AppLovin (APP) – Formers Allege Ad Fraud; Is DTC Hype Actually 'Stealing' Meta's Data; Illegal Tracking of Children & Serving Sex Ads to Kids

by Fuzzy Panda Research / in AppLovin

AppLovin (APP) is an ad-tech company in the mobile gaming space. In recent years, AppLovin has had exceptional revenue growth while growing EBITDA and cash flow even faster. The impressive financial performance has turned AppLovin into a Wall Street darling with its shares up +>3,600 % since 2023. Some investors and former employees have even praised AppLovin's CEO, Adam Foroughi, as the next Mark Zuckerberg. But no one seems to know what AppLovin does. The company credits its success to Axon 2.0, a black-box machine-learning (ML) algorithm that serves as the "matchmaker" between advertisers and publishers.

Our research discovered that Axon 2.0 is the nexus of a House of Cards built upon tactics that formers and experts refer to as **"Ad Fraud."** We believe AppLovin has pulled every trick in the book. We've been told they are stealing data from Meta in their e-commerce push. We also discovered AppLovin exploiting consumers and their data in ways which are clear violations of Google and Apple's app store policies.

We are short AppLovin. We believe these so-called dark ad practices explain the truth behind how AppLovin seems to have achieved its great growth. We believe Apple, Google, and Meta all have a vested interest in putting a stop to it.

Our research into AppLovin discovered:

- The bull thesis focuses on expanding TAM from mobile games into e-commerce, but experts say the early e-commerce success came from **"Copying Meta's Homework"** by **"reverse engineering" Meta's data**.
  - Experts said "Facebook is getting the great ROAS… and **AppLovin is just stealing the credit**."
- We were told AppLovin e-commerce playbook reverse engineers Meta's data in the following ways:
  - APP convinces e-com customers to use an AppLovin SDK for mediation.
  - APP requires $600k of monthly Ad spend to join the beta, which doesn't make sense.
  - This allows AppLovin to "peek" at a large enough sample of Meta's successful ads via their mediation platform.
    - APP allegedly then knows which customers are most likely to convert.
  - APP's MAX ad auction bidding platform then gives them a real-time view into Meta's $ bids and values for each consumer.
  - APP also requires e-com companies to use the exact same Meta ads enabling AppLovin to serve up the same winning ads that Meta would have.
  - AppLovin allegedly combines all these data points with 3rd party data brokers and an AppLovin tracking IDs to **reverse engineer Meta's valuable data**.
  - This apparently allows AppLovin to know which consumers are the likeliest to **convert and then front-run Meta**.
- We uncovered a **confidential study** which found an **impossibly high correlation >12.7 std deviations between AppLovin e-commerce targeting & Meta's**.
  - E-com founders told us of similar experiences – **"When Meta dips in performance, AppLovin is also dipping in performance."**
- Meta Senior Executives said if/when AppLovin is caught, **"Meta will shut it down."**
- AppLovin has impossibly high CTRs (click-thru rates) of 30-40%, 10x the industry norms. Formers and Experts told us this was obvious evidence of what they best described as **"Ad Fraud**."
- We played AppLovin games and experienced the shady ads first hand and discovered:
  - **"Manipulative End Card Practices"** in ads where close buttons "X" and skip ">>" do the exact opposite and instead open the App Store.
  - Ad Experts told us "**[AppLovin] is making money on fake activity**."
  - Ads which are programmed to "click themselves" and open the App Store. We saw this in the code too.
  - Multiple other dark ad practices, like unreadable ads and UX tricks meant to coerce an unintentional install.
  - Experts say the shady ad tactics are obvious due to impossibly high CTRs (click thru rates).
- We found ~25% of AppLovin's AI Team came from Meta.
- Our tests on Children's Devices Uncovered **AppLovin Serving Sex Ads to 7- & 12-year-old girls**
- **AppLovin appears to be Illegally Tracking Children**.
  - "**Do Not Track" children accounts** were assigned a **unique identifying number by AppLovin that persists across multiple apps**.
  - Studied an **older version of the SDK**. **It revealed AppLovin collecting 50 attributes on kids** that could enable the company to **fingerprint children and track their locations**.
  - We learned user data is sent to third-party data brokers to enhance the fingerprinting.
  - MoPub, MoProblems – MoPub previously was sued for this exact behavior.
- Undisclosed lawsuit against AppLovin alleges **tracking users without consent** even when location services are turned off.
- **Tracking children without consent is both illegal** and **will likely result in AppLovin's SDKs getting kicked out of the Apple iOS & Google stores.**

Culper Research, another short-seller, shared some of their research with us that we believe, if correct, is a major revelation. Culper believes they uncovered code that appears to enable AppLovin to directly download apps onto consumers' phones without their knowledge or approval. The AppLovin direct download program appears to have begun right at the end of 2022, which is when AppLovin's high margin software revenue began exploding.

- **Culper Research reveals "Direct Download" program as AppLovin's suspected major revenue driver**.
  - Culper believes AppLovin made deals with Samsung, T-Mobile, Sprint, and Indonesia-based OPPO to enable the direct download of apps onto Android phones w/out actual engagement.
  - In a direct download if there is zero cost to install — could AppLovin be booking 100% gross margins on some of its installs?
  - This began at the end of 2022; right when high margin revenue growth took off.
- We **confirmed the direct download program** with a Mobile gaming C-suite Executive.

- Culper found former employees bragging that Direct Downloads are the "Top Revenue Driver."
- Culper says they verified the spikes in downloads via individual apps download data.
- Culper also discovered AppLovin senior management's history of deep connections to "notorious spyware" and "scammy ad" companies.

We also tested T-Mobile devices and found preinstalled bloatware on Android devices that could enable AppLovin to trigger "silent installs." The code looks like AppLovin can do "direct downloads" without user approval.

- Renowned Ad Fraud researcher found "AppLovin's source code contains repeated references to 'direct download.'"

We think AppLovin's fate is clear. Even without large fines by the FTC or for violating California privacy laws, the power to stop AppLovin's atrocious business practices lies in the hands of three of the largest tech companies – Apple, Google and Meta. All of them say they are committed to protecting their users, and more importantly all of them directly compete with AppLovin.

