXON. In Q2 2023, APP launched AXON 2.0, which includes *"cutting-edge AI technologies"* and which the Company credits as the primary driver of its recent success.[5]



AppLovin's Software Platform has surged since Q1 2023. Installation volumes are the primary driver, up 115% while revenue per installation has grown just 28%. This growth is especially striking given the broad decline in mobile game installations. SensorTower reports a 6% decline last year. **It is also critical to recognize that 84% of mobile gaming applications are installed to Google Play devices – AppLovin lives and breathes on this ecosystem.**[6]



Yet both the scale and speed of AppLovin's "AI-driven" turnaround has been shocking; AXON 2.0 was brought to market in less than a year. One former AppLovin engineer we spoke with suggested that management only

[5] CEO Foroughi, Q1 2024 earnings call, May 8, 2024

[6] SensorTower, worldwide installations in 2024.

became interest in AI began after seeing the successes of OpenAI and NVIDIA, *"with the whole AI stocks thing."* The former engineer also found it worthwhile to tell us that the Company had *"wanted to do all this NFT stuff too..."* We remind readers that AppLovin also launched an NFT marketplace called "Vessel" in October 2022. Vessel's website is now defunct.

Over the past 2 years, AppLovin CEO Adam Foroughi has never fully described what makes AppLovin's AXON 2.0 platform so unique.[7] When asked directly, Foroughi has either hidden behind the *"black box"* label, or rambled on about culture.

> **AppLovin Q4 2023 Earnings Call, February 14, 2024**
>
> William Blair Analyst Ralph Schackart: *"We get the question all the time in simple terms, if you could explain what's the main difference from AXON 2 versus AXON 1. Maybe just for simplicity sake, for investors sort of frame what's the biggest change or observation you see on your end?"*
>
> AppLovin CEO Foroughi: *"**Yes, it's just better**. I mean just the technology is built to scale better, it's more efficient, more effective. These are predictive technologies at the end of the day... what we can't see in **a black box algorithm** is a type in and a result... there's a whole bunch of predictions along the way, and AXON 2 makes them better than the prior version. And that creates a lot of efficiency gain, both for our business and that of our partners."*
>
> **51st NASDAQ London Investor Conference, December 11, 2024**
>
> Morgan Stanley Analyst Matthew Cost: *"So we've seen an extraordinary inflection in the growth of your business over the past 2 years. And I want to pose a question that I hear from investors quite often as they're ramping on your company. What have you built in AppLovin that's driven this outperformance? And what differentiates it from your competitors?"*
>
> AppLovin CEO Foroughi: "***So I talk a lot about culture***, *and I think this is one of the main differentiators. And our culture seems to me to be different from a lot of other technology companies that have scaled. And it's predicated on a concept that I've built multiple companies, and I want to work with builders. And people who build companies tend to want to work at small early-stage businesses. And I never understood why these same people who have exceptional ability end up churning out of companies when those companies scale. Why does companies become less efficient when they scale? Why is there more process when companies scale So we wanted to build a culture that inspired that same entrepreneurial spirit as it scaled, and that is predicated on building a team of doers, getting process out of their way and allowing them to execute as if the company was still 10 people. And we pride ourselves on being able to do this now at a very large scale."*

Investors have seemingly become content with these responses, and in fact have cheered them on as the very same "black box" now underpins the Company's e-commerce aspirations. But we believe AppLovin's success isn't a black box at all – it's glass, and its vile contents are plainly visible.

The Glass Box: AppLovin's Backdoor One-Click "Direct Download" Program

We believe AppLovin's success has been driven not by AI, but by the systematic integration and exploitation of notoriously dangerous app permissions that silently trigger backdoor app installations. **In honor of those who came before us: we think this is the AdTech equivalent of "the truck rolling down the hill."** Our research

[7] Former AppLovin employees and partners we spoke with couldn't articulate what apparently made AXON 2.0 so different, either. One said, *"I couldn't tell you why. It's a mystery even for me."* Another said, *"I'd only be hypothesizing on that because I don't know."*

details the exact step-by-step process by which we believe AppLovin has executed this scheme over the past 2 years. There are three major elements.

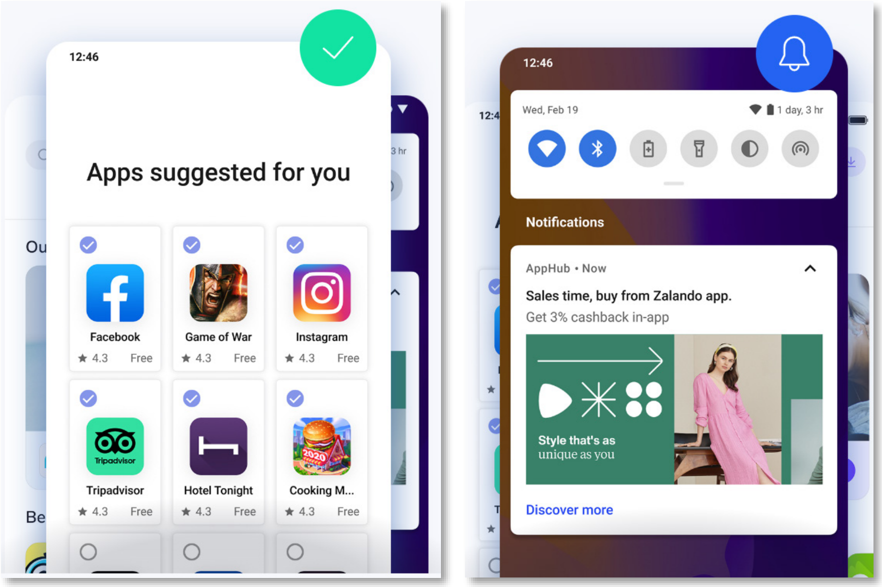
- In late 2022, AppLovin launched Array, an internal initiative whereby AppLovin partners to mobile phone carriers and OEMs including T-Mobile/Sprint, Samsung, OPPO, RealMe, TCL, Xiaomi, and Sliide. Array in turn offers "AppHub" to OEMs, a system-level software that is pre-loaded directly onto new devices. AppLovin markets AppHub as a platform that helps new phone owners easily install their favorite apps upon device setup. As such, **AppHub is granted unique permissions that enable it to initiate direct installations of third-party apps from outside of the Google Play store, upon just a single click**.

- Since Array's late 2022 launch, AppLovin has smuggled "AppHub binding" permissions into thousands of both its own and its partners' apps. **When binding to AppHub, these apps inherit AppHub's permissions, allowing the apps *themselves* to initiate installations of third-party apps from outside of the Google Play store, again upon just a single click.**

- **AppLovin apps then hijack these binded AppHub permission to force-feed illicit app installations,** often without user knowledge or explicit consent. This not only inflates the Company's reported installation volumes and revenues at 100% incremental margins, but opens the door for bad actors. We provide direct proof of all of this in the pages that follow.

Part 1: AppLovin's Obtains Notoriously Powerful, System-Level "Direct Download" Permissions via Array's Partnerships with OEMs and Carriers

In 2022, AppLovin launched Array, an internal initiative which the Company characterized as, "*a software solution that enables mobile manufacturers (OEMs) to unlock increased monetization opportunities throughout the device lifecycle.*"



Sales time, buy from Zalando app.
Get 3% cashback in-app

Source: AppLovin Array

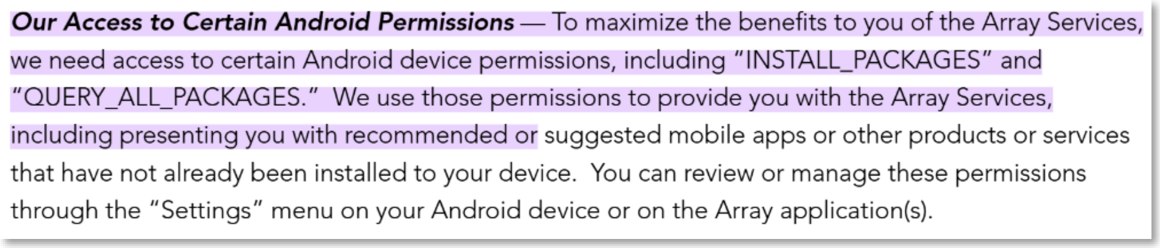
In layman's terms, AppLovin claims that Array was spun up to show ads on the users phone (e.g. in notifications), and to preload certain relevant apps when the user first unboxes their device. For the latter purpose, Array, and by extension, AppHub, is automatically granted certain permissions including:

QUERY_ALL_PACKAGES

and

INSTALL_PACKAGES

These permissions are disclosed in Array's Terms & Conditions:



Our Access to Certain Android Permissions — To maximize the benefits to you of the Array Services, we need access to certain Android device permissions, including "INSTALL_PACKAGES" and "QUERY_ALL_PACKAGES." We use those permissions to provide you with the Array Services, including presenting you with recommended or suggested mobile apps or other products or services that have not already been installed to your device. You can review or manage these permissions through the "Settings" menu on your Android device or on the Array application(s).

Source: Terms & Conditions

While these permissions have been granted to AppHub, **the Google Play store restricts the use of these permissions within standardized apps**, deeming them "high risk" and "sensitive" so as to prevent this very sort of conduct from occurring. Anecdotal reports suggest Google bans third-party apps found with such permissions.

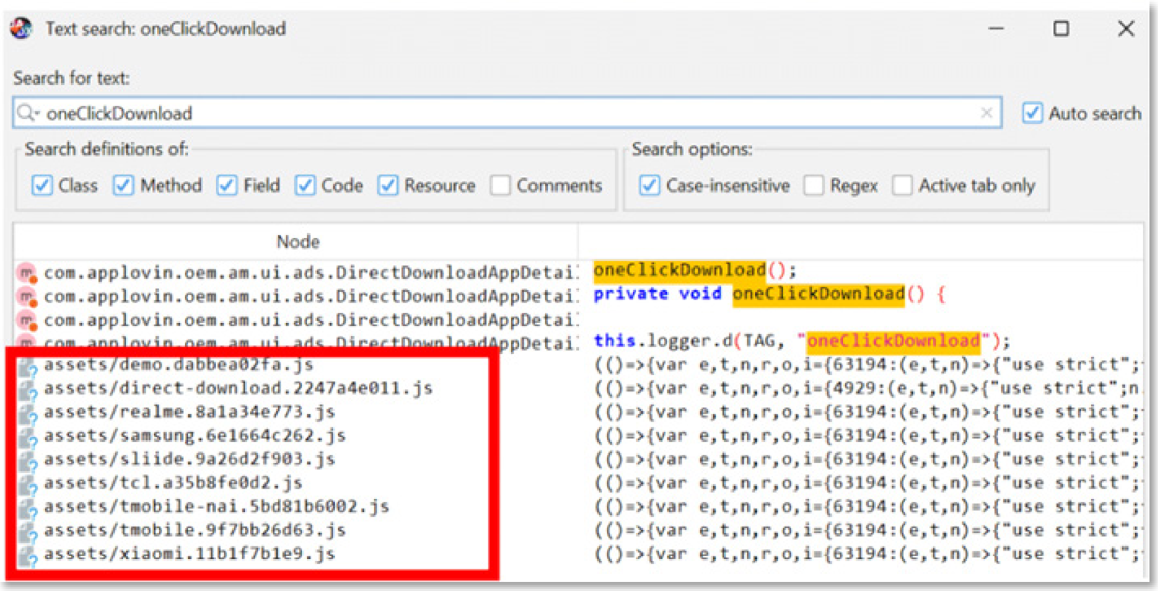
Since its introduction in 2022, AppLovin disclosed certain agreements with three partners.

- In 2022, AppLovin began with Sprint/T-Mobile.

- In May 2023, AppLovin announced that "Array Extends Global Partnership with OPPO to Deliver Best-in-Class Mobile App Recommendations For Users."

- In September 2023, AppLovin disclosed in a blog post that "*AppLovin Array **Expands** Samsung Partnership in LATAM, Launching On Samsung Devices in Brazil."* This was the first mention we can find of Array's relationship with Samsung, despite the language implying a pre-existing relationship.

We decompiled AppHub's code and uncovered a function named oneClickDownload that appears to initiate AppLovin's "Direct Download" function. We searched for all mentions of this function and discovered asset file references that name what appear as additional carriers and OEMs including RealMe, Sliide, TCL, and Xiaomi.



Search for text: oneClickDownload ☑ Auto search

Search definitions of: ☑ Class ☑ Method ☑ Field ☑ Code ☑ Resource ☐ Comments

Search options: ☑ Case-insensitive ☐ Regex ☐ Active tab only

```
Node
com.applovin.oem.am.ui.ads.DirectDownloadAppDetai  oneClickDownload();
com.applovin.oem.am.ui.ads.DirectDownloadAppDetai  private void oneClickDownload() {
com.applovin.oem.am.ui.ads.DirectDownloadAppDetai
com.applovin.oem.am.ui.ads.DirectDownloadAppDetai  this.logger.d(TAG, "oneClickDownload");
assets/demo.dabbea02fa.js                          (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/direct-download.2247a4e011.js               (()=>{var e,t,n,r,o,i={4929:(e,t,n)=>{"use strict";n
assets/realme.8a1a34e773.js                        (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/samsung.6e1664c262.js                       (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/sliide.9a26d2f903.js                        (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/tcl.a35b8fe0d2.js                           (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/tmobile-nai.5bd81b6002.js                   (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/tmobile.9f7bb26d63.js                       (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
assets/xiaomi.11b1f7b1e9.js                        (()=>{var e,t,n,r,o,i={63194:(e,t,n)=>{"use strict";
```

Source: AppHub v1.17.2 code, available here[8]

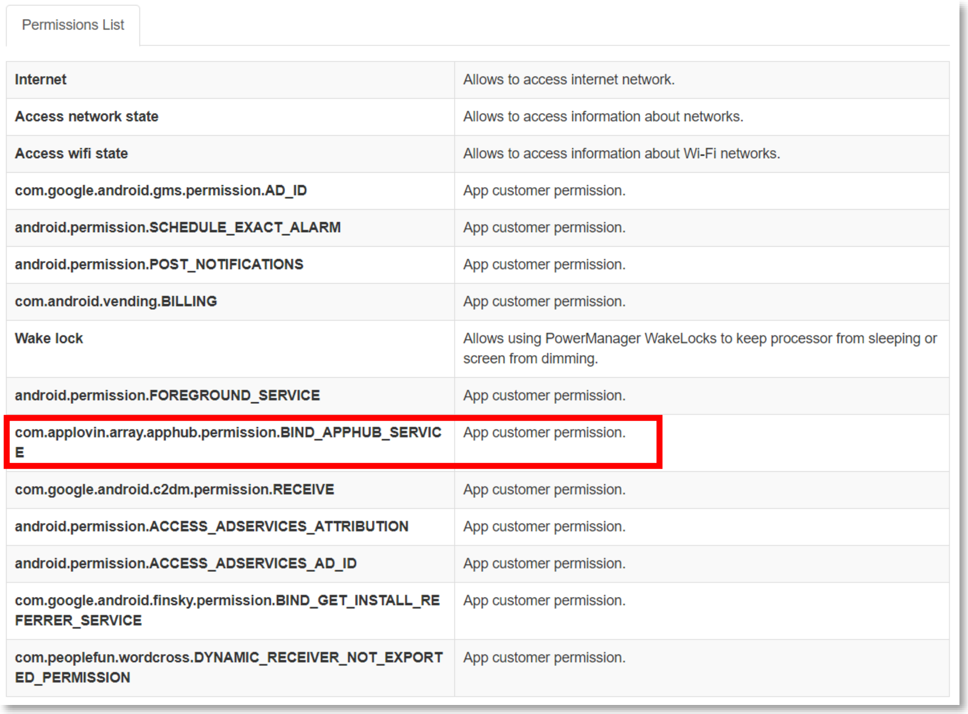
It seems odd to us that AppLovin seems to have formed, and yet never disclosed these additional partnerships. Similarly, AppLovin called out Array in each one of its quarterly earnings calls from Q2 2022 through Q4 2023, but has never mentioned Array in any call since – even as CFO Matt Stumpf called out seeing *"early contributions from our Array business"* on that Q4 2023 call. **As such, investors have remained totally in the dark as to how many devices around the world now contain such powerful permissions.**

Part 2: AppLovin Smuggles Binding Permissions Into Apps via AppLovin SDKs

Our review of app code among a variety of top AppLovin-owned or MAX customer apps reveals that since at least November 2022, AppLovin has smuggled a new permission into the apps by way of SDK updates. See for example from "Wordscapes" from PeopleFun – one of AppLovin's now former studios.

"com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE"

[8] We also see that AppHub's APK includes packages that reference the OEMs and carriers by name.



Permissions List

Internet	Allows to access internet network.
Access network state	Allows to access information about networks.
Access wifi state	Allows to access information about Wi-Fi networks.
com.google.android.gms.permission.AD_ID	App customer permission.
android.permission.SCHEDULE_EXACT_ALARM	App customer permission.
android.permission.POST_NOTIFICATIONS	App customer permission.
com.android.vending.BILLING	App customer permission.
Wake lock	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.
android.permission.FOREGROUND_SERVICE	App customer permission.
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	App customer permission.
com.google.android.c2dm.permission.RECEIVE	App customer permission.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	App customer permission.
android.permission.ACCESS_ADSERVICES_AD_ID	App customer permission.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	App customer permission.
com.peoplefun.wordcross.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	App customer permission.

SDKs are not inherently problematic. For example, Instagram permissions allow it to take photos with the phone's camera, rather than users being forced to import photos manually. Yet when binding to AppHub, AppHub effectively lends *its own permissions* to these apps – **including the permission to initiate direct downloads outside of the Google Play store.**

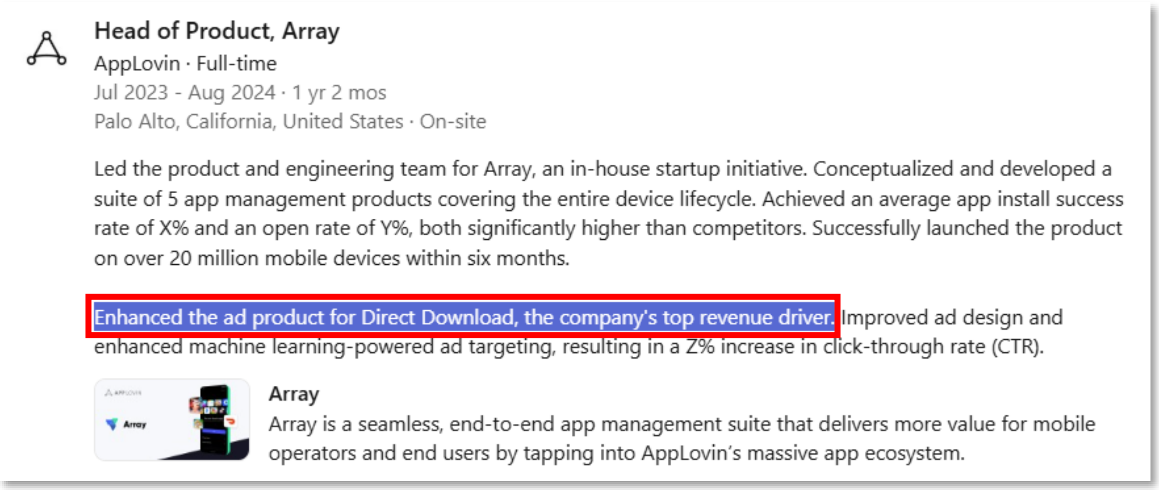
Our review of apps across both AppLovin's previously owned studios and studio partner network reveals that the permission has been added to thousands of apps since late 2022. These apps include some of the most popular games in the world, including Subway Surfers, 8 Ball Pool, Wordscapes, and Angry Birds, representing billions in lifetime installations.[9] We provide a sample of additional apps that have now integrated the permission, focusing on games developed by AppLovin's (now formerly) owned and partnered studios.[10]

[9] Readers can check the permissions by downloading the APK and examining manually, or more easily in the APKpure links provided, by clicking the "download" button, then navigating to the "Permissions" hyperlink, which will then display the relevant "com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE" permission.

[10] By contrast and for absence of doubt, the AppHub binding permission has not been integrated widely into what we'd consider more reputable apps such as Facebook, Instagram, ChatGPT, or even Roblox – these apps have no apparent need to trigger third-party downloads from outside of the Play store.

Name of Game	Type	Update Version	Date	Play Store Downloads	Source
Mr Bullet	Owned	5.24.0	Nov-22	100M+	APKPure
Prison Break Story	Customer	1.40.0.0	Nov-22	100M+	APKPure
Worms Zone	Customer	4.1.2-b	Nov-22	100M+	APKPure
Bermuda Adventures Farm	Owned	1.7.3	Nov-22	10M+	JADX
High Heels!	Customer	3.7.9	Nov-22	100M+	APKMirror
Dream League Soccer 2024	Customer	10.0.0	Dec-22	100M+	APKMirror
Clockmaker: Jewel Match 3	Owned	69.0.0	Jan-23	10M+	JADX
Johnny Trigger	Customer	1.12.24	Feb-23	100M+	APKPure
Bricks N Balls	Owned	3.15.3	Feb-23	10M+	JADX
Sand Balls	Customer	2.3.27	Feb-23	100M+	APKMirror
Paper.io 2	Customer	2.3.6.1	Feb-23	100M+	APKMirror
Mob Control	Customer	2.50.1	Mar-23	100M+	APKMirror
Helix Jump	Customer	5.3.2	Mar-23	100M+	APKMirror
Twerk Race 3D	Customer	1.47.1	Mar-23	100M+	JADX
West Game	Customer	5.1.0	Mar-23	10M+	APKMirror
Project Makeover	Owned	2.60.1	Mar-23	100M+	APKMirror
Tangle Master 3D	Customer	42.9.91	May-23	100M+	APKMirror
Count Masters: Stickman Games	Customer	1.56.2	Jul-23	100M+	APKPure
Coin Master	Customer	3.5.1840	Oct-24	100M+	APKMirror
Woody Block Puzzle	Customer	3.1.3	unknown	10M+	JADX

We don't believe there's any reason for AppLovin-affiliated apps to bind to AppHub – except to push installations. **Indeed, current and former AppLovin employees boast in plain sight not only about the Company's ability to download games directly from ads, but that *"the ad product for Direct Download"* is *"the company's top revenue driver."***



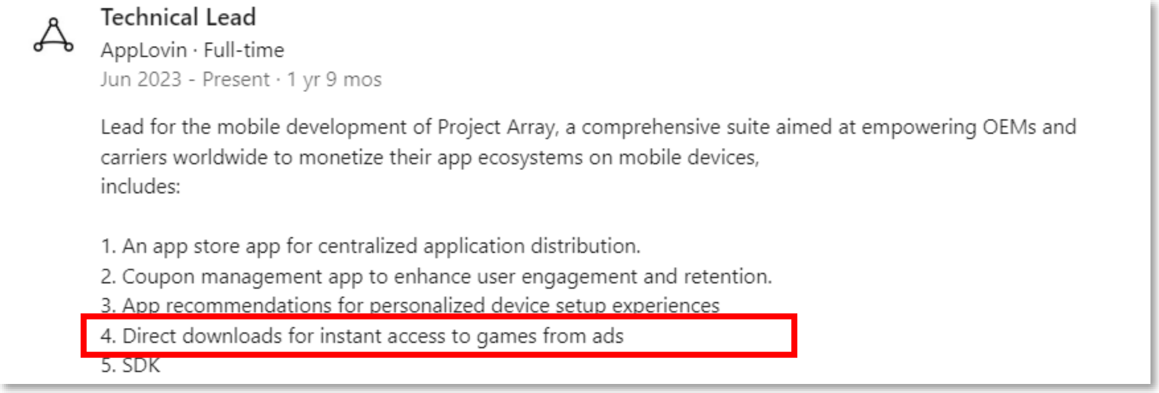
Head of Product, Array
AppLovin · Full-time
Jul 2023 - Aug 2024 · 1 yr 2 mos
Palo Alto, California, United States · On-site

Led the product and engineering team for Array, an in-house startup initiative. Conceptualized and developed a suite of 5 app management products covering the entire device lifecycle. Achieved an average app install success rate of X% and an open rate of Y%, both significantly higher than competitors. Successfully launched the product on over 20 million mobile devices within six months.

Enhanced the ad product for Direct Download, the company's top revenue driver. Improved ad design and enhanced machine learning-powered ad targeting, resulting in a Z% increase in click-through rate (CTR).

Array
Array is a seamless, end-to-end app management suite that delivers more value for mobile operators and end users by tapping into AppLovin's massive app ecosystem.

Source: LinkedIn



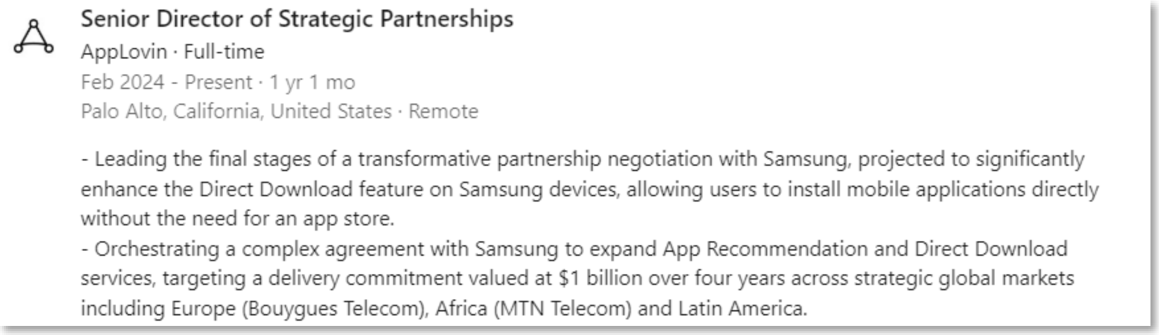
Technical Lead
AppLovin · Full-time
Jun 2023 - Present · 1 yr 9 mos

Lead for the mobile development of Project Array, a comprehensive suite aimed at empowering OEMs and carriers worldwide to monetize their app ecosystems on mobile devices,
includes:

1. An app store app for centralized application distribution.
2. Coupon management app to enhance user engagement and retention.
3. App recommendations for personalized device setup experiences
4. Direct downloads for instant access to games from ads
5. SDK

Source: LinkedIn

AppLovin's current Senior Director of Strategic Partnerships also confirms the ability to download games "without the need for an app store" **and touts a potential Samsung expansion deal worth $1 billion.**[11]



Senior Director of Strategic Partnerships
AppLovin · Full-time
Feb 2024 - Present · 1 yr 1 mo
Palo Alto, California, United States · Remote

- Leading the final stages of a transformative partnership negotiation with Samsung, projected to significantly enhance the Direct Download feature on Samsung devices, allowing users to install mobile applications directly without the need for an app store.
- Orchestrating a complex agreement with Samsung to expand App Recommendation and Direct Download services, targeting a delivery commitment valued at $1 billion over four years across strategic global markets including Europe (Bouygues Telecom), Africa (MTN Telecom) and Latin America.

Source: LinkedIn

[11] This is not to be taken as "$1 billion" in illicit installations; we believe this figure was likely cited in reference to "initial unboxing" type direct downloads. Yet we believe both the apparent materiality of the potential deal and its nature make it worthy of further disclosure by AppLovin.

Our code review demonstrates the exact steps by which apps initiate direct downloads, and we present extensive evidence suggesting that this has happened across many high-grossing AppLovin-owned or affiliated apps. Nevertheless, we anticipate that investors and/or the Company might argue that the binding permission was smuggled in not to force-feed installations, but to utilize some other bit of AppHub's technology to improve in-app advertisements. Yet CEO Foroughi himself has repeatedly described this relation in *exactly the opposite way* – AppLovin integrated AXON 2.0 *into AppHub* to improve AppHub's recommendation abilities, not vice versa.

> *"Additionally, this quarter, we'll be extending AXON 2 to Array and expect it will materially accelerate the potential to scale that business."*
> – CEO Adam Foroughi, Q3 2023 earnings call, November 8, 2023

The existence of the permissions proves their purpose, and our research suggests they've been exploited at scale.

Our Review of Code Details The Step-by-Step Process Whereby Apps Themselves Initiate Installations From Outside of the Play Store with a Single Ad Click, Outside of Google Play Store

The following describes a summary of the mechanics by which AppLovin allows apps to bind to AppHub and initiate downloads. Readers who are uninterested in this process can feel free to skip ahead, while readers who are interested in seeing more comprehensive details can find them in the Appendix.

1. Ads use classes AppLovinAdServiceImpl and AppLovinAdBase. When an app shows an ad, it requests an ad from AppLovin through AppLovinAdServiceImpl.

2. AppLovinAdServiceImpl loads the ad, which is an instance of a class of type AppLovinAdBase.

3. AppLovinAdServiceImpl listens for a user click event on an advertisement via the functions trackAndLaunchVideoClick and trackAndLaunchClick

4. AppLovinAdClickListener appears to be invoked when an ad is clicked. Importantly, we do not find anything to suggest that any particular place within the ad must be clicked – it can be anywhere.[12]

5. When a user clicks on an ad – as determined by AppLovinAdClickListener – it initiates startDirectInstallOrDownloadProcess with a new ArrayService object.

6. ArrayService then creates an intent to bind to an "AppHubService." The app binds to AppHub.

7. StartDirectInstallOrDownloadProcess then checks: is "isDirectDownloadEnabled" true?

8. **If so, then the function installs the advertised app via ArrayService's connection to AppHub.**

Further, we engaged Dr. Ben Edelman – renowned ad fraud researcher, previous HBS faculty member, and later a Chief Economist at Microsoft – to ensure our correct understanding of the code's abilities and practical functioning. In Dr. Edelman's words:

> *"It is difficult to conceive of a proper purpose, within the expected/legitimate functioning of AppHub, why a game would need to bind to Apphub. But if AppLovin wants to use Apphub to install additional apps/games when its SDK is embedded within some other game or app A, it seems that game A would need to include this binding among its permissions.*

[12] As we describe on pages 25 and 26, we believe that this is the exact mechanism by which AppLovin's well-documented tactics to inflate CTRs has translated to inflated installs.

> *The source code contains repeated references to direct download. The context and architecture of this code indicate that it performs the type of download described above.*
>
> *The AppLovinAdServiceImpl loads, then listens for a user click. A click is handled via trackAndLaunchVideoClick and trackAndLaunchClick. Those functions check whether isDirectDownloadEnabled. If so, execution proceeds to startDirectInstallOrDownloadProcess which passes control to an Apphub/Array DirectDownloadListener which downloads the file as the name suggests.*
>
> *...it's not routine for an Android app to download and install arbitrary other apps, because the standard Android security architecture doesn't allow this."*

Edelman also brought our attention to an element of the code that we had previously overlooked – the code indicates that an installation is prompted only if a "download token" is sent by AppLovin to the SDK within the application. Edelman suggested that this element allows AppLovin to "flip the switch" on direct downloads based on any number of parameters. He added that if AppHub were truly functioning solely as AppLovin describes it, there would not only be no such need for the permission, but no such need for this token.