We believe:

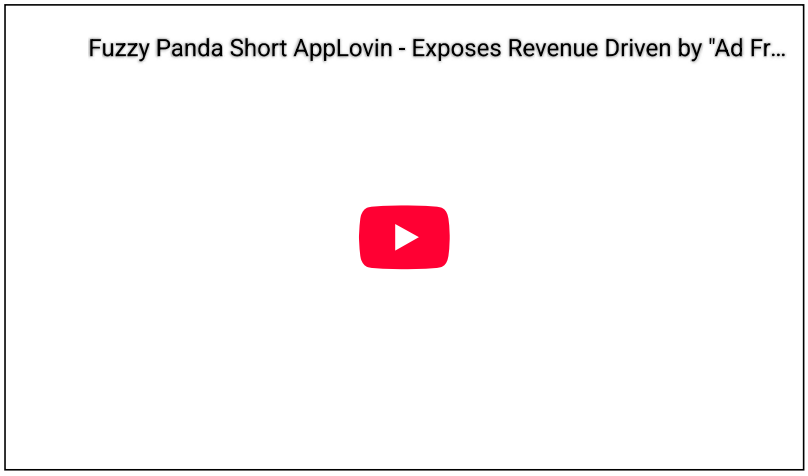
- Apple will likely kick out AppLovin SDKs and/or AppLovin gaming apps that are caught tracking children, violate children's privacy, or that engage in illicit fingerprinting.
- Google will likely have no choice but to ban AppLovin SDKs for numerous violations of Google Play Store policies. Plus, based on Culper's "Direct Download" discovery, we think Google will have no choice but to stop the loophole that is reportedly AppLovin's top revenue driver.
- Meta now knows that AppLovin could be stealing their data and some of their e-commerce revenue. We believe Meta will act quickly to "shut it down."

AppLovin has been playing a dangerous game and is risking a permanent ban from the duopoly mobile app store platforms that controls the gateway to >99% of the market.

We are short AppLovin (APP) because we think major technology companies are going to hit AppLovin where it hurts … right in the ROAS.

Fuzzy Panda Research is Short AppLovin (APP)

Fuzzy Panda Research and Fuzzy Panda "Affiliates" are short securities of AppLovin (APP). Fuzzy Panda Research and Culper Research respectively shared some of our findings during the course of our independent research into APP and prior to the publication of this report. Please see additional disclosures at end of report and in our terms of service.



INTRODUCTION – The Black Box – Short AppLovin

What is Hiding in AppLovin's Black Box?

AppLovin's secret sauce, the Axon 2.0 AI that is credited for driving the company's exceptional revenue and EBITDA growth, is a black box.

Management preaches that Axon 2.0's performance has driven advertising revenue up 380% to >$3.2bn LTM. But how can that be? AppLovin spent $640m on total R&D in FY 2024 and appears to only have ~20 AI engineers on its research science team (5 of which came from Meta … more on that later). This is a pittance of what major AI companies are spending.

Through our interviews and data analysis we found AppLovin is:

- Hiding what Data is Collected from Users;
- Ad Behavior Changes When APP Knows it is Being Watched;
- Hiding Data from their Own Employees; and
- Hiding the Ads from DTC Customers.

Hiding the Fingerprinting Data Being Collected? – AppLovin currently goes to great lengths to obfuscate the data that it sends to its servers. We dug through the data AppLovin is sending/collecting when ads are served and APP's current SDK obfuscates the data collected via proprietary encryption/encoding. But we also found an older AppLovin SDK that's still in use (v10.3.5) and were able to discover it sending a large amount of personal tracking data belonging to a 10-year-old boy that could be used for "fingerprinting." We think the reason AppLovin is hiding the data its SDKs collect is to obscure practices that would violate Apple and Google rules against tracking children.

Hiding When Outsiders are Watching – The strangest behavior we observed in AppLovin's ads emerged when our tech team signaled that we were monitoring the data exchange. Suddenly, AppLovin's ads appeared to behave! Those horrible ad experiences disappeared, skip and close buttons suddenly worked consistently. We think we might have observed the ads behaving differently when AppLovin believes someone might be watching them.

Hiding Data from Employees – AppLovin's own former employees say they often didn't have access to same amount of performance data that was standard at other tech companies.

Hiding Where Ads are Shown from Advertisers – AppLovin's new DTC Customers told us that APP refuses to tell them where the ads run and to whom they are being shown. AppLovin also does not allow marketers to target by group or demographic profiles, the advertisers said, and APP does not even let companies deselect for their current customers.

> "You do not get to know where (the ads) run and that's a limiting aspect of it … they will never have interest-based targeting … in the sense of you have no direction of controls"
>
> ~DTC Company Co-Founder

Why doesn't AppLovin's data advantage make sense?

What is AppLovin hiding in its black box?

PART I – "Copying Meta's Homework" – Short AppLovin

Experts Say AppLovin Is Copying Meta's Targeting Data in DTC E-Commerce Push

- Experts Believe AppLovin is "Stealing" Meta's Data
- Confidential Study Claims to Corroborate Theft of META's Data
- AppLovin Insists E-Com clients Advertise on Meta – And Use the Same Ads on Both Platforms

> "Facebook is getting the great return on ad spend and **AppLovin is just stealing the credit**"
>
> ~ Ad Fraud Expert C

How is AppLovin suddenly able to get great metrics and target e-commerce customers with results that closely match Meta's?

It seems too good to be true, and we think it is. So do experts. Advertising experts told us that AppLovin was essentially copying its homework from Meta, the industry leader in mobile e-com advertising. We spoke to multiple former and current senior Meta employees, and they told us there is no way that the relationship is symbiotic, and that Meta likely would not have any need for AppLovin's data.

Why would AppLovin insist its e-commerce customers spend >$600k a month on Meta advertising and use their top Meta ads with AppLovin?

Experts Explain How AppLovin Could "Steal" Meta's Data

Multiple AdTech experts said they think the reason AppLovin's e-com ads produce ROAS similar to Meta's is likely rooted in AppLovin having found a creative solution for how to harness and piggyback on Meta's user PII and rich targeting data.

> "**They're taking a bunch of different data points that Meta sends in different contexts**. And then if you combine them together, **it creates a persistent identifier**."
>
> ~Ad Executive D

Experts first explained that Meta does not need AppLovin. Second, they told us that these incremental ad dollars to AppLovin are essentially directly coming from Meta's bottom-line. This is the exact opposite to what Adam Foroughi told investors in the Q4-2024 earnings call.

Below is our best effort at summarizing multiple ad tech experts' viewpoints on the very complicated way that AppLovin reverse engineers Meta's targeting methods:

They explained their theory of how they believe that AppLovin is able to see who Meta is targeting with specific ads. AppLovin sees the real-time prices Meta is bidding on the AppLovin "MAX" platform. That data is one of the keys for AppLovin to "copy" or essentially "reverse engineer" Meta's targeting. The experts believed this is why it is essential that AppLovin advertisers also spend $600k a month on Meta – AppLovin needs the same customers so it can replicate Meta's targeting strategy for each brand.

The required Meta ad spend could be so there is a significant sample size of Meta's data flowing through AppLovin's mediation platform. Thus, AppLovin can see which Meta Ads have been winning via mediation and also see exactly who the highest value targets are via current Meta bids on the AppLovin's ad auction network. Having the same ads makes it even easier for AppLovin.

The experts told us that AppLovin likely then combines the Meta bid information, the AppLovin device fingerprint, and data being bought from third party data brokers (that includes a vast amount of personal information) to essentially "steal" Meta's data on consumers. AppLovin then can use that info to enhance their own fingerprint of a user and then bid similar prices for users when targeting them with AppLovin served ads.