> *"**This architecture allows AppLovin to condition a direct download on any information known to the server as it sends the ad to the client**. This certainly allows AppLovin to end all direct downloads on a moment's notice—as it is likely to do if it faces public criticism of this practice, and crucially without waiting for app updates to propagate. It certainly allows AppLovin to target direct downloads by IP address, such as never performing direct downloads to countries or regions deemed high-risk. I am confident that a request for an ad includes which app/game the user is playing and probably a user ID that can be connected back to the user's prior activity (prior duration of play, ads shown, ads clicked, other apps installed). No doubt device type (make and model, screen resolution, etc.)...*
>
> *The use of the "token" architecture is fairly read as indicating knowledge that direct download is a sensitive function and might need to be scaled back or limited in some important way, including on short notice. In general app developers use tokens for capabilities they want to importantly restrict, and when they anticipate wanting to impose restrictions in the future. **In contrast, for a fundamental capability that is offered indefinitely and without limitation, to all users all the time, there is no need for a token architecture or associated security and complexity**."*

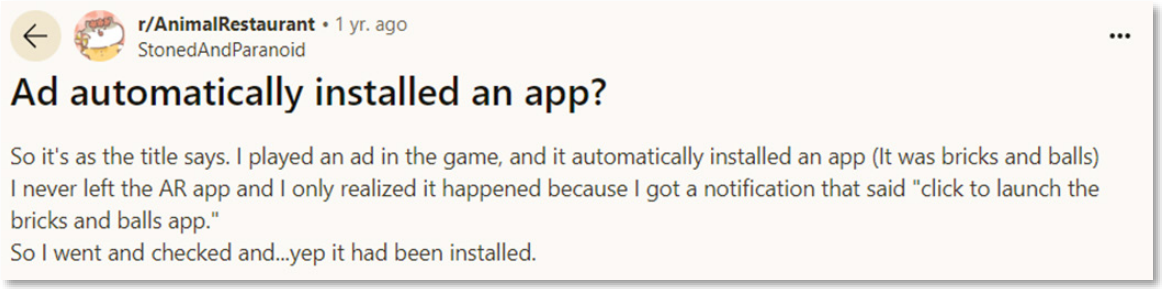
Part 3: Exploit One-Click Direct Download Permissions to Drive Installations

We believe these permissions have been exploited to drive installation volumes higher over the past 2 years. Our view is based on (a) user complaints of automatic downloads prompted by AppLovin-integrated apps, (b) user complaints of unwanted app downloads from customers of Array's OEM and carrier partners, (c) app download data that in our view exhibits patterns consistent with force-fed downloads, and (d) characterizations from AppLovin's own employees, who refer for example to *"the ad product for direct download"* as *"the company's top revenue driver."*

Case Study: "Animal Restaurant" (Allegedly) Pushed Installations of AppLovin App, "Bricks n Balls" in Brazil and India – Immediately After Array Formed Partnerships in Those Regions

We provide a case study which encapsulates many aspects of what we believe has happened across AppLovin's network. In this case:

- A user complained that while playing the Animal Restaurant app, which our checks show contained the relevant binding permission, the app *"automatically installed an app"* called "Bricks n Balls."

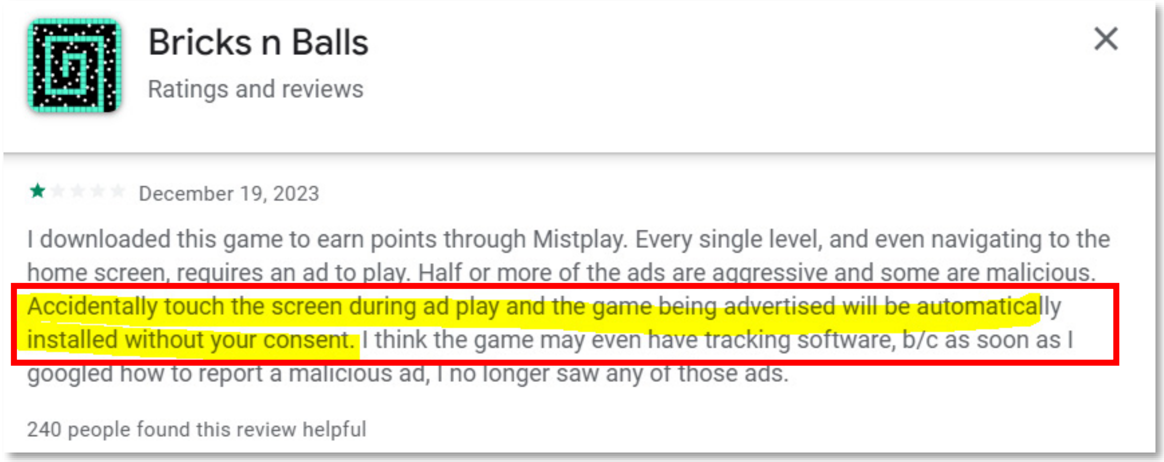


r/AnimalRestaurant • 1 yr. ago
StonedAndParanoid

Ad automatically installed an app?

So it's as the title says. I played an ad in the game, and it automatically installed an app (It was bricks and balls)
I never left the AR app and I only realized it happened because I got a notification that said "click to launch the bricks and balls app."
So I went and checked and...yep it had been installed.

- Bricks n Balls was owned by AppLovin through the Company's PeopleFun subsidiary.[13] Reviews for the app allege *that it is also being used* to download *additional* third-party apps *"without consent"*, perpetuating the illicit download cycle.



Bricks n Balls
Ratings and reviews

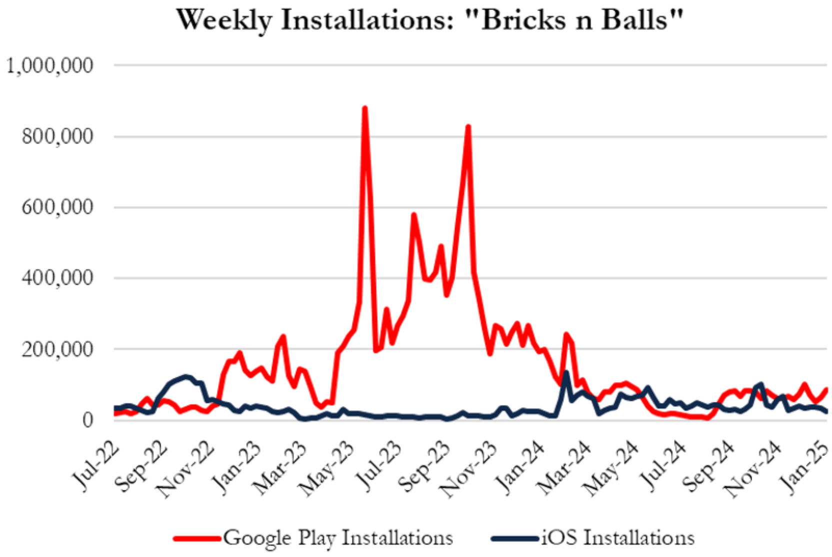
★☆☆☆☆ December 19, 2023

I downloaded this game to earn points through Mistplay. Every single level, and even navigating to the home screen, requires an ad to play. Half or more of the ads are aggressive and some are malicious. Accidentally touch the screen during ad play and the game being advertised will be automatically installed without your consent. I think the game may even have tracking software, b/c as soon as I googled how to report a malicious ad, I no longer saw any of those ads.

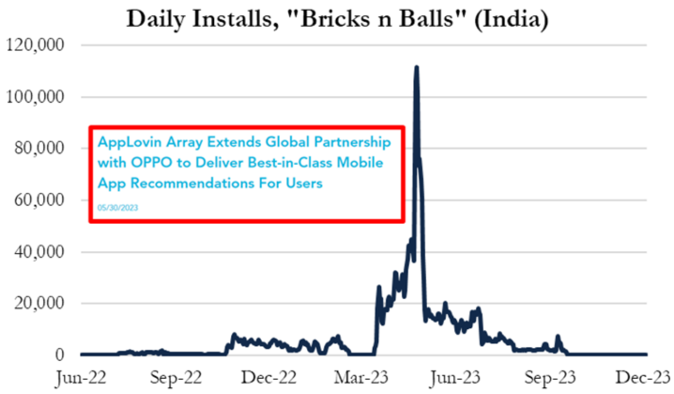
240 people found this review helpful

- Third-party download data for Bricks n Balls reveals what we view as an otherwise highly anomalous pattern that exhibits a spike in installations in both May 2023 and the Fall of 2023, coinciding with user complaints. Moreover, spikes were seen only among Android users, and not among iOS users.

[13] AppLovin formed an agreement to sell its apps business in February 2025.

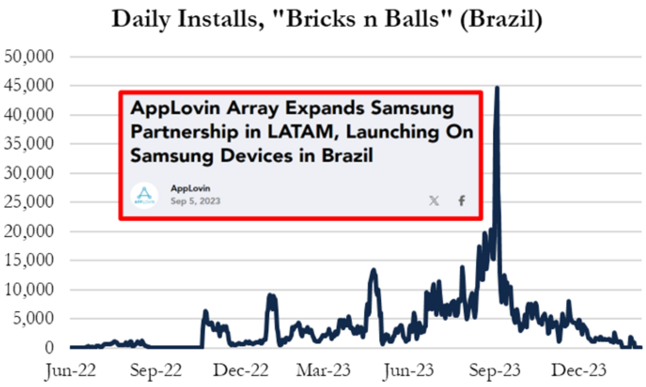

Weekly Installations: "Bricks n Balls"

- Finally, and perhaps most importantly, these installations were especially concentrated in Brazil (in May 2023) and in India (in September 2023) – immediately after Array formed partnerships with OEMs and carriers in these regions, suggesting that the downloads were enabled by AppHub integration onto devices concentrated in these regions.


Daily Installs, "Bricks n Balls" (India)

AppLovin Array Extends Global Partnership with OPPO to Deliver Best-in-Class Mobile App Recommendations For Users

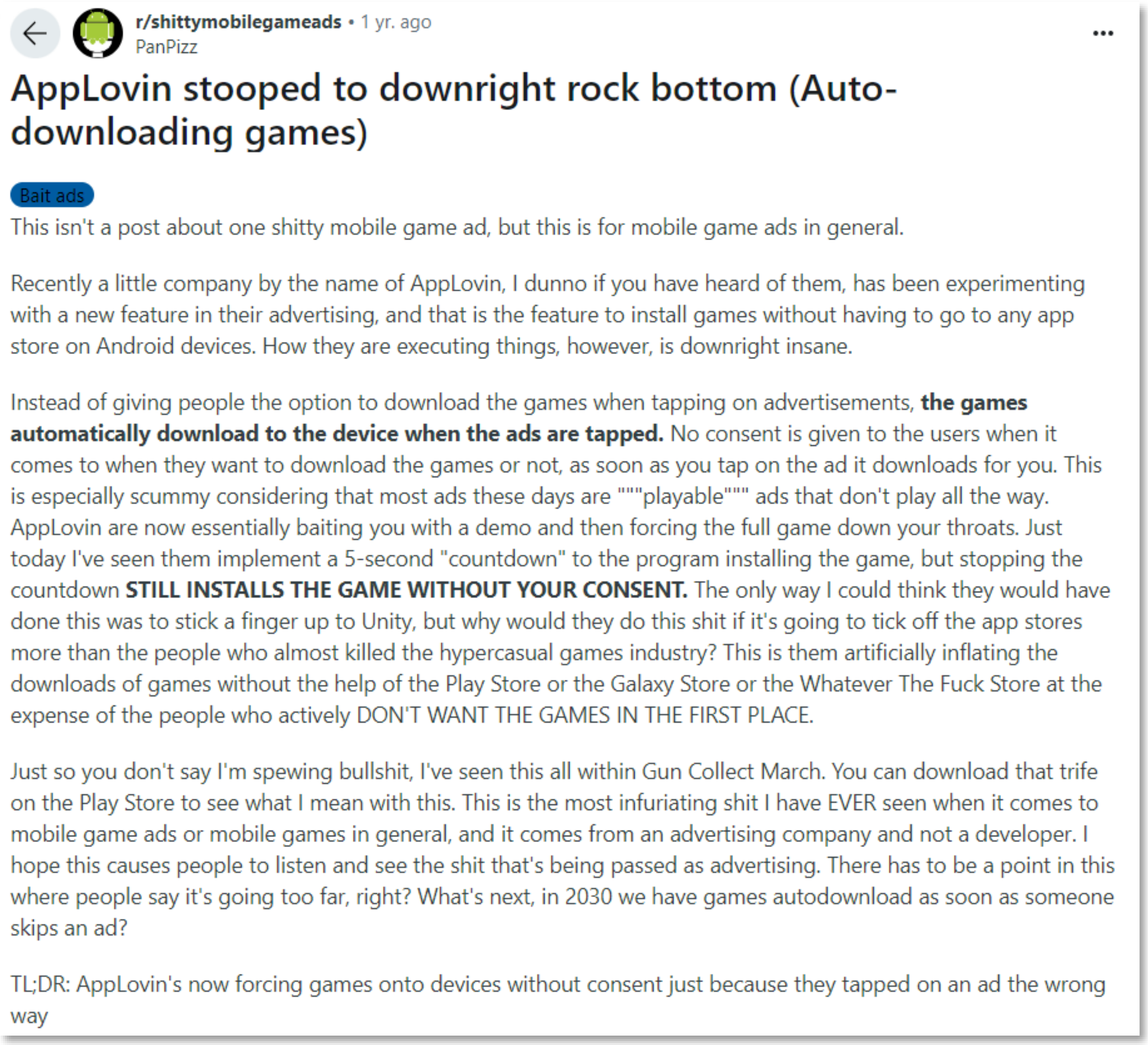
05/30/2023


Daily Installs, "Bricks n Balls" (Brazil)

AppLovin Array Expands Samsung Partnership in LATAM, Launching On Samsung Devices in Brazil

AppLovin
Sep 5, 2023

<u>Widespread Complaints of Unsolicited Downloads via AppHub Visible in Search Interest</u>



r/shittymobilegameads • 1 yr. ago
PanPizz

AppLovin stooped to downright rock bottom (Auto-downloading games)

Bait ads

This isn't a post about one shitty mobile game ad, but this is for mobile game ads in general.

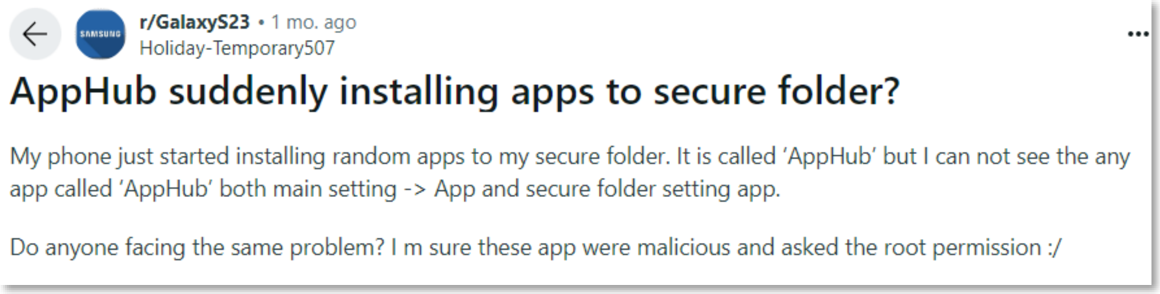
Recently a little company by the name of AppLovin, I dunno if you have heard of them, has been experimenting with a new feature in their advertising, and that is the feature to install games without having to go to any app store on Android devices. How they are executing things, however, is downright insane.

Instead of giving people the option to download the games when tapping on advertisements, **the games automatically download to the device when the ads are tapped.** No consent is given to the users when it comes to when they want to download the games or not, as soon as you tap on the ad it downloads for you. This is especially scummy considering that most ads these days are """playable""" ads that don't play all the way. AppLovin are now essentially baiting you with a demo and then forcing the full game down your throats. Just today I've seen them implement a 5-second "countdown" to the program installing the game, but stopping the countdown **STILL INSTALLS THE GAME WITHOUT YOUR CONSENT.** The only way I could think they would have done this was to stick a finger up to Unity, but why would they do this shit if it's going to tick off the app stores more than the people who almost killed the hypercasual games industry? This is them artificially inflating the downloads of games without the help of the Play Store or the Galaxy Store or the Whatever The Fuck Store at the expense of the people who actively DON'T WANT THE GAMES IN THE FIRST PLACE.

Just so you don't say I'm spewing bullshit, I've seen this all within Gun Collect March. You can download that trife on the Play Store to see what I mean with this. This is the most infuriating shit I have EVER seen when it comes to mobile game ads or mobile games in general, and it comes from an advertising company and not a developer. I hope this causes people to listen and see the shit that's being passed as advertising. There has to be a point in this where people say it's going too far, right? What's next, in 2030 we have games autodownload as soon as someone skips an ad?

TL;DR: AppLovin's now forcing games onto devices without consent just because they tapped on an ad the wrong way

Source: *Reddit*



r/GalaxyS23 • 1 mo. ago
Holiday-Temporary507

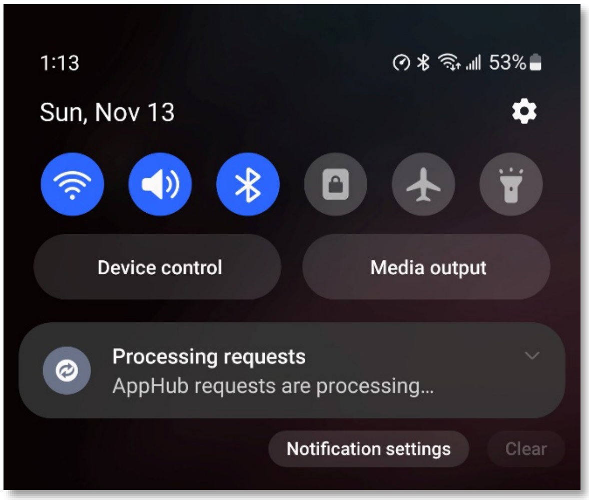
AppHub suddenly installing apps to secure folder?

My phone just started installing random apps to my secure folder. It is called 'AppHub' but I can not see the any app called 'AppHub' both main setting -> App and secure folder setting app.

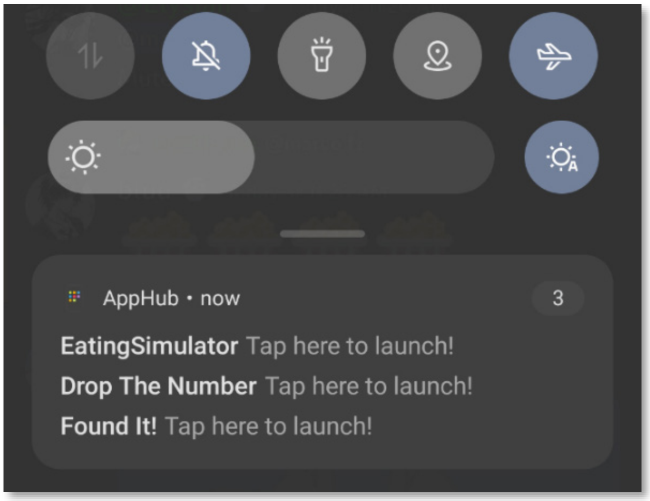
Do anyone facing the same problem? I m sure these app were malicious and asked the root permission :/

Source: *Reddit*

Our review of user complaints across forums such as Reddit, T-Mobile's user forums, and Android Central suggests that users often discover installations after the fact, or when AppHub appears as an active process.



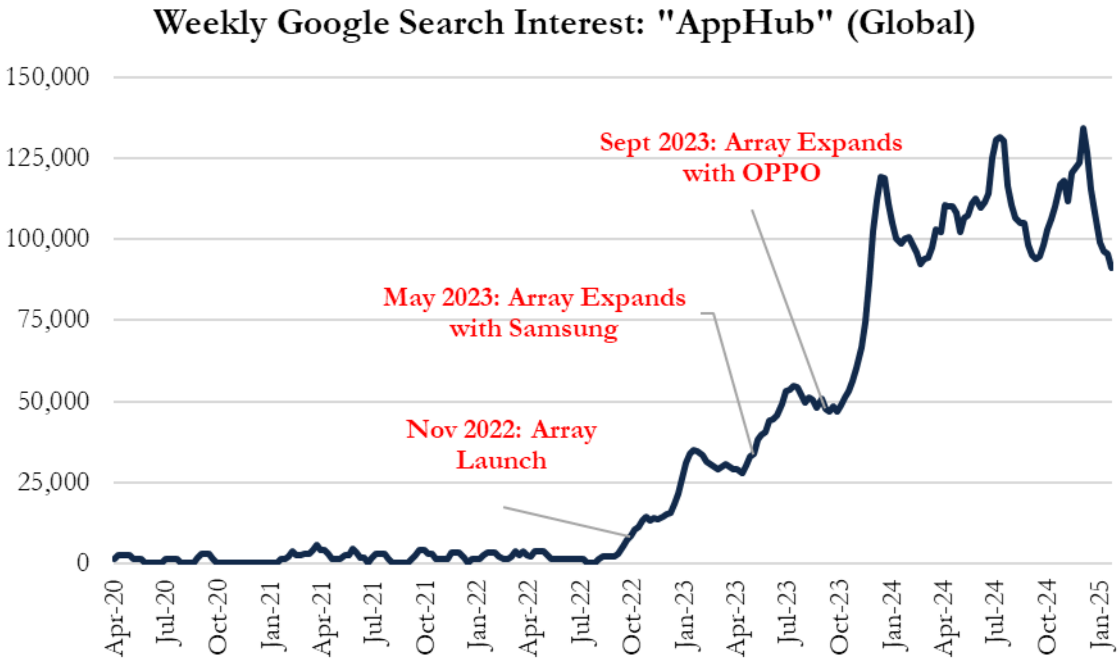
Processing requests
AppHub requests are processing…



AppHub • now

EatingSimulator Tap here to launch!
Drop The Number Tap here to launch!
Found It! Tap here to launch!

Users find themselves puzzled by the sudden appearance of a program installing games that they don't recall ever requesting. So they Google "AppHub." Prior to Array's launch, "AppHub" saw virtually zero search interest. But interest surged at three critical points: Array's late 2022 launch, the May 2023 Samsung expansion, and the September 2023 OPPO expansion.



Weekly Google Search Interest: "AppHub" (Global)

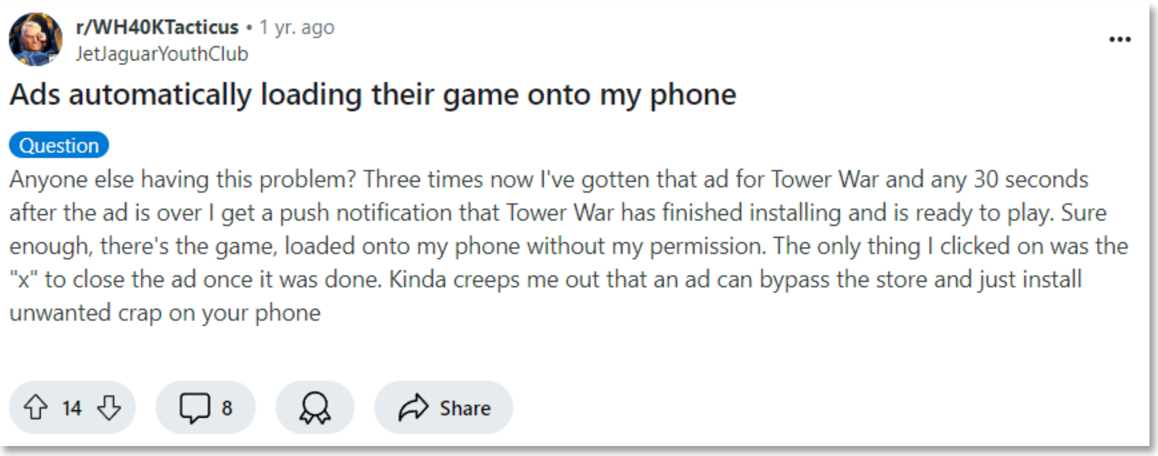
Sept 2023: Array Expands with OPPO

May 2023: Array Expands with Samsung

Nov 2022: Array Launch

A similar dynamic exists on Reddit, where user complaints have exploded, **some referring to AppHub as "pure cancer."**[14] For example, in a subreddit dedicated to the popular miniature wargame "Warhammer 40,000: Tacticus", a user complains that "Tower War" was automatically downloaded to their device after an advertisement for that game. As expected, Warhammer's APK contains the AppHub binding permission.

[14] We could fill an entire report with screenshots of complaints, but for everyone's sake, we won't. See more examples of user complaints here, here, here, here, here, here, here, and here.

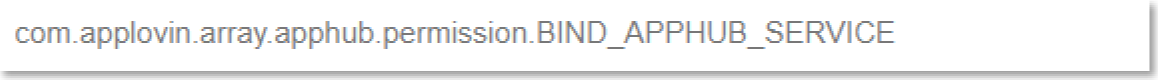


r/WH40KTacticus • 1 yr. ago
JetJaguarYouthClub

Ads automatically loading their game onto my phone

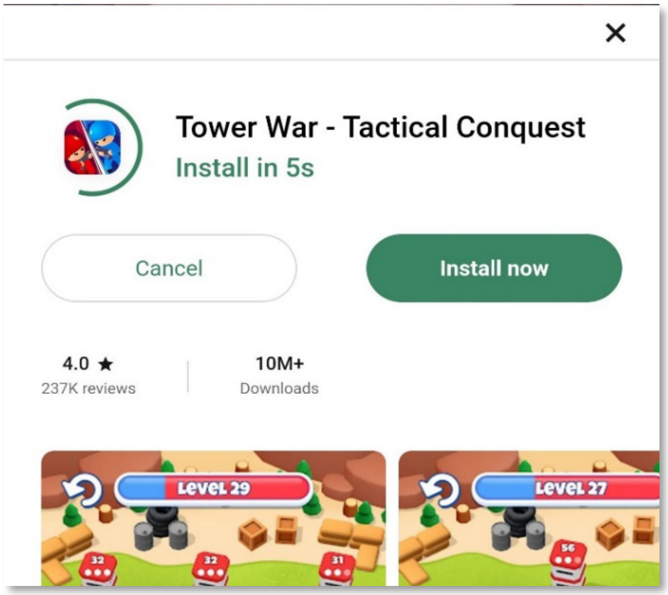
Question

Anyone else having this problem? Three times now I've gotten that ad for Tower War and any 30 seconds after the ad is over I get a push notification that Tower War has finished installing and is ready to play. Sure enough, there's the game, loaded onto my phone without my permission. The only thing I clicked on was the "x" to close the ad once it was done. Kinda creeps me out that an ad can bypass the store and just install unwanted crap on your phone



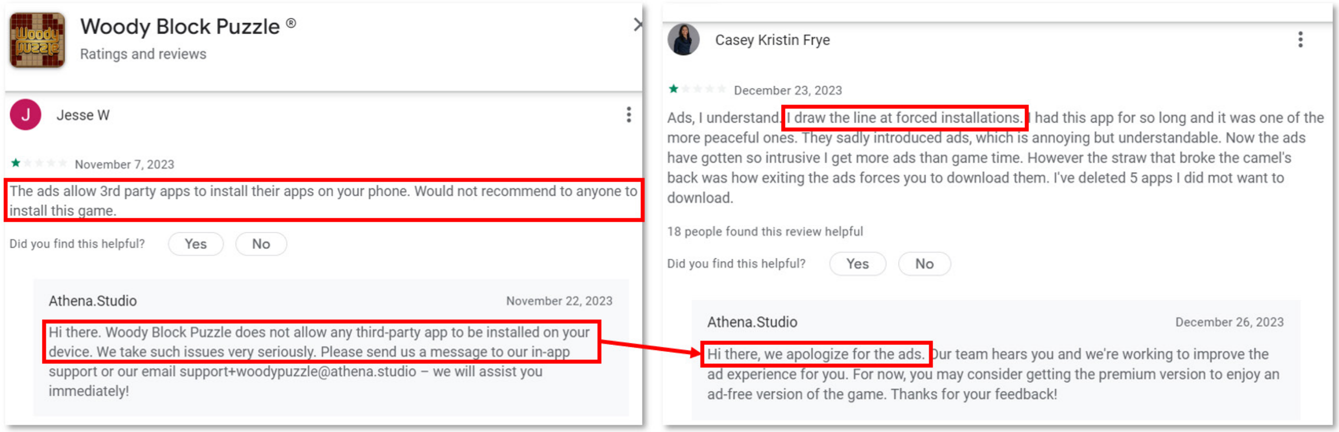
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE

<u>To reiterate: as the apps enable "one-click" direct downloads, simply clicking anywhere on this ad – including not quite exactly on the "X" – could potentially cause an automatic installation of the game.</u>



Tower War - Tactical Conquest
Install in 5s

Our review of complaints also uncovered some uniquely telling incidents. For example, in November 2023, one user of the Woody Block Puzzle app complained that the ads *"allow 3rd party apps to install their apps on your phone."* We note that the app is one of the thousands that has been equipped with AppLovin's binding permission, and that the game was made by Athena Studio, which the Company proudly lists among its partner studios. The studio responded to the review, denying the ability for third-party app installation and adding *"we take such issues very seriously."* Yet less than two months later when another user lodged the very same complaint of *"forced installations"*, Athena never denied the allegation. We can only speculate that perhaps the game studio's social media manager had been advised that actually, *their apps do allow* for this behavior.



Woody Block Puzzle ®
Ratings and reviews

Jesse W

★☆☆☆☆ November 7, 2023

The ads allow 3rd party apps to install their apps on your phone. Would not recommend to anyone to install this game.

Did you find this helpful? Yes No

Athena.Studio November 22, 2023

Hi there. Woody Block Puzzle does not allow any third-party app to be installed on your device. We take such issues very seriously. Please send us a message to our in-app support or our email support+woodypuzzle@athena.studio – we will assist you immediately!

Casey Kristin Frye

★☆☆☆☆ December 23, 2023

Ads, I understand. I draw the line at forced installations. I had this app for so long and it was one of the more peaceful ones. They sadly introduced ads, which is annoying but understandable. Now the ads have gotten so intrusive I get more ads than game time. However the straw that broke the camel's back was how exiting the ads forces you to download them. I've deleted 5 apps I did mot want to download.