It's a clever strategy, but one that we heard will turn into a disaster once AppLovin is caught by Meta. When that inevitably happens, executives and formers at the social media giant told us that Meta would shut it down immediately.

> "You don't want to poke the bear… **Meta would shut it down**."
>
> ~ Meta Senior Executive

David Nyurenberg, an advertising executive, publicly raised these same questions about AppLovin's targeting and its reliance on Meta that are now being widely asked in a recent LinkedIn post.

Confidential Data Study Being Released Soon?!?

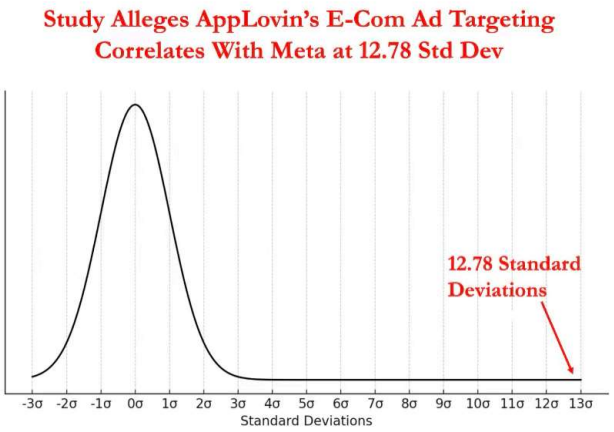
Study Exposes AppLovin's Theft of Meta's Data—Finds AppLovin & Meta Targeting Correlated >12 Std Deviations

We uncovered a confidential analysis by a whistleblower and AdTech expert that says they utilized multiple of AppLovin's DTC E-com advertisers' actual performance data in their analysis. The whistleblower told us their statistical analysis found AppLovin's e-commerce ad targeting correlates with Meta's at 12.78 standard deviations.

That is a one-in-a-trillion probability.

It's more likely that Drake and Kendrick will become besties.

Another expert told us the statistical analysis proves AppLovin is "quite literally stealing the secret sauce" that powers Meta.



Source (Fuzzy Panda Research Chart of standard deviation graph with 12.78 standard deviations)

Unfortunately, we cannot publicly release this study today as the whistleblower(s) who executed the analysis evidently sold the rights to publish their analysis to a hedge fund with an expertise in short-selling.

Thus, we have not been able to independently review or confirm their analysis. We have reviewed a summary of the analysis and believe it to be credible. We are including references to it within our report because we believe investors deserve to know of its existence. We believe this "damning" study will likely be published soon and can't wait to scrutinize the results.

The study's conclusions also map with other e-commerce customers who told us that their results on AppLovin track the results they see on Meta but not on other networks, like YouTube or Pinterest.

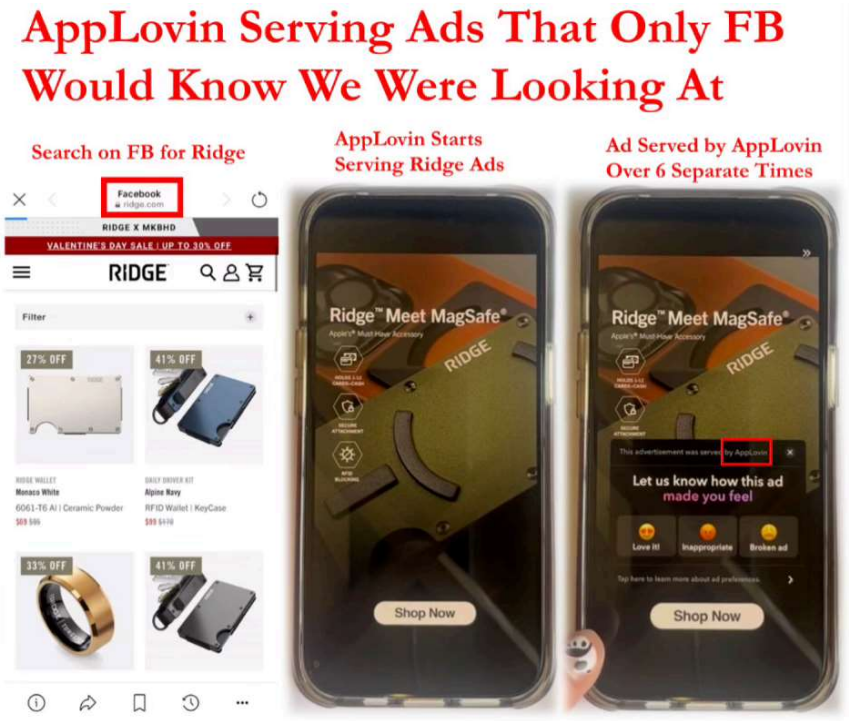
> "**When Meta dips in performance, AppLovin is also dipping in performance**,"
>
> ~ DTC company co-founder

How Does AppLovin Know Our Facebook Searches?

In multiple instances during our research, we searched for products on Facebook and then we were promptly served ads for the same products by AppLovin.

Example 1 – AppLovin Knowing our Facebook Searches? We searched for Ridge wallets on Facebook on an iPhone.* Then we began playing an AppLovin game, "Happy Glass" and were immediately served ads for Ridge wallets. The ads continued at each game level instead of the ads for other AppLovin games that we were typically served when playing.

** – Please see the process for how to ensure retargeting isn't via an AppLovin pixel on the Ridge webpage in Appendix B*



Example 2 – AppLovin Knowing our Facebook Marketplace Searches – In another instance, a member of the Fuzzy Panda research team had been searching for hot tubs on Facebook marketplace. Then suddenly that person began to be served ads in AppLovin games for hot tubs. *(Did AppLovin's magical Axon 2.0 AI figure out that we actually prefer the movie "Hot Tub Time Machine" to "Superbad"? You're probably asking, "who the heck searches for a used hot-tub on Facebook Marketplace?" We 100% agree with you. We made lots of internal jokes about this team member's FB marketplace search history.)*

Example 3 – We also searched for the fintech app Robinhood on Facebook. Shortly afterwards we began being targeted by AppLovin for Robinhood ads within AppLovin games.

In all these instances, the data shows that the signals sent seemed to show that the ads were being served by AppLovin on behalf of AppLovin so it is highly doubtful that AppLovin can claim they were serving these ads on behalf of Meta.

But don't take our word for it. You can do this yourself at home!

25% of AppLovin's AI Engineers Came from Meta

AppLovin appears to have only ~20 engineers on staff whose LinkedIn bios make any mention of AI or machine learning. Of those ~20, we only identified 11 people on AppLovin's "Research Science Team," who are charged with developing learning models for AI-powered tools like Axon 2.0.

It must be a huge coincidence that five of the 11 previously worked at Meta. (Source – LinkedIn's 1, 2, 3, 4, 5)

Meta Knows You in Ways AppLovin Never Will

There's a reason you keep clicking on Instagram or Facebook ads (hi mom!) – Meta has turned its vast troves of user data into an industry-leading e-commerce advertising machine.