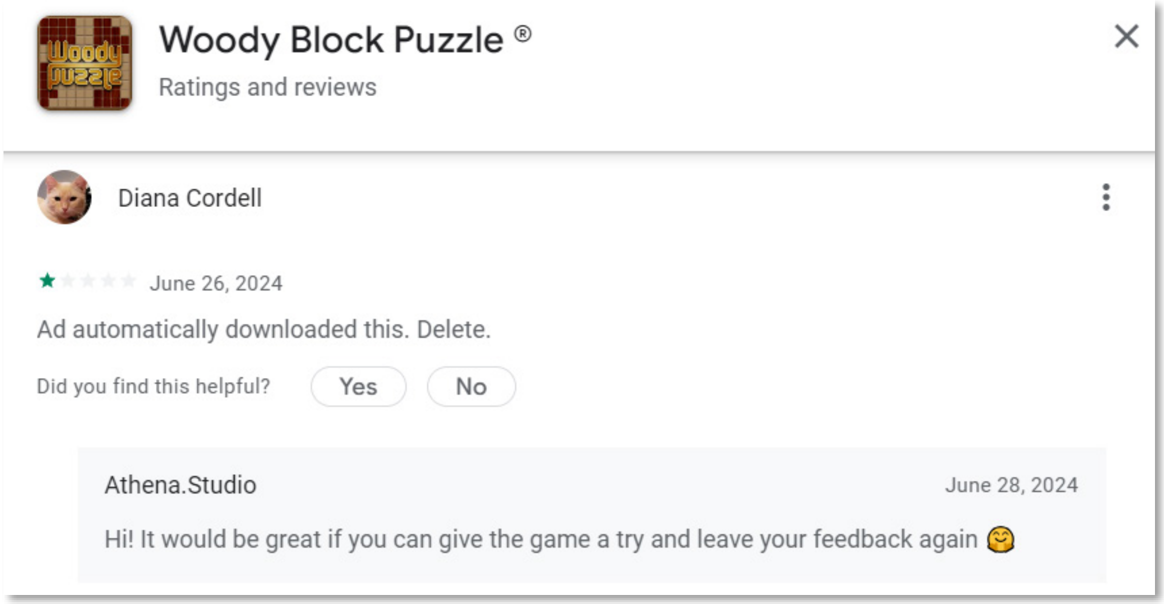
18 people found this review helpful

Did you find this helpful? Yes No

Athena.Studio December 26, 2023

Hi there, we apologize for the ads. Our team hears you and we're working to improve the ad experience for you. For now, you may consider getting the premium version to enjoy an ad-free version of the game. Thanks for your feedback!

One later review suggests of the very same game complained **<u>not only that it was *forcing* third-party app downloads, but was one such app that *had been forced* onto users – again mirroring the self-reinforcing loop suggested by the Bricks n Balls data.</u>** For its part, Athena Studio had seemingly already given up all pretense – rather than deny or apologize, they pled *"give the game a try."*



Woody Block Puzzle ®
Ratings and reviews

Diana Cordell

★☆☆☆☆ June 26, 2024

Ad automatically downloaded this. Delete.

Did you find this helpful? Yes No

Athena.Studio June 28, 2024

Hi! It would be great if you can give the game a try and leave your feedback again 🤗

We pored over Google Play reviews among many of the most popular apps containing the AppHub binding permission. We believe the reviews demonstrate that ads within these games have continued to trigger unwanted downloads consistently on user devices not only starting in late 2022 but to the present day. We include examples from the oft-bemoaned Tower War app below.

<u>"Tower War – Tactical Conquest" – 50M+ Downloads</u>	
Date	**Review (edited for brevity if necessary)**
1/25/25	*...the app automatically opens other games and the Android store without clicking anything. It automatically starts to download games as well. Better to delete the clickbait possible mallard that installs software without you agreeing to install.*
12/15/24	*Has awful add that automatically opens Google store*

10/28/24	*It installs other apps from the ads it shows you. AUTOMATICALLY WITHOUT MY PERMISSION!*
9/20/24	*...There is also a banner ad at the bottom that will automatically open a web browser instance and go to a website that is questionable....*
9/17/24	*The ads are ridiculous... Every second ad you close automatically opens the play Store. I understand the need for ads but it's very intrusive when they keep redirecting to the play Store!!*
6/8/24	*...there are ads that have no x to close them or they even automatically take you to the play store...*
4/15/24	*If you accidentally touch an ad, it automatically installs an app on your phone. This game hides your home row buttons, so it's challenging to exit.*
3/12/24	*...I'm honestly uninstalling every game app on Google Play. It's not cool, nor should it be legal for your ads to automatically install games on my phone. I have multiple systems, I do not need phone games, and I am extremely tired of it. A lot of the games now are doing this. I am officially boycotting all of them.*
3/12/24	*...Some ads automatically download software without the user taking action or granting additional permissions. This is MALWARE.*
3/5/24	*It's an ad game. I've been playing with this game for some time now. It's time to stop playing this game and uninstall it when it begins to automatically install games and open webpages in my browser. Unscrupulous business methods!*

Finally, customers of AppLovin's OEM partners such as Samsung and RealMe also complain about unwanted installations through AppHub.

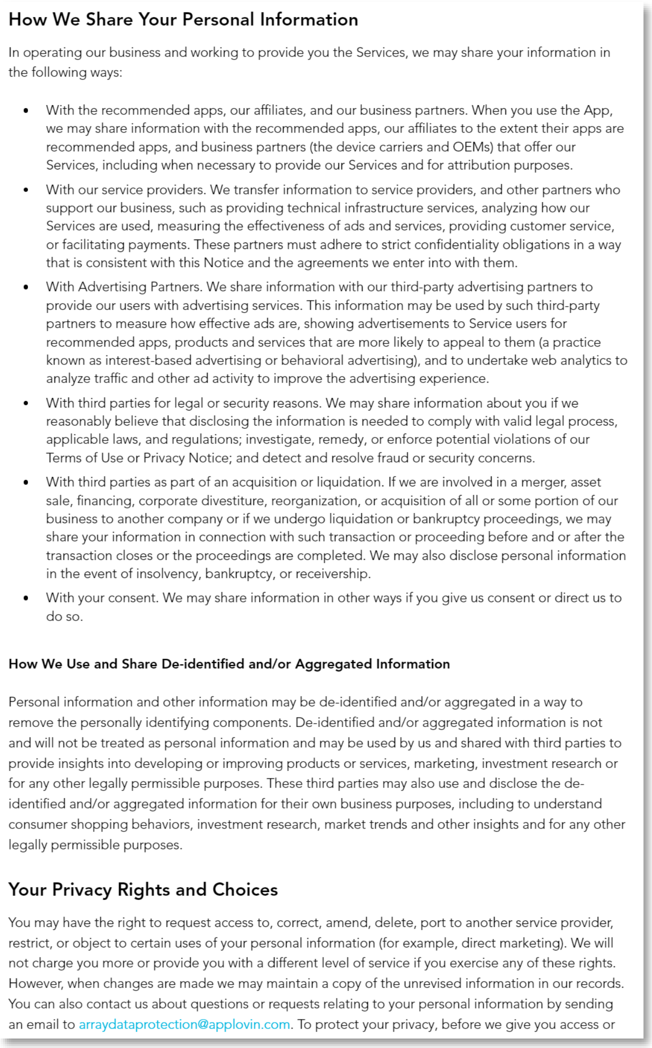
- Samsung's Spanish language user forums contain numerous complaints of AppHub's *"installing applications automatically without asking for permissions."*

- Among RealMe users, the blowback was apparently so prevalent that in January 2024, RealMe itself authored a blog post instructing users how to disable AppHub.[15]

June 2024: Array Updates its Privacy Policies in What Appears a "CYA" Maneuver

We also find it puzzling that in June 2024, Array updated its privacy policy to include a new section on "Direct Download Services." This is the only material change that we see from the previous April 2023 version, and yet if this feature was always inherent to Array's existence, why the update?

[15] The page cites that the topic was last updated February 19, 2025, as of the time of our writing.



How We Share Your Personal Information

In operating our business and working to provide you the Services, we may share your information in the following ways:

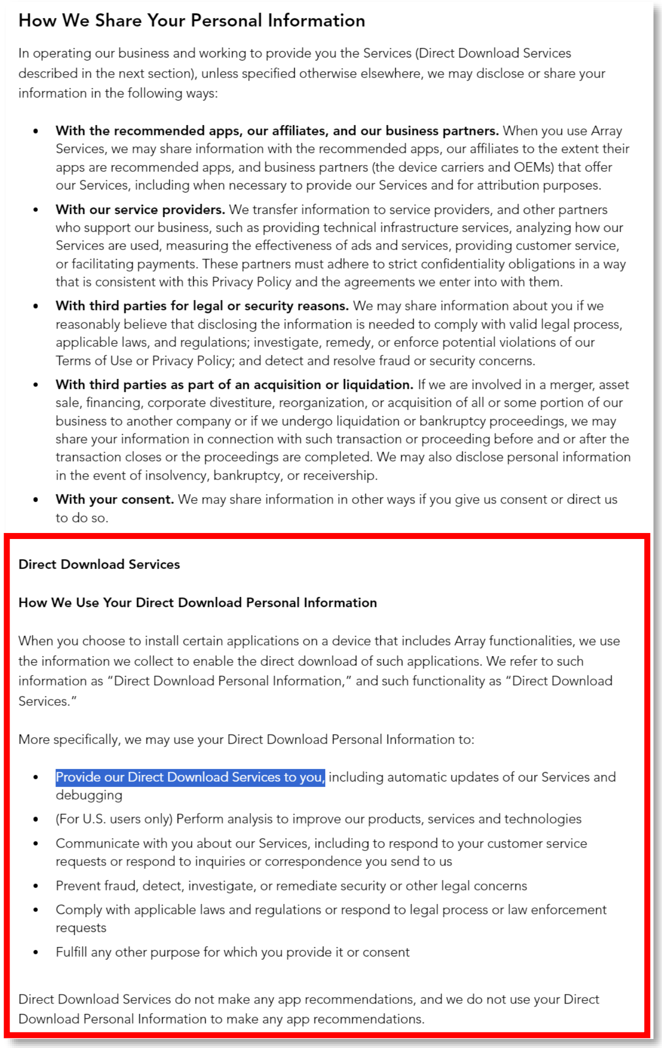
- With the recommended apps, our affiliates, and our business partners. When you use the App, we may share information with the recommended apps, our affiliates to the extent their apps are recommended apps, and business partners (the device carriers and OEMs) that offer our Services, including when necessary to provide our Services and for attribution purposes.
- With our service providers. We transfer information to service providers, and other partners who support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, or facilitating payments. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Notice and the agreements we enter into with them.
- With Advertising Partners. We share information with our third-party advertising partners to provide our users with advertising services. This information may be used by such third-party partners to measure how effective ads are, showing advertisements to Service users for recommended apps, products and services that are more likely to appeal to them (a practice known as interest-based advertising or behavioral advertising), and to undertake web analytics to analyze traffic and other ad activity to improve the advertising experience.
- With third parties for legal or security reasons. We may share information about you if we reasonably believe that disclosing the information is needed to comply with valid legal process, applicable laws, and regulations; investigate, remedy, or enforce potential violations of our Terms of Use or Privacy Notice; and detect and resolve fraud or security concerns.
- With third parties as part of an acquisition or liquidation. If we are involved in a merger, asset sale, financing, corporate divestiture, reorganization, or acquisition of all or some portion of our business to another company or if we undergo liquidation or bankruptcy proceedings, we may share your information in connection with such transaction or proceeding before and or after the transaction closes or the proceedings are completed. We may also disclose personal information in the event of insolvency, bankruptcy, or receivership.
- With your consent. We may share information in other ways if you give us consent or direct us to do so.

How We Use and Share De-identified and/or Aggregated Information

Personal information and other information may be de-identified and/or aggregated in a way to remove the personally identifying components. De-identified and/or aggregated information is not and will not be treated as personal information and may be used by us and shared with third parties to provide insights into developing or improving products or services, marketing, investment research or for any other legally permissible purposes. These third parties may also use and disclose the de-identified and/or aggregated information for their own business purposes, including to understand consumer shopping behaviors, investment research, market trends and other insights and for any other legally permissible purposes.

Your Privacy Rights and Choices

You may have the right to request access to, correct, amend, delete, port to another service provider, restrict, or object to certain uses of your personal information (for example, direct marketing). We will not charge you more or provide you with a different level of service if you exercise any of these rights. However, when changes are made we may maintain a copy of the unrevised information in our records. You can also contact us about questions or requests relating to your personal information by sending an email to arraydataprotection@applovin.com. To protect your privacy, before we give you access or



How We Share Your Personal Information

In operating our business and working to provide you the Services (Direct Download Services described in the next section), unless specified otherwise elsewhere, we may disclose or share your information in the following ways:

- **With the recommended apps, our affiliates, and our business partners.** When you use Array Services, we may share information with the recommended apps, our affiliates to the extent their apps are recommended apps, and business partners (the device carriers and OEMs) that offer our Services, including when necessary to provide our Services and for attribution purposes.
- **With our service providers.** We transfer information to service providers, and other partners who support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, or facilitating payments. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Privacy Policy and the agreements we enter into with them.
- **With third parties for legal or security reasons.** We may share information about you if we reasonably believe that disclosing the information is needed to comply with valid legal process, applicable laws, and regulations; investigate, remedy, or enforce potential violations of our Terms of Use or Privacy Policy; and detect and resolve fraud or security concerns.
- **With third parties as part of an acquisition or liquidation.** If we are involved in a merger, asset sale, financing, corporate divestiture, reorganization, or acquisition of all or some portion of our business to another company or if we undergo liquidation or bankruptcy proceedings, we may share your information in connection with such transaction or proceeding before and or after the transaction closes or the proceedings are completed. We may also disclose personal information in the event of insolvency, bankruptcy, or receivership.
- **With your consent.** We may share information in other ways if you give us consent or direct us to do so.

Direct Download Services

How We Use Your Direct Download Personal Information

When you choose to install certain applications on a device that includes Array functionalities, we use the information we collect to enable the direct download of such applications. We refer to such information as "Direct Download Personal Information," and such functionality as "Direct Download Services."

More specifically, we may use your Direct Download Personal Information to:

- Provide our Direct Download Services to you, including automatic updates of our Services and debugging
- (For U.S. users only) Perform analysis to improve our products, services and technologies
- Communicate with you about our Services, including to respond to your customer service requests or respond to inquiries or correspondence you send to us
- Prevent fraud, detect, investigate, or remediate security or other legal concerns
- Comply with applicable laws and regulations or respond to legal process or law enforcement requests
- Fulfill any other purpose for which you provide it or consent

Direct Download Services do not make any app recommendations, and we do not use your Direct Download Personal Information to make any app recommendations.

AppLovin's Notorious UX Tactics Now Translate More Directly to Installs

AppLovin's UX tactics – such as the countdown timer shown above – can be described as gimmicky at best. We applaud the skeptics who have presented their own views prior to us – including Fuzzy Panda Research. Many have documented these practices in detail; we won't take up further airspace discussing them here. Our view is that while such gimmicks result in high click-through rates ("CTRs") – often unbelievably so – their deployment has *historically* been limited by the implicit cost of brand damage resulting from user frustration. No one enjoys an ad-riddled game. We believe, however, that AppLovin has now gone one step further: by deploying the direct download via the mechanisms we've described herein, such UX tactics have not only become advantageous, but integral to the very model. We think this ends badly... Consider that:

- With more installations, it appears to game studios as if their advertising dollars are becoming more efficient.

- Recall, however, that the vast majority of AppLovin's ads are being bought and sold within the existing mobile gaming ecosystem, and the vast majority of studios seek to make their money primarily by re-selling the ad inventory from those new users.

- As such, the value of the install is dependent upon users actually playing the games. If acquired installs don't result in more impressions on the back end (i.e., users aren't actually playing the games), then these apps will not be profitable on the re-sale of that newly acquired ad space.

- So, how might one combat the rapidly declining value of that ad space? One option is to deploy an increasing number of gimmicks.

To that end, both app user reviews and experts we spoke with suggested that AppLovin's UX tactics have become considerably more exploitative over the past 2 years.[16]

> *"I'm cursing AppLovin because my kids are having to click out three times just to kick a stupid soccer ball or something. It's just like, how many ads can you stuff into this experience? I paid $8 to not see ads, but I still see ads. So that seems to not apply anymore."*
> – Former AppLovin Executive
>
> *"The big difference [the reason for AppLovin's success] is aggressiveness of their ads, and how they [AppLovin] attributes them... The ads – I apologize, but you watch them, and they're shitty."*[17]
> – Current Apps Industry Consultant
>
> *"If you hit X they'll give you a new page and then another page that'll bring you to the app store. They were paving the way there..."* – Employee at AppLovin Competitor

In this context, employing more and more outrageous gimmicks have not only become advantageous, but necessary to maintain the illusion that AppLovin's ads are as effective as they are. There's a term for this.