> "Meta is so successful because they have that first party data … AppLovin has none…the only way this DTC game works is if you have that [Meta's] data."
>
> ~ Ad Fraud Expert C

Other social networks like TikTok and Pinterest do the same, though not as well because they don't have as comprehensive of a picture of users. Outside of social, most e-commerce advertising is little better than a crapshoot, experts and marketers said.

Applovin appears to know less about its users than even Pinterest. In an interview from 2019 AppLovin's CEO, Adam Foroughi explains, "[We] don't know anything about the individual. I don't even know if it's an individual, male or female." So, what has changed since 2019? Do games yield that much user data?

Is AppLovin's E-Com Hype Already Dying Off?

Excitement was originally driven by free ad credits and the hope for a new mobile e-com platform. But our conversations and research showed it has since slowed.

The co-founder of a small DTC apparel company who has been widely cited in positive stories about AppLovin poured cold water on AppLovin's e-commerce hype. They told us that the excitement around AppLovin's consumer push is already dying down.

> **"It was hype city, but it's died off like crazy. Nobody is talking about it anymore."**
>
> – DTC Company Co-Founder

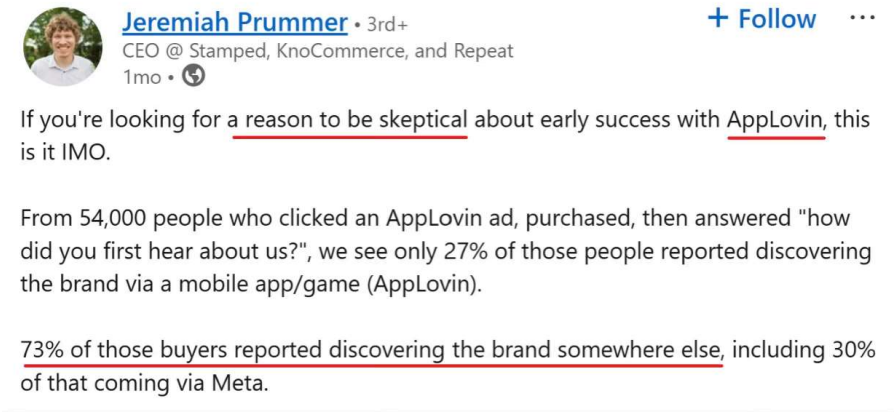
Another early AppLovin customer has seen the excitement dissipate:

> "You all still spending on Applovin? It has gone pretty quiet on here."
>
> ~ Cody Plofker, CEO of Jones Road Beauty in a tweet

Survey Says … 73% of AppLovin E-com Consumers Give Credit Elsewhere:

A survey of consumers for which AppLovin has taken a referral credit found that when asked, those very same consumers said they learned of specific brands from other platforms.

- 73% discovered the brand elsewhere, including 30% on Meta
- Only 1/4 AppLovin shoppers are saying it was AppLovin that did the discovery work



Obvious Major Issues with AppLovin for E-Commerce

Other issues that we have heard from E-Commerce advertisers mention regarding AppLovin's ability to serve DTC Ads are:

- No ability to exclude current customers.
- No visibility into where your ads are served.
- AppLovin won't let E-Com customers target specific demographics – you just have to trust they do it right.
- Inventory – Subpar ad inventory since AppLovin is mobile gaming focused.

PART II – Formers Allege Ad Fraud – Short AppLovin

Formers Allege Ad-Fraud – APP Caught Using Fake Clicks & Other Dirty Tricks To 'Game' Installs

- Shady Ad Practices
- Clickjacking & Click Spoofing? = Monetization of Mistaps? Deliberate False Engagement?
- Code Reveals AppLovin Counting FAKE Clicks & Downloads

> "**Everybody in the industry knows that AppLovin** is full of sh*t and that **it's fraudulent**."
>
> ~Former AppLovin Anti-Fraud Executive B

We interviewed a multitude of industry and ad fraud experts who consistently told us that AppLovin is deeply engaged in "Ad Fraud." We experienced AppLovin's shady ad practices first-hand. We played the games, we analyzed the data APP collected from us, and we discovered a multitude of dark business practices ad fraud experts told us is "100% fraud."

AppLovin primarily charges advertisers on ROAS (Return on Ad Spend) basis or on a Cost Per Install (CPI) or a CPA (Cost per Action) basis. But every accidental mis-click that causes an app installation can lead to a real user, and that is why AppLovin appears to be employing every manipulative ad technique in the book.

These bad ad practices also put AppLovin in a position to claim credit via Adjust, the mediation network it owns, which cannibalizes what would have otherwise been organic free installs for independent gaming companies.

We engaged renowned ad fraud researcher Ben Edelman — previously HBS faculty member, later a Chief Economist at Microsoft — to help us analyze some of AppLovin's ad practices.

> "I encountered a significant number of elements to cause **inadvertent ad clicks**. First, Applovin routinely showed **ads with fake user interface elements** including instructions like ads reading "drag to move" or "swipe to run", seemingly playable right there within the ad, but actually the play features didn't work. If a user followed the text instructions within the ad to, supposedly, interact with the ad, **the ad instead opened Google Play to install the game**. Second, Applovin ads **intentionally blocked closing and exiting an ad,** including presenting these buttons only with a delay and alternating between different corners of the ad.
>
> ~Ben Edelman

Dark Ad Practices We Experienced Included:

- Testing games revealed the AppLovin SDK sending messages to its servers that appear to be false interactions
- Clickjacking/Click Spoofing?
  - User hit "X" to close = ad interaction recorded + opened App Store.
  - User hits ">>" to skip = ad interaction recorded + opened App Store.
- Fake Clicks = more Downloads?
  - User takes NO action = ad interaction recorded + opened App Store.
  - Unplayable in-game ads that coerce consumers to click download.
- False Impressions?
  - Ads that are too small to see; yet APP appears to record an impression.
  - Game design that causes user to swipe through an ad
- Ads that bypassed Child Protection settings.

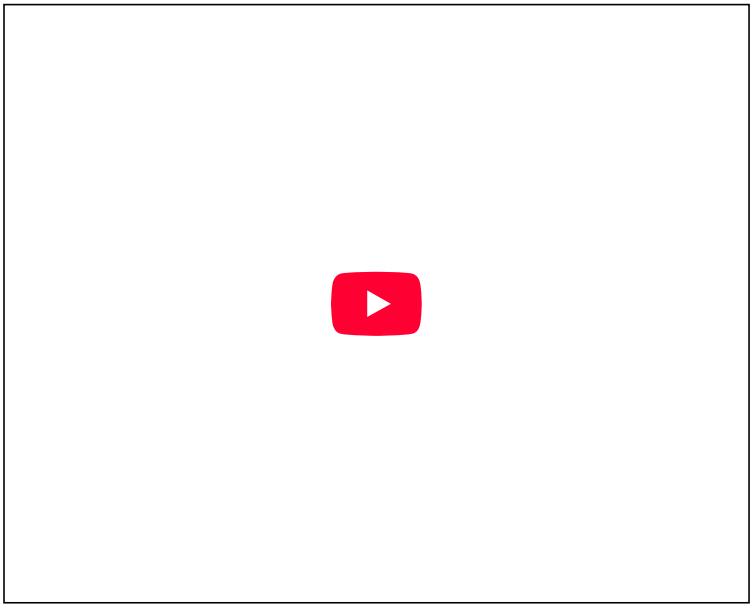
Data Reveals APP SDK Sending Obfuscated Messages That Appear to Be False Interactions:

Analyzing the network traffic sent by AppLovin's SDK reveals that it is likely sending false impression data and potentially counting user interactions that never occurred. A consumer touches absolutely nothing during an ad, yet the AppLovin ad programmatically opens the Apple/Android App Store for a new download and sends an obfuscated message to AppLovin's own mediation server and it looks similar to when a user click is recorded.

In this issue reported on Github, you can see that AppLovin ads are specifically configured to enable that behavior.

- "`isAutoOpenOnVideoEnd`" – to enable auto open
- `"skip": {"mode": "OpenAndSkip"}` possibly to enable behavior to open [AppStore] & skip the ad video.

Our Video of Code Revealing False Interactions?



Source – FPR Video AppLovin Ad

The true extent of this practice is masked since AppLovin's SDK sends obfuscated proprietary encrypted messages that hide what exactly APP recorded. Furthermore, APP doesn't disclose the details to its advertisers. We've been told this level of black box encryption is abnormal.

Click Jacking?/Click Spoofing?

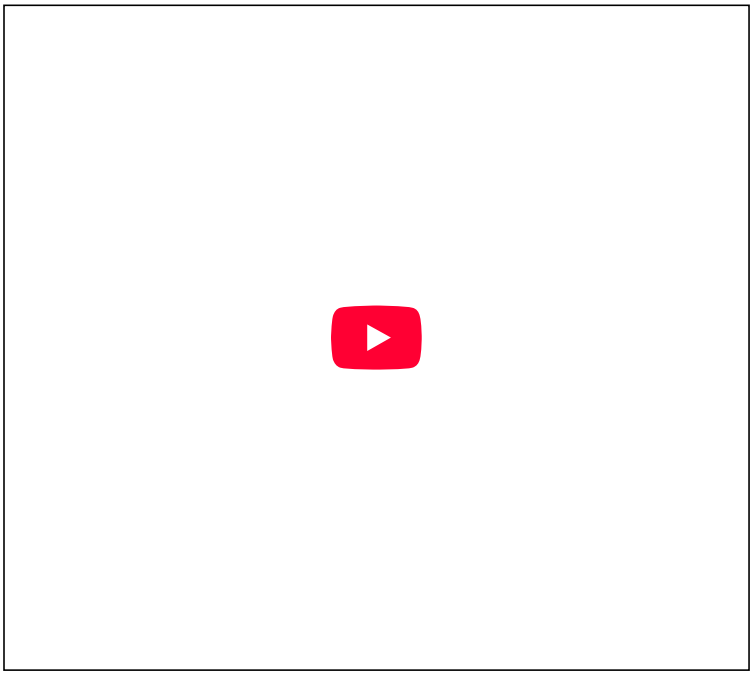
It is no wonder consumers and industry insiders have begun calling AppLovin ads "malware ads."

It is something you have to see to believe.

AppLovin's ad format prompts consumers to click close "X" or skip ">>." BUT instead of closing the ad, AppLovin opens the app store. It's no wonder that AppLovin's install conversion has skyrocketed when they are forcing consumers into the app store instead of letting them exit an ad.

> "They **[AppLovin] are calling a click when it's not a click**. So, all of their metrics look amazing"
>
> ~Former Adjust Executive K

Video of Ad's Opening App Store when 'X' & '>>' Clicked



(Source – FPR Video AppLovin Ad within an AppLovin Game. We reported missing close "X" & skip ">>" buttons. APP ad within an APP game took us to the App store 5 times instead of closing or skipping the ad. A deceptive practice to cause additional downloads)

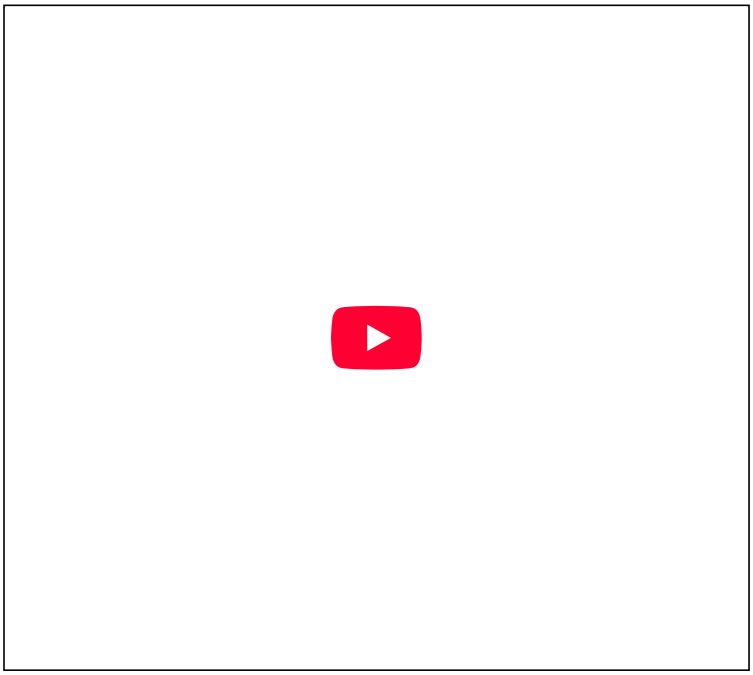
Fake Clicks = More False Downloads?

If a user completely ignores an AppLovin Ad, and they click nothing … the App Store still opens.

The act of completely ignoring AppLovin sends a user engagement message to the AppLovin-controlled mediation service that an interaction with the ad has been registered and then the ad automatically opens the App Store.

> "[AppLovin] is at the forefront of **manipulative end card practices**. Where you think you're clicking out, but it in fact takes you to the App Store, or changing the position of the close button to the other corner, so you think you're going to click on close, but you're actually it actually takes you to the App Store."
>
> ~Former AppLovin Senior Engineer G

Ads that Click Themselves



False Impressions?