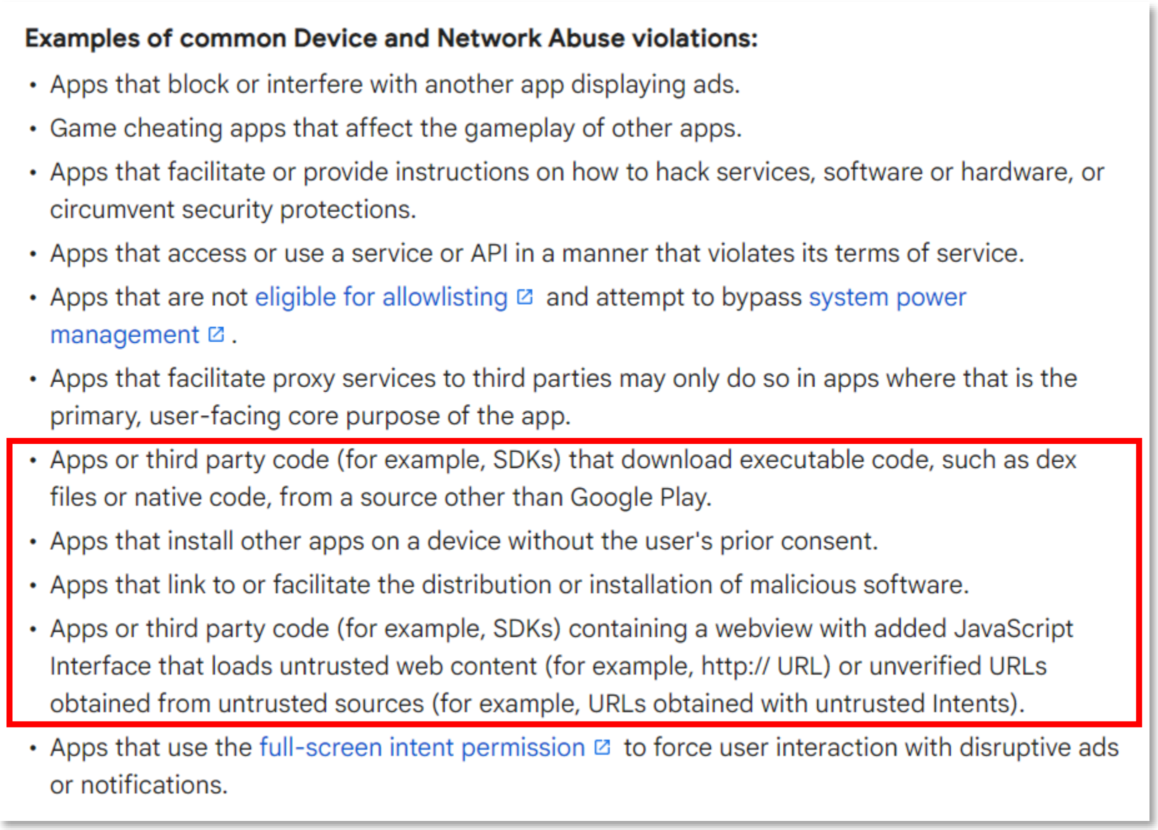
> *"**I'm almost certain that what they're doing is a Ponzi scheme...** It's junk inventory, junk apps... They've changed recently... It's kicked you out of the app and forced you to download the other app via the ad. Then when you log back in, it counts you again, so it shows you as a repeating user, but in reality it's a really poor experience. It's dirty metrics."* – AdTech Industry Executive

SDK Permissions Also Open Users' Devices to Potential Bad Actors, Appear to Violate Google Play Terms and Conditions

We believe AppLovin risks fallout from Google Play, as AppHub's APK includes high risk permissions, including the INSTALL_PACKAGES permission that Google Play has already deemed *"not for use by third-party applications."* We believe AppLovin abuses these permissions in a manner that directly violates Google Play's Device and Network Abuse policy by way of their SDK integration that allows third-party apps to bind to AppHub. Subsequent to the release of this report, we intend to issue an open letter to Google Play.

[16] For brevity, see user reviews in Appendix C.

[17] More on AppLovin's attribution process on pages 26 and 27.



Examples of common Device and Network Abuse 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 allowlisting 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 (for example, 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.
- Apps or third party code (for example, SDKs) containing a webview with added JavaScript Interface that loads untrusted web content (for example, http:// URL) or unverified URLs obtained from untrusted sources (for example, URLs obtained with untrusted Intents).
- Apps that use the full-screen intent permission to force user interaction with disruptive ads or notifications.

AppLovin's e-Commerce Push is a Smoke and Mirrors Game, Rigged from the Start

We believe AppLovin is entirely aware that its gaming promotion is unsustainable, and the Company has thus hung its hat on e-commerce. CEO Adam Foroughi claims that e-commerce is the *"best product"* he's ever seen released by AppLovin, touting *"a lot of proof of life"* and *"really positive results"* from pilot tests that began late last year. Investors have cheered these results on, but we believe AppLovin has been playing a rigged game from the start. We think there's meaningful risk that Meta takes action.

<u>AppLovin Requires Customers First Spend Big on Meta. Why? We Believe It's To Steal Attribution</u>

Public comments from advertisers mention AppLovin requires significant minimum spend on Meta to gain eligibility to the program, which we confirmed independently from multiple industry sources.

> *"…they're currently only allowing advertisers into the program who spend $600k/mo or more on Meta."*
>
> *"…for ecom, you currently need to be spending $600k/mo on meta to be considered…"*
>
> *"Smaller or less established brands might not be able to adapt to a new channel quite as easily, or be able to afford the minimum $20,000 per day ad spend AppLovin requires at this time."*

The Company doesn't appear to publicly disclose this requirement to investors, let alone provide an explanation of why it exists. We anticipate that AppLovin will likely argue that the requirement is there to ensure high-quality program participants, we think it serves a more underhanded purpose. It's unclear to us why AppLovin would require its users to rely on any other platform at all. Meta certainly doesn't require advertisers to spend on AppLovin first, so the Company's reliance on Meta is telling.[18]

Several former AppLovin employees and competitors suggested to us that the true purpose likely relates back to AppLovin's ability to "see" Meta's existing advertising, thanks to the Company's ownership of the MAX mediation layer. As such, AppLovin can quite literally copy Meta's homework.

> *"The budget is enormous, which means it's going broad spend across Meta. Which then means, they're [AppLovin is] able to collect those intent signals, probably through Adjust apps that are being tracked, and then take the credit. I don't trust it at all. There's no way."* – Former Adjust Employee
>
> *"They see everything… They could be playing attribution games. People that Meta targeted on their site, [AppLovin] might get the attribution…"* – AppLovin Competitor
>
> *"It's not black or white whether [AppLovin] should get credit for the sale."*
> – Former AppLovin Executive
>
> *"It makes it easy…to claim credit by stepping in front of what's already happening. They can see, in general, who's purchasing and then just serve ads to people they're highly confident will make a purchase."* – Current e-commerce Customer

Our concerns were also alluded to in a Business Insider article.

> *"Jeromy Sonne, the founder of marketing AI technology company Simbiant, has been monitoring the early AppLovin e-commerce results.*
>
> *He said he'd seen an 'extremely high correlation' between when AppLovin sees a spike in conversions and when Meta sees an increase in ad spend. He said he hadn't seen a similar trend when comparing Meta and Google or AppLovin and Google.*
>
> *He said that made him wonder if AppLovin was driving real incremental value or whether its campaigns were just reaching the exact same audience as Meta in some way.*
>
> *He said he'd also seen a "concerning overlap" where Shopify sales purportedly driven by AppLovin have a very high geographic overlap with where Meta ad website traffic was coming from."*

AppLovin Then Encourages Customers to Use Adjust: "Grading Their Own Test"

We believe AppLovin then encourages advertisers to use Adjust, its attribution platform acquired in 2021, to effectively grade its own tests and report "A+" results back to advertisers. In tandem, AppLovin is able to hand-pick customers from its waitlist of potential advertisers. Sources say the Company favors those with low SKU counts and those without data science teams of their own – in other words, groups that lack the resources to independently validate the Company's claims.

> *"Acquiring Adjust allowed them to see all the data and game it."* – Former AppLovin Employee
>
> *"[Customers] don't have data scientist guys to verify it themselves…they're trusting what AppLovin gives them."* – Former AppLovin Executive

[18] To be clear, based on our numerous conversations with industry participants and current AppLovin e-commerce advertisers, we don't believe AppLovin and Facebook are parties to any sort of reciprocal data sharing agreement, either.

> *"We take it at face value. We don't really shy away from it. We trust it just based on the rapport that they've held in the market... We're working on assigning based on all the different platforms that everyone knows – Google, Meta, Amazon... but I have not compared. But if I had to compare, Instagram is definitely better."* – Current AppLovin e-commerce Customer
>
> *"They don't have a lot of incentive to dig into it, because it looks good."* – Former Exec at AppLovin Competitor
>
> "*In the studio, when you were testing, you'd see a huge increase on AppLovin's side…they were just attributing it to themselves. If you ask other people, they'd say the same thing."* – Industry Participant

AppLovin even appears to be taking desperate measures to move their customers onto Adjust:

> "*They're giving Adjust away for free." – Former Adjust Executive*
>
> *"Now they're trying to force Adjust onto advertisers." – Former Exec at AppLovin Competitor*

Much like we believe AppLovin's Array has been quietly deployed to illicitly inflate the Company's mobile gaming results, we also believe that MAX and Adjust have aided AppLovin in creating a "rigged game" that will fall apart upon either action by Meta, or the natural expansion outside of relatively few advertisers currently on Meta. To that end, we believe these practices violate the privacy of Meta's users, and we also plan to author an open letter to Meta that addresses these concerns.

Regarding the latter, we find it telling that APP has yet to open up the program to a wider set of advertisers. One former AppLovin executive we spoke with suggested this was because CEO Adam Foroughi knows that it would result in lower performance.

> *"There are very specific commonalities to how it's growing... What they didn't disclose is that they only had too many SKUs. They only took the customers that had a few SKUs [because] the retargeting has a greater effect – if the customer leaves, but then the customer back in, it gets* attributed to you... *He said on the earnings call he'll open to 10 million customers – they won't do that in 2025, because it'll open them up to lower performance."* – Former AppLovin Executive

AppLovin CEO Foroughi: Advertising God? A Different "G-Word" Comes to Mind

AppLovin bulls have arrived at the mistaken conclusion that AppLovin CEO Adam Foroughi is something akin to an AdTech God. They often cite his previous ventures – LifeStreet and Social Hour. Yet the performance of these companies were each troubling.

Foroughi previously worked at Gator Corporation (later renamed Claria Corporation) in roughly 2004. As far as we can tell, this role has never been disclosed in AppLovin's public filings. Gator was, however "*Notorious as one of the first widespread spyware applications"* which *"inadvertently created a revolution in consumer backlash against irresponsible computer program design and malware proliferation."* Foroughi's boss at Gator was reportedly Mitchell Weisman. Per press reports at the time, *"Weisman was in charge of Claria's adware distribution partnerships, including its key relationship with file-sharing service Kazaa."*

Weisman, Foroughi, and ousted Gator CEO Jeff McFadden then left Gator and founded LifeStreet Media. Weisman is still at LifeStreet today. Today, LifeStreet lists APP as a partner on its website. APP's current VP of

Commerce (joined January 2024) Paul Kennedy was previously co-founder of LifeStreet and before that was also employed at Claria/Gator.

APP CEO Foroughi then founded Social Hour with APP co-founder Andrew Karam. Foroughi was CEO from August 2008 to July 2010. This business also seemed problematic: in June 2009, Facebook banned Social Hour's advertising, due to misleading/scam-like advertisements. Per Facebook:

> *"... deceptive content in ads placed within apps by developers... We have had the ads removed from a number of apps and prohibited two advertising networks from providing services to applications on Facebook's Platform..."*

In the LTM, AppLovin insiders have sold nearly $2.0 billion in stock, while KKR has dumped the entirety of its remaining $7.3 billion stake. We are short AppLovin and believe shares are headed lower.

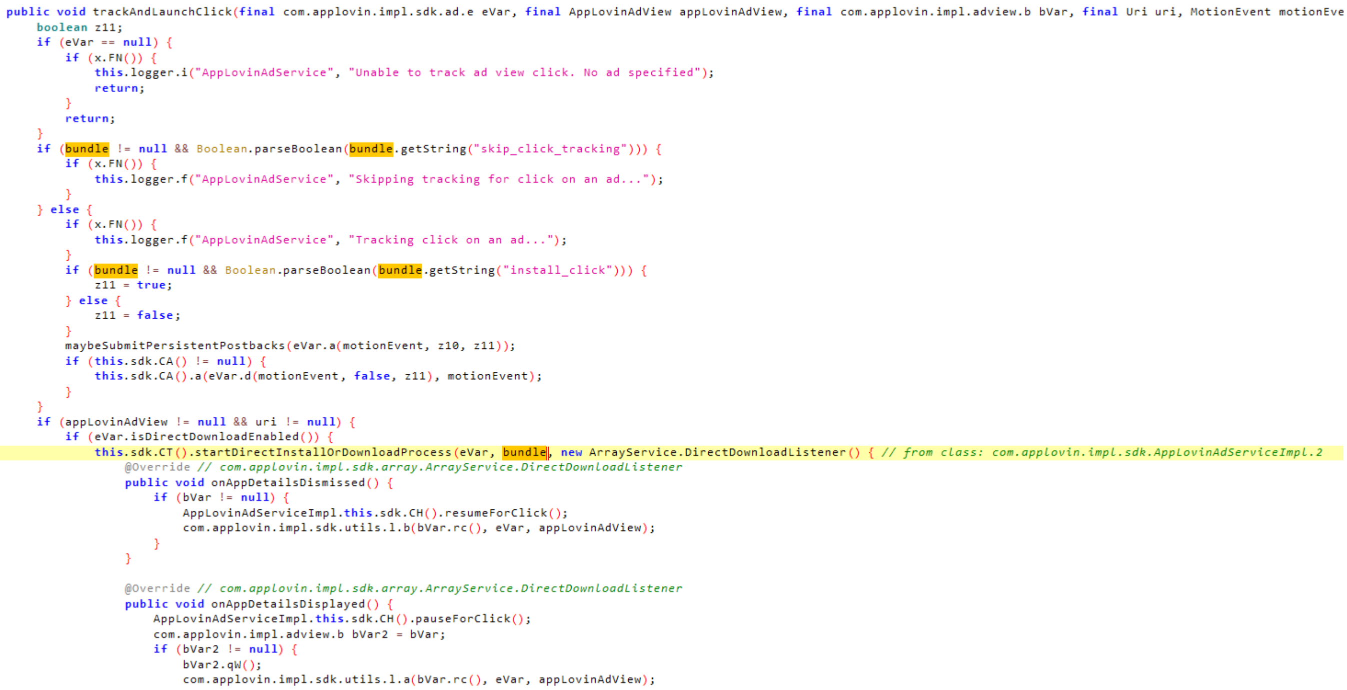
Appendix A: Code Review RE: One-Click Direct Downloads

In Subway Surfers' source code (obtained by putting Subway Surfer's APK in JADX), we view the code for the actual ads on the Subway Surfers app.

These ads use classes AppLovinAdServiceImpl and AppLovinAdBase. This means that when Subway Surfers wants to show an ad, Subway Surfers requests an ad from AppLovin through AppLovinAdServiceImpl.

AppLovinAdServiceImpl loads the ad, which is an instance of a class of type AppLovinAdBase.

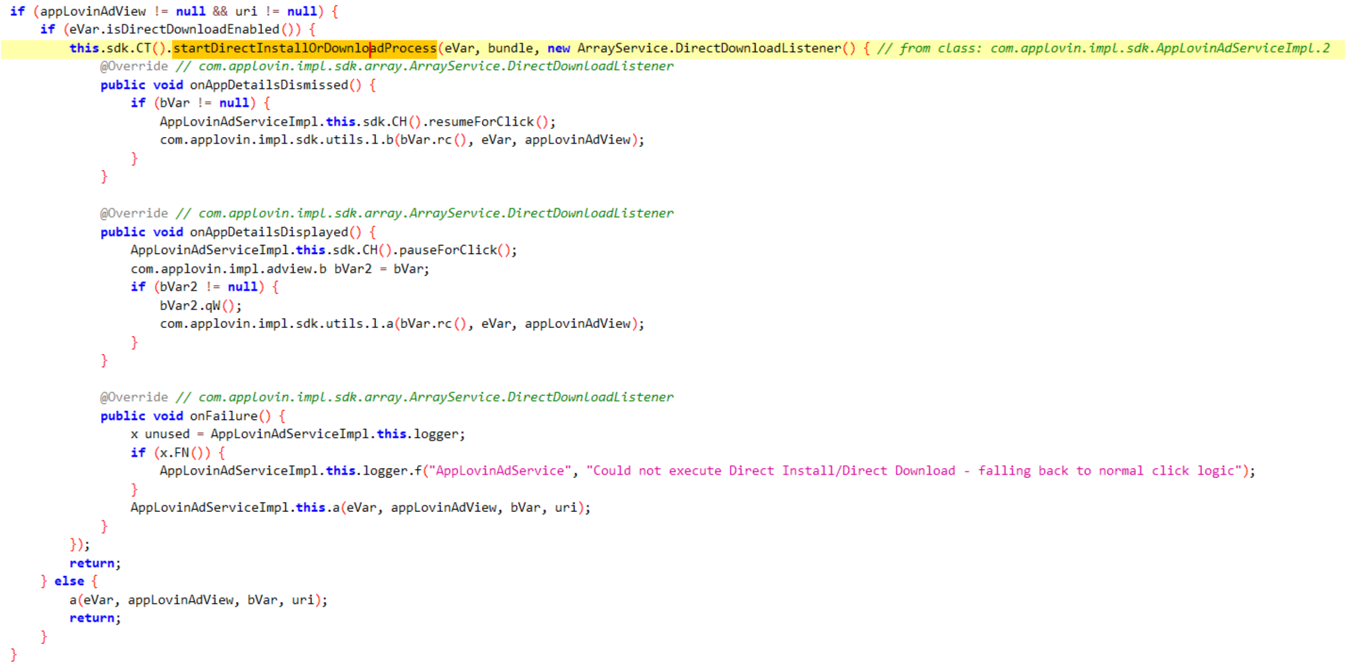
AppLovinAdServiceImpl then listens for a user click event on an advertisement via the functions trackAndLaunchVideoClick and trackAndLaunchClick. See a subsection of the latter function below:



```
public void trackAndLaunchClick(final com.applovin.impl.sdk.ad.e eVar, final AppLovinAdView appLovinAdView, final com.applovin.impl.adview.b bVar, final Uri uri, MotionEvent motionEve
    boolean z11;
    if (eVar == null) {
        if (x.FN()) {
            this.logger.i("AppLovinAdService", "Unable to track ad view click. No ad specified");
            return;
        }
        return;
    }
    if (bundle != null && Boolean.parseBoolean(bundle.getString("skip_click_tracking"))) {
        if (x.FN()) {
            this.logger.f("AppLovinAdService", "Skipping tracking for click on an ad...");
        }
    } else {
        if (x.FN()) {
            this.logger.f("AppLovinAdService", "Tracking click on an ad...");
        }
        if (bundle != null && Boolean.parseBoolean(bundle.getString("install_click"))) {
            z11 = true;
        } else {
            z11 = false;
        }
        maybeSubmitPersistentPostbacks(eVar.a(motionEvent, z10, z11));
        if (this.sdk.CA() != null) {
            this.sdk.CA().a(eVar.d(motionEvent, false, z11), motionEvent);
        }
    }
    if (appLovinAdView != null && uri != null) {
        if (eVar.isDirectDownloadEnabled()) {
            this.sdk.CT().startDirectInstallOrDownloadProcess(eVar, bundle, new ArrayService.DirectDownloadListener() { // from class: com.applovin.impl.sdk.AppLovinAdServiceImpl.2
                @Override // com.applovin.impl.sdk.array.ArrayService.DirectDownloadListener
                public void onAppDetailsDismissed() {
                    if (bVar != null) {
                        AppLovinAdServiceImpl.this.sdk.CH().resumeForClick();
                        com.applovin.impl.sdk.utils.l.b(bVar.rc(), eVar, appLovinAdView);
                    }
                }

                @Override // com.applovin.impl.sdk.array.ArrayService.DirectDownloadListener
                public void onAppDetailsDisplayed() {
                    AppLovinAdServiceImpl.this.sdk.CH().pauseForClick();
                    com.applovin.impl.adview.b bVar2 = bVar;
                    if (bVar2 != null) {
                        bVar2.qW();
                        com.applovin.impl.sdk.utils.l.a(bVar.rc(), eVar, appLovinAdView);
```

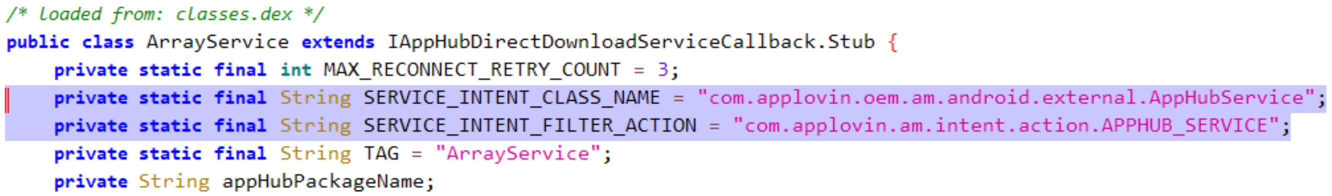
These functions use a custom click listener called AppLovinAdClickListener. Documentation shows this listener is triggered when the user clicks anywhere on an ad once.

When the user clicks on an ad as determined by AppLovinAdClickListener, this prompts startDirectInstallOrDownloadProcess with a new ArrayService object.



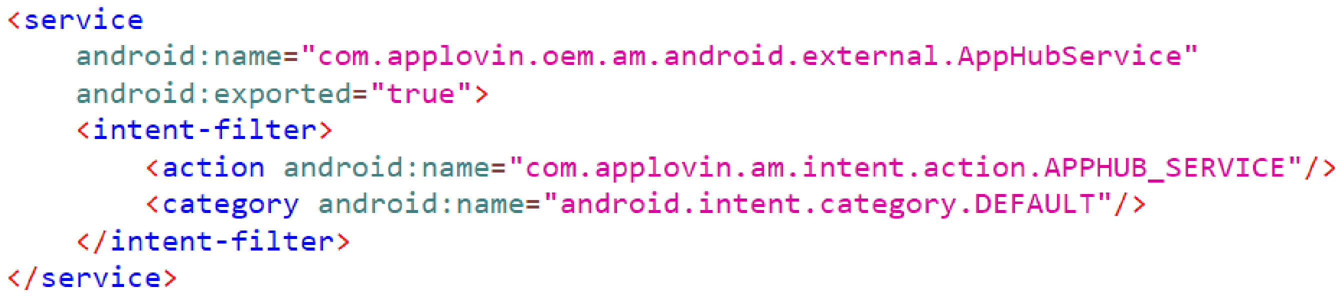
```
if (appLovinAdView != null && uri != null) {
    if (eVar.isDirectDownloadEnabled()) {
        this.sdk.CT().startDirectInstallOrDownloadProcess(eVar, bundle, new ArrayService.DirectDownloadListener() { // from class: com.applovin.impl.sdk.AppLovinAdServiceImpl.2
            @Override // com.applovin.impl.sdk.array.ArrayService.DirectDownloadListener
            public void onAppDetailsDismissed() {
                if (bVar != null) {
                    AppLovinAdServiceImpl.this.sdk.CH().resumeForClick();
                    com.applovin.impl.sdk.utils.l.b(bVar.rc(), eVar, appLovinAdView);
                }
            }

            @Override // com.applovin.impl.sdk.array.ArrayService.DirectDownloadListener
            public void onAppDetailsDisplayed() {
                AppLovinAdServiceImpl.this.sdk.CH().pauseForClick();
                com.applovin.impl.adview.b bVar2 = bVar;
                if (bVar2 != null) {
                    bVar2.qW();
                    com.applovin.impl.sdk.utils.l.a(bVar.rc(), eVar, appLovinAdView);
                }
            }

            @Override // com.applovin.impl.sdk.array.ArrayService.DirectDownloadListener
            public void onFailure() {
                x unused = AppLovinAdServiceImpl.this.logger;
                if (x.FN()) {
                    AppLovinAdServiceImpl.this.logger.f("AppLovinAdService", "Could not execute Direct Install/Direct Download - falling back to normal click logic");
                }
                AppLovinAdServiceImpl.this.a(eVar, appLovinAdView, bVar, uri);
            }
        });
        return;
    } else {
        a(eVar, appLovinAdView, bVar, uri);
        return;
    }
}
```

ArrayService creates an intent to bind to an external “AppHubService”



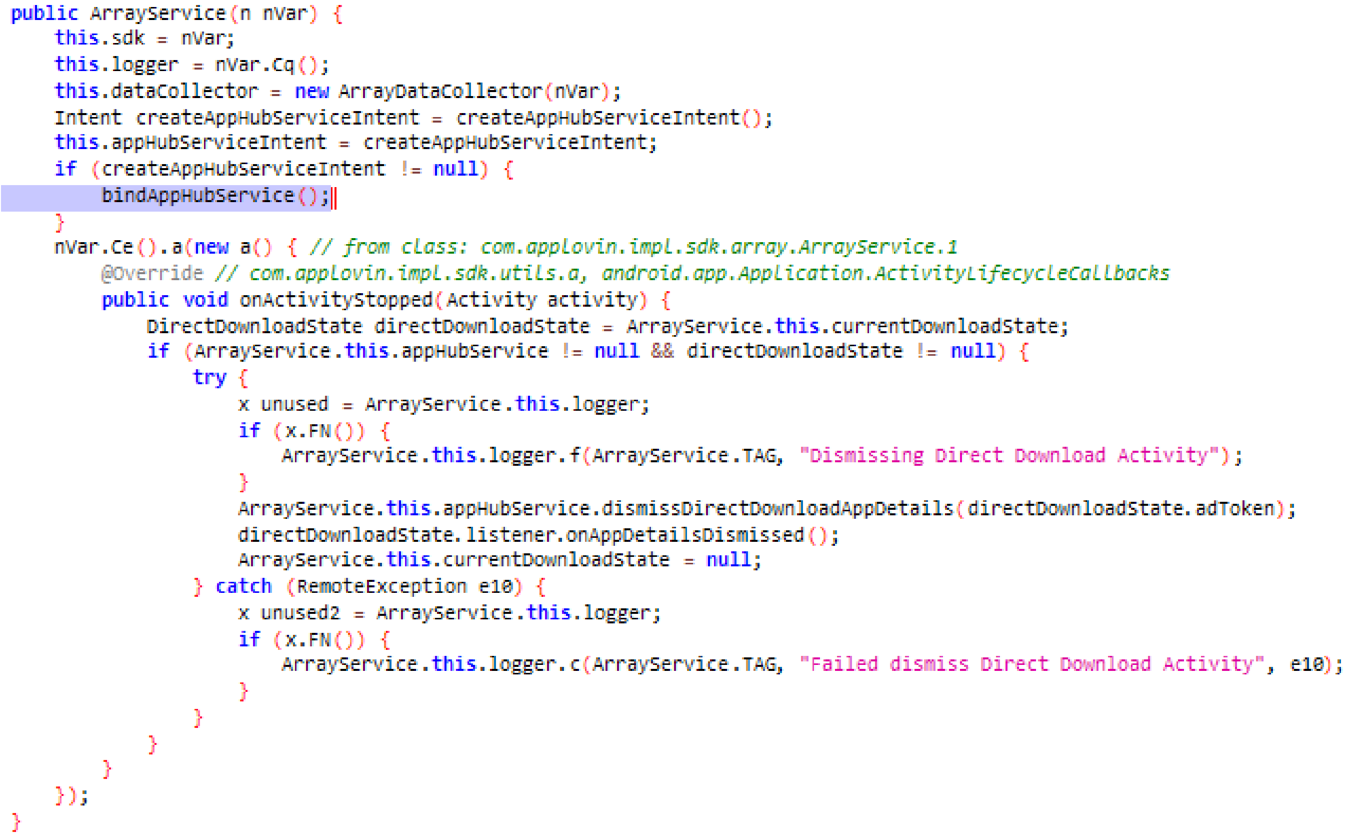
```
/* loaded from: classes.dex */
public class ArrayService extends IAppHubDirectDownloadServiceCallback.Stub {
    private static final int MAX_RECONNECT_RETRY_COUNT = 3;
    private static final String SERVICE_INTENT_CLASS_NAME = "com.applovin.oem.am.android.external.AppHubService";
    private static final String SERVICE_INTENT_FILTER_ACTION = "com.applovin.am.intent.action.APPHUB_SERVICE";
    private static final String TAG = "ArrayService";
    private String appHubPackageName;
```

AppHub’s Android Manifest xml file (obtained by putting AppHub’s APK into JADX) contains the matching service (see below). Importantly, android:exported is set to true here, confirming that AppHubService can be triggered by an external app, e.g. Subway Surfers, rather than within AppHub (as per AppLovin’s description of Array as being used in the context of new device setup):