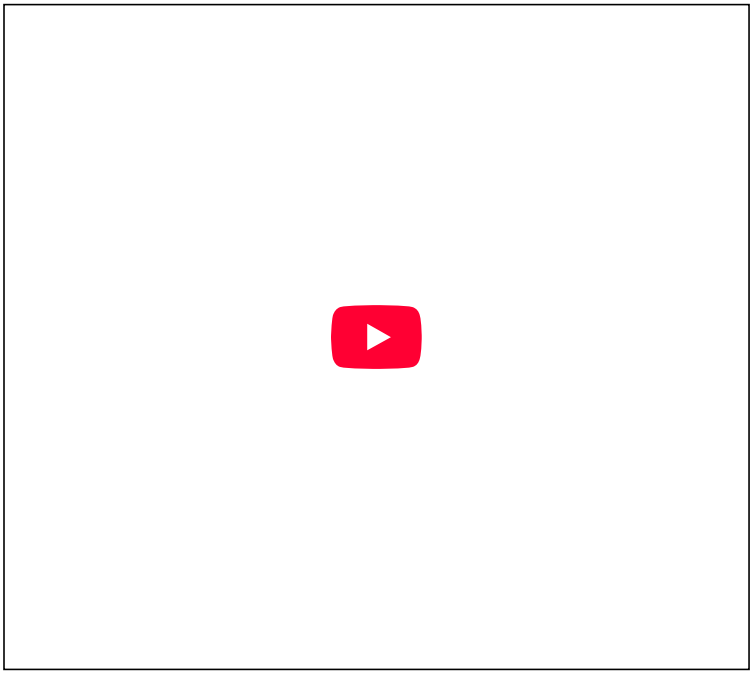
Another deceptive practice by AppLovin includes showing tiny unviewable ads within their game.

At other times, the consumer is forced to swipe directly through the tiny ad to continue game play (see below).

Due to the black box nature of AppLovin's SDK messages we can't confirm if APP is miscounting a forced interaction with the ad as user engagement/false impression. Either way, we wouldn't want to be an E-com advertiser paying for these low-quality CPMs or CPC's when it comes time for AppLovin to choose which ad network should win the attribution.

> "So now **[AppLovin] is making money on fake activity**. This is a **very prolific type of fraud** that's happening…If you think about ad formats and **having a click get sent when no one's clicked anything, that's fraud** and that's perpetrated by them. **That is 100% fraud**"
>
> ~Former Adjust Executive K

Unviewable Ad



Playable Game Becomes Static Screen – Another shady tactic to increase downloads can be found in the UX of AppLovin ads. AppLovin will serve playable videogame ads that then unexpectedly change into a static screen. If the user tries to continue playing the ad, they instead find that they triggered the game to download.

Our tests showed that AppLovin consistently tries to trick/coerce users into accidentally downloading apps or clicking ads that they had no intention of doing. Industry experts told us time and again that they considered practices like this "Ad Fraud."

More Proof = Impossibly High Click Thru Rates – 30-40%

> "AppLovin would always have a **click thru rate north of 30% and a click to install conversion rate of below 0.1%** which by all means tells anybody in the space that knows a little that there's no human involved in the clicking of the ads."
>
> ~ Former AppLovin Anti-Fraud Executive B

Advertising executives told us that in their tests and analysis they saw the same obviously "too good to be true" click through rates:

> "I could show you data like we're talking a 30-40% click-through rate on these games, which is completely unbelievable… The average for mobile games is typically 3-5%…**most of these clicks are not legitimate**…I'd go as far as to say **90% of the clicks are bullshit**."
>
> ~Ad Fraud Expert C

Ad Fraud experts told us that only false and coerced downloads can yield reported click-through rates that are so much higher than rates that would be considered good by the industry. To the experts, the abnormally high click-through rates indicate that there are either bot farms involved, malicious code in the ads, or an ad platform is tricking consumers into interactions that they do not actually want to take.

PART III – Short It for the Kids – Short AppLovin

AppLovin is Serving Sex Ads to Kids

- Ads Served to <13 Include Explicit Sexual & Violent Content

We tested multiple children's devices and were shocked by the graphic sexual and violent ads that AppLovin served to children. The ads were cartoons that clearly had been made for children – yet were wildly inappropriate by any measure.

We tested devices for children (7- & 12-year-old girls and a 10-year-old boy) which were all configured as <13 kids and which had parental controls fully enabled. Then we downloaded and played age appropriate AppLovin games.

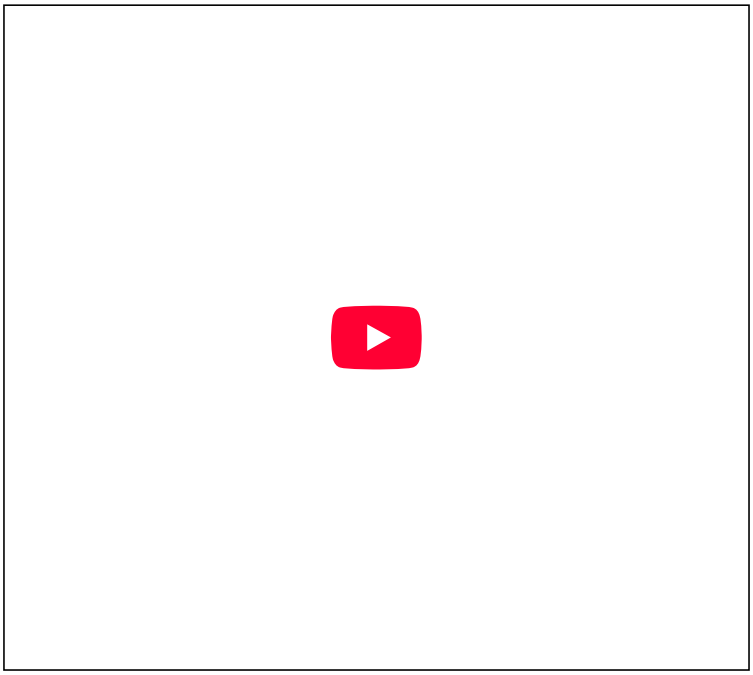
The AppLovin Ads depicted:

- Sex Acts
- Graphic Sexual Situations (including a boss spanking a scantily clad subordinate)
- Violent Sexual Assault & Suicide
- Assaulting the elderly (killing a grandmother, wtf!)

Below is a small subset of the horrific content that AppLovin served children during our tests:

Actual Explicit Ads Shown to 7- & 12-Year-Old Girls by AppLovin:

Video of Sex & Violence Ads shown to Children



AppLovin Appears to be Illegally Tracking Children

- Unique Identifier Follows Kids Across Apps
- Old SDK Reveals 50 Data Attributes Collected to "Fingerprint" Children
- Private User Data Sent to 3rd Party Data Brokers
- Undisclosed Lawsuit on Tracking w/out Consent

As if the explicit and violent ads were not bad enough, we also caught AppLovin games transmitting data that appeared to show the platform tracking children in violation of federal laws and Apple's and Google's app store policies. It is ILLEGAL to track children without explicit permission from a parent.

Our test of a 10-year-old boy's account discovered AppLovin:

- Issuing a unique CUID number that follows the 10-year-old across apps
- Collected additional data to assign a "fingerprint" to children specifically marked "Do Not Track"
- Combining those items with third-party broker data to enhance the fingerprint and effectively track children

Former employees confirmed that AppLovin did NOT stop fingerprinting consumers after Apple released iOS 14.5 and tightened its privacy controls.

> "Back then when Apple announced iOS 14, they said that when 14.5 will be released, **fingerprinting will be disabled. Never happened**. And so yeah, **obviously while this thing is not mandatory, why would someone stop themselves from doing it?**"
>
> ~AppLovin Former Employee H

Old SDK Reveals Private Data Collected on Kids

We were considering reverse engineering AppLovin's SDK to see all the data that they were actually collecting on children. But luckily AppLovin decided to save us the money by kindly leaving their older SDK sitting in some of their older Apps to analyze. We found exactly what parents everywhere fear.

In the Old SDK we uncovered AppLovin is collecting 50 different attributes from children's devices including (geolocation data; unique device identification; and even the exact boot-up time to millisecond!).

It might sound mundane but all these data points are essential for AppLovin to be able tell users from the same household apart since multiple household members share the same IP address or use the same wifi. These other attributes are essential for building a fingerprint for devices and allowing AppLovin to distinguish mom or dad's iPhones from lil' Susie's iPad.

All of this data was collected when the users is specifically marked "DO NOT TRACK."

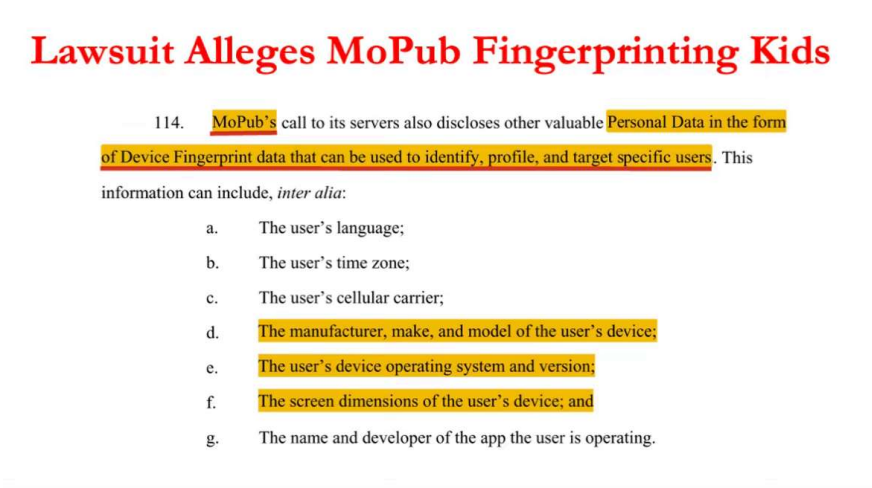
MoPub – Mo'Problems

MoPub Was Sued for Exfiltrating Children's Personal Data

APP subsidiary MoPub was previously sued for violations regarding the collection of children's data. The 2017 lawsuit (which MoPub settled) alleged that MoPub was used to "exfiltrate children's personal data" and that the data could be used to "track children's online behavior."

AppLovin acquired MoPub from Twitter in January 2022 and then merged MoPub into their AppLovin MAX SDK. In our analysis of the AppLovin old SDK, we discovered that AppLovin is still collecting these same personal data attributes from the device of a child, and we have strong reason to believe that the new encrypted/encoded SDK is still collecting this data.

The lawsuit shows MoPub collecting the same specific user data (device id, screen size, operating system, login time to millisecond, etc) as we found AppLovin recently collected on a child.



Lawsuit Alleges MoPub Fingerprinting Kids

114. MoPub's call to its servers also discloses other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific users. This information can include, *inter alia*:

a. The user's language;
b. The user's time zone;
c. The user's cellular carrier;
d. The manufacturer, make, and model of the user's device;
e. The user's device operating system and version;
f. The screen dimensions of the user's device; and
g. The name and developer of the app the user is operating.

Source: Rushing v. Disney – Amended Class Action Complaint

3rd Party Data Brokers Allegedly Used to Build Out Fingerprint on All Users, Including Children:

We have heard from multiple sources (former employees and third-party data brokers themselves) that AppLovin utilizes the unique ID tracking number for all users including children that are listed "do not track" and then enhances the AppLovin tracking data from third party data brokers to create a better "fingerprint" for the user and device.

You can find the >100 data brokers that AppLovin shares your data with by declining their end user license agreement, which will bring up a long list of data brokers that your information is being shared with.

The ONLY Time Adam Pays MORE! – 3rd Party Data Brokers

AppLovin's CEO, Adam Foroughi, is known for his cost cutting and willingness to run the leanest possible organization. We were shocked when we discovered that there was actually an area where Adam & AppLovin was willing to OVERPAY. The one time AppLovin offers to pay more is with data brokers.

One data analytics company explained how AppLovin offered to pay them >50% over their normal rate to enhance AppLovin's user data with their own dataset.

How AppLovin Is Allegedly Tracking Children:

Here is how we believe AppLovin's tracking works for "Do Not Track" individuals:

- Google and Apple mark children's device's "Do Not Track" with a numerical identifier that is a string of 0's. IDFA = "0000-0000-0000"
- AppLovin then assigns another numerical ID to the user, even if it's a CHILD.
- This unique tracking ID persists for the child across all AppLovin apps by the same developer.
- We discovered AppLovin was also sending other data including IP addresses (used to track locations), configuration, device type, screen size, reboot time, etc.
- Combining IDFV/CUID with information about the device like configuration, last reboot time, make and model is enough to "fingerprint" the device for identification and tracking.
- Data brokers told us that AppLovin then enhances this fingerprint via third party data brokers who have additional personal information (email address, phone number, age, etc).
- If permission to track is asked, then it is only asked directly of the child who wants to play a game rather than from the parental account. Tracking permission is often asked in a misleading way to trick encourage the child into accepting. As a result, parental consent for tracking is not given.

Combining Unique Identifiers With 3rd Party Data & Fingerprinting Is Prohibited by Apple

Apple Policy States NO "Fingerprinting"

Developer

App Store

User privacy and data use

Using the AppTrackingTransparency framework

The ID for Vendors (IDFV), may be used for analytics across apps from the same content provider. In this case, the use of the AppTrackingTransparency framework is not required. The IDFV may not be combined with other data to track a user across apps and websites owned by other companies. You remain fully responsible to ensure that your collection and use of the IDFV complies with applicable law.

Can I fingerprint or use signals from the device to try to identify the device or a user?

No. Per the Apple Developer Program License Agreement, you may not derive data from a device for the purpose of uniquely identifying it. Examples of user or device data include, but are not limited to: properties of a user's web browser and its configuration, the user's device and its configuration, the user's location, or the user's network connection. Apps that are found to be engaging in this practice, or that reference SDKs (including but not limited to Ad Networks, Attribution services, and Analytics) that are, may be rejected from the App Store.

Source: https://developer.apple.com/app-store/user-privacy-and-data-use

New Undisclosed On-Going Lawsuit—AppLovin Tracks Users Without Consent

An undisclosed on-going class-action lawsuit filed in California in August 2024 accuses AppLovin of using its Adjust SDK to collect a "wealth of information" and track users without their consent.