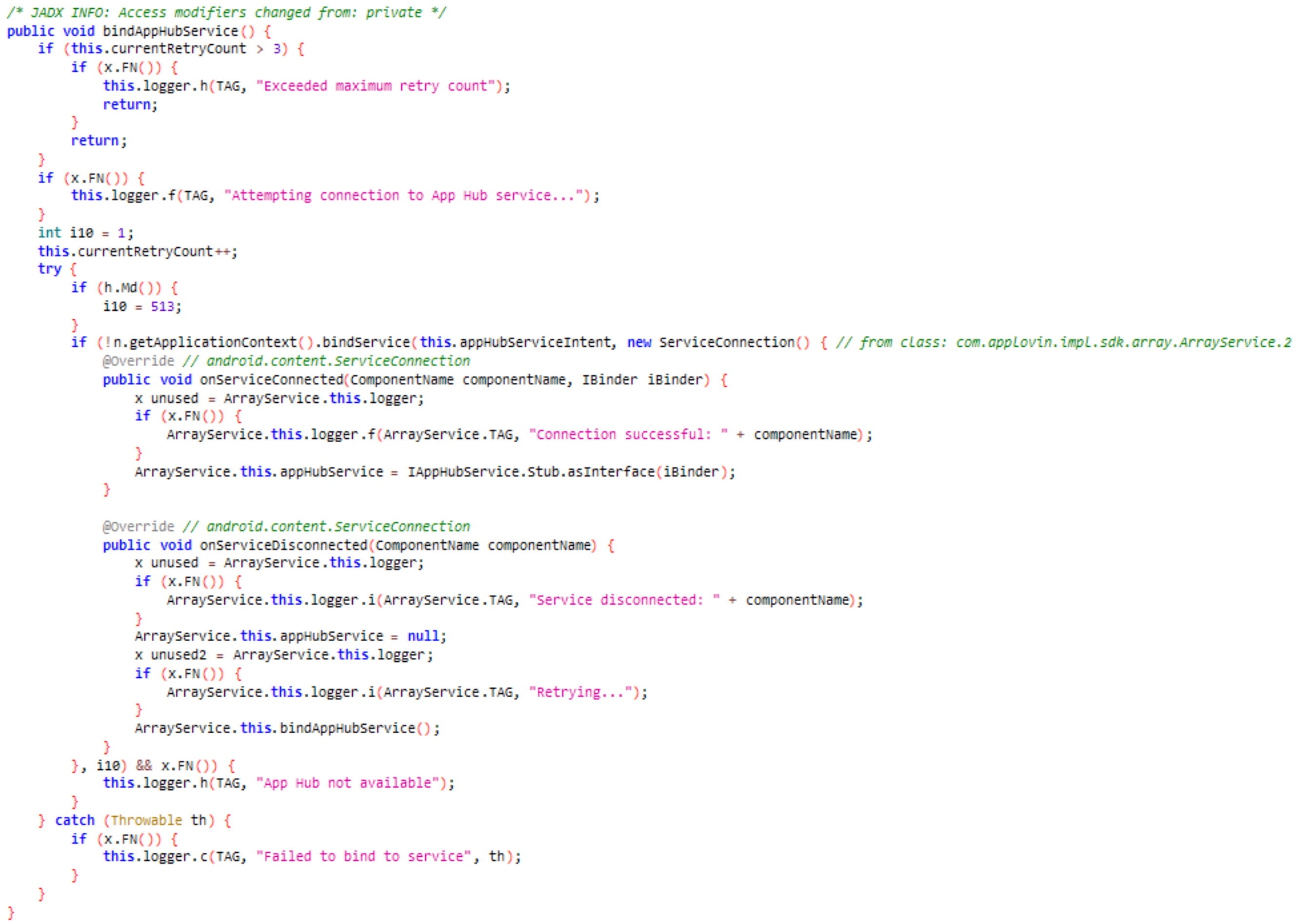


```
<service
    android:name="com.applovin.oem.am.android.external.AppHubService"
    android:exported="true">
    <intent-filter>
        <action android:name="com.applovin.am.intent.action.APPHUB_SERVICE"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</service>
```

ArrayService from Subway Surfers binds to AppHubService (Below is the constructor for ArrayService in Subway Surfers. Highlighted in blue is the call of the binding function, which is shown further below:

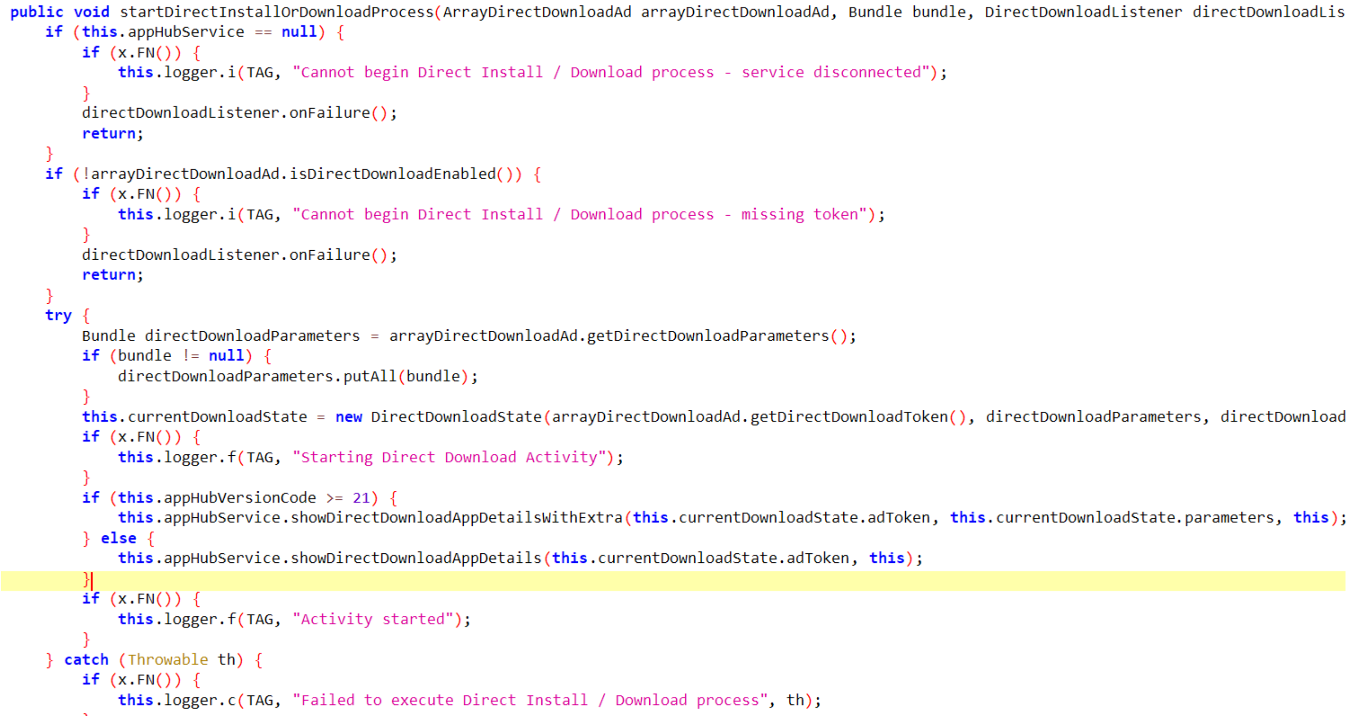


```java
public ArrayService(n nVar) {
    this.sdk = nVar;
    this.logger = nVar.Cq();
    this.dataCollector = new ArrayDataCollector(nVar);
    Intent createAppHubServiceIntent = createAppHubServiceIntent();
    this.appHubServiceIntent = createAppHubServiceIntent;
    if (createAppHubServiceIntent != null) {
        bindAppHubService();
    }
    nVar.Ce().a(new a() { // from class: com.applovin.impl.sdk.array.ArrayService.1
        @Override // com.applovin.impl.sdk.utils.a, android.app.Application.ActivityLifecycleCallbacks
        public void onActivityStopped(Activity activity) {
            DirectDownloadState directDownloadState = ArrayService.this.currentDownloadState;
            if (ArrayService.this.appHubService != null && directDownloadState != null) {
                try {
                    x unused = ArrayService.this.logger;
                    if (x.FN()) {
                        ArrayService.this.logger.f(ArrayService.TAG, "Dismissing Direct Download Activity");
                    }
                    ArrayService.this.appHubService.dismissDirectDownloadAppDetails(directDownloadState.adToken);
                    directDownloadState.listener.onAppDetailsDismissed();
                    ArrayService.this.currentDownloadState = null;
                } catch (RemoteException e10) {
                    x unused2 = ArrayService.this.logger;
                    if (x.FN()) {
                        ArrayService.this.logger.c(ArrayService.TAG, "Failed dismiss Direct Download Activity", e10);
                    }
                }
            }
        }
    });
}
```



```java
/* JADX INFO: Access modifiers changed from: private */
public void bindAppHubService() {
    if (this.currentRetryCount > 3) {
        if (x.FN()) {
            this.logger.h(TAG, "Exceeded maximum retry count");
            return;
        }
        return;
    }
    if (x.FN()) {
        this.logger.f(TAG, "Attempting connection to App Hub service...");
    }
    int i10 = 1;
    this.currentRetryCount++;
    try {
        if (h.Md()) {
            i10 = 513;
        }
        if (!n.getApplicationContext().bindService(this.appHubServiceIntent, new ServiceConnection() { // from class: com.applovin.impl.sdk.array.ArrayService.2
            @Override // android.content.ServiceConnection
            public void onServiceConnected(ComponentName componentName, IBinder iBinder) {
                x unused = ArrayService.this.logger;
                if (x.FN()) {
                    ArrayService.this.logger.f(ArrayService.TAG, "Connection successful: " + componentName);
                }
                ArrayService.this.appHubService = IAppHubService.Stub.asInterface(iBinder);
            }

            @Override // android.content.ServiceConnection
            public void onServiceDisconnected(ComponentName componentName) {
                x unused = ArrayService.this.logger;
                if (x.FN()) {
                    ArrayService.this.logger.i(ArrayService.TAG, "Service disconnected: " + componentName);
                }
                ArrayService.this.appHubService = null;
                x unused2 = ArrayService.this.logger;
                if (x.FN()) {
                    ArrayService.this.logger.i(ArrayService.TAG, "Retrying...");
                }
                ArrayService.this.bindAppHubService();
            }
        }, i10) && x.FN()) {
            this.logger.h(TAG, "App Hub not available");
        }
    } catch (Throwable th) {
        if (x.FN()) {
            this.logger.c(TAG, "Failed to bind to service", th);
        }
    }
}
```

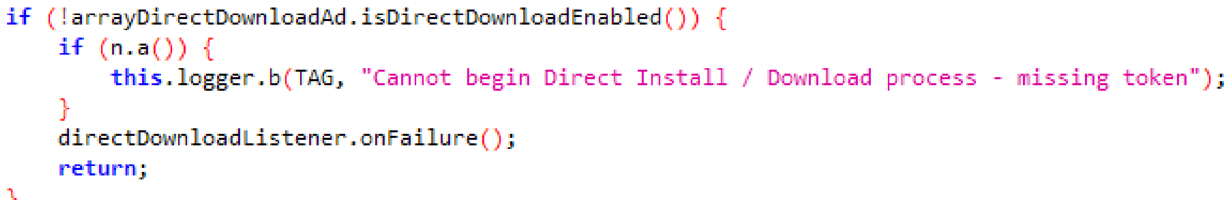
Going back to the startDirectInstallOrDownloadProcess function. Once Subway Surfers has successfully connected or "binded" to AppHub, startDirectInstallOrDownloadProcess checks if the ad's isDirectDownloadEnabled is true. If it is true, then the function begins installing the advertised app via ArrayService's connection to AppHub service.



```
public void startDirectInstallOrDownloadProcess(ArrayDirectDownloadAd arrayDirectDownloadAd, Bundle bundle, DirectDownloadListener directDownloadLis
    if (this.appHubService == null) {
        if (x.FN()) {
            this.logger.i(TAG, "Cannot begin Direct Install / Download process - service disconnected");
        }
        directDownloadListener.onFailure();
        return;
    }
    if (!arrayDirectDownloadAd.isDirectDownloadEnabled()) {
        if (x.FN()) {
            this.logger.i(TAG, "Cannot begin Direct Install / Download process - missing token");
        }
        directDownloadListener.onFailure();
        return;
    }
    try {
        Bundle directDownloadParameters = arrayDirectDownloadAd.getDirectDownloadParameters();
        if (bundle != null) {
            directDownloadParameters.putAll(bundle);
        }
        this.currentDownloadState = new DirectDownloadState(arrayDirectDownloadAd.getDirectDownloadToken(), directDownloadParameters, directDownload
        if (x.FN()) {
            this.logger.f(TAG, "Starting Direct Download Activity");
        }
        if (this.appHubVersionCode >= 21) {
            this.appHubService.showDirectDownloadAppDetailsWithExtra(this.currentDownloadState.adToken, this.currentDownloadState.parameters, this);
        } else {
            this.appHubService.showDirectDownloadAppDetails(this.currentDownloadState.adToken, this);
        }
        if (x.FN()) {
            this.logger.f(TAG, "Activity started");
        }
    } catch (Throwable th) {
        if (x.FN()) {
            this.logger.c(TAG, "Failed to execute Direct Install / Download process", th);
```

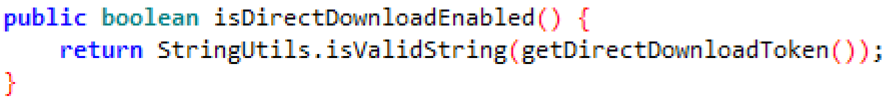
Appendix B: Code Review RE: Direct Download Tokens

The startDirectInstallOrDownloadProcess() code also indicates that direct downloads occur only if a required "download token" is sent, by AppLovin to the app/SDK, to authorize a direct download. Copying from within startDirectInstallOrDownloadProcess():



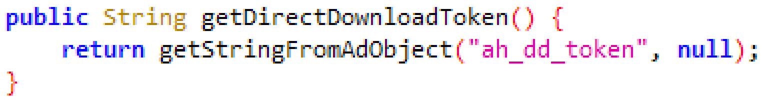
```
if (!arrayDirectDownloadAd.isDirectDownloadEnabled()) {
    if (n.a()) {
        this.logger.b(TAG, "Cannot begin Direct Install / Download process - missing token");
    }
    directDownloadListener.onFailure();
    return;
}
```

The underlying isDirectDownloadEnabled():

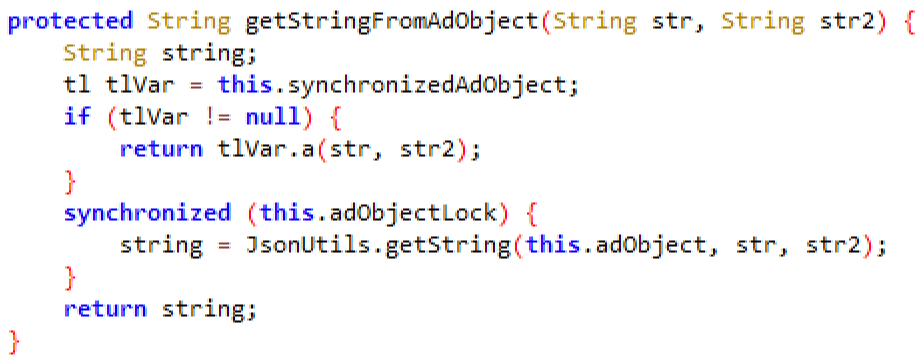


```
public boolean isDirectDownloadEnabled() {
    return StringUtils.isValidString(getDirectDownloadToken());
}
```

The token is retrieved from within the ad object (i.e. delivered along with ad creative):

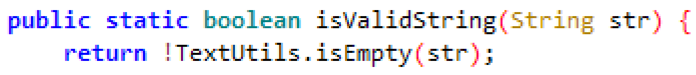


```
public String getDirectDownloadToken() {
    return getStringFromAdObject("ah_dd_token", null);
}
```



```
protected String getStringFromAdObject(String str, String str2) {
    String string;
    tl tlVar = this.synchronizedAdObject;
    if (tlVar != null) {
        return tlVar.a(str, str2);
    }
    synchronized (this.adObjectLock) {
        string = JsonUtils.getString(this.adObject, str, str2);
    }
    return string;
}
```

It turns out “isValid” just means nonempty:



```
public static boolean isValidString(String str) {
    return !TextUtils.isEmpty(str);
```

Appendix C: Tower War Reviews

“Sincerely one of the best time Killers its strategic it's great game I couldn't recommend a better game to you but it just ruined it by putting an ad after every single round retarded I quit playing it for 3 years used to be the greatest and now it's not even on my list” – Tower War Review, February 15, 2025

“...Every update add more ads and make game worse...” – Tower War Review, February 11, 2025

“*There's at least 4 ads after every level. It's absurd, and getting worse by the day. Don't bother, unless you're in it just to watch the same ads over and over again.”* – Tower War Review, February 8, 2025

“*I love this game, but it has too many ads! I used to get an ad every three levels, but now I get one after every level. I'm thinking about deleting the game if they don't change this.”* – Tower War Review, December 29, 2024

“It's embarrassing. This used to be my favourite game to commute, but now it started having adds of dating apps and porn games, the adds displays semi naked people and it's embarrassing to have this in public.” – Tower War Review, December 22, 2024

“Used to be a great game, way too many ads now.” – Tower War Review, December 17, 2024