- Lawsuit States Tracking Occurs Even When Location Services Are Off
- Complaint States APP Bought Adjust to Bypass Apple Privacy Protections

The lawsuit accuses AppLovin of tracking users even AFTER location services have been disabled.

Undisclosed Lawsuit Alleges AppLovin Tracking Users

51. The Adjust SDK also intercepts and collects personally identifying location data even when location services have been disabled by using a process referred to as "reverse IP lookup."

Source: Mitchell v. AppLovin – Santa Clara County Court Case No. 24CV434574

According to the lawsuit:

- AppLovin uses Adjust SDK to tracks users' precise locations, IP addresses, device IDs and other information about their behavior.
- AppLovin then siphons that location data directly into data brokers and cross-referencing the location data against a commercial database that tracks IP locations.
- AppLovin uses a "reverse IP lookup" to track when users disable location services.
- It does it by intercepting IP address and AppLovin then uses that data and other device information to "fingerprint" users and track across apps and devices.
- This work around allows AppLovin to overcome Apple protections, and fingerprint and track users without consent.

56. The Adjust SDK generates precise geolocation data in this very fashion even when a device's location services are disabled. The Adjust SDK intercepts the device's IP address, then cross-references it against the MaxMind database in order to generate longitudinal and latitudinal coordinates that reflect the device's precise location. The resulting location data is then associated with the MAID or IDFV collected from the device in order to fingerprint users without their consent, just as it does when location services are enabled.

Source: Mitchell v. AppLovin – Santa Clara County Court Case No. 24CV434574

> “When consumers … tried to protect their privacy … [AppLovin] eviscerated those efforts by doing an end-run around those consumer protections.”
>
> ~ Mitchell v. AppLovin

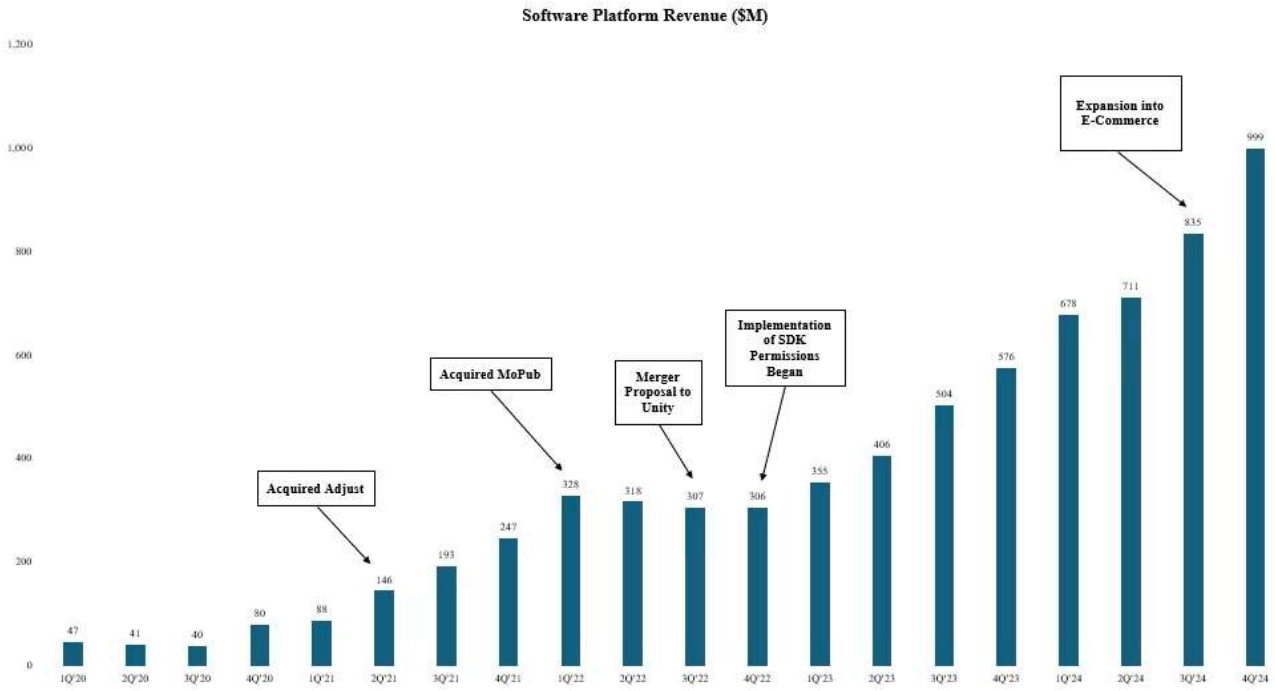
What if Axon 2.0 is Actually the Modern Day Windowless White Paneled Van?

What if the secret sauce for Axon 2.0 really comes from all the private data they have harvested on children and other users? Harvesting children’s data is a violation of both Apple’s & Google’s app store rules and government child privacy laws.

In 2022, AppLovin bought MoPub, which the FTC mentioned had access to kids’ private data. A MoPub lawsuit also alleged MoPub was collecting extensive data on kids and other users. And in our analysis, we learned that AppLovin is still collecting that type of data.

In 2021, AppLovin bought Adjust, which was recently accused in an undisclosed lawsuit of tracking users without their consent.

AppLovin’s software revenue inflected at the beginning of 2023 right after AppLovin acquired both MoPub and Adjust.



Is it possible that the revenue inflection due to Axon 2.0 is really because AppLovin became able to build out a better fingerprint on their users? And is it possible that they were using that enhanced data to better target all users, especially children?

We believe that the secret sauce behind AppLovin’s significant revenue and margin growth could actually be coming from this better “fingerprinting” data on all users, including children. If that is indeed AppLovin’s secret sauce, then does that make Axon 2.0 less like advanced AI and more like the creep lurking around the neighborhood in a white windowless van, but this time he’s trying to take your children’s data?

PART IV – “Adjusting Metrics?” – Short AppLovin

Is AppLovin Adjust’ing its Metrics?

- Adjust Formers Disclose AppLovin was a Worst Offender for “Manipulation”
- APP Fired the Fraud Team After Buying Adjust
- Formers said AppLovin “Whitelisted” Itself and Now “Grades their Own Homework”
- Apple Briefly Banned Apps Using Adjust SDK for Fingerprinting in 2021

AppLovin bought Adjust in 2021 and immediately gave itself a huge advantage in the mobile ad game: Adjust is one of the leading platforms that analyzes lead sources for consumer downloads and then decides which company gets paid for the referral after an install. Before it was bought by AppLovin, Adjust’s anti-fraud suite set the industry standard for identifying and blocking fraudulent traffic like fake installs and click spam.

Former Adjust executives and engineers told us before Adjust was acquired that AppLovin was one of the networks most often tagged for fraud.

> "**AppLovin was one of the biggest accounts when it came to manipulations** … we have had run-ins and escalations with them for years."
>
> ~Former Adjust Executive L

Adjust formers told us that the numbers were very obviously unbelievable. AppLovin would report to Adjust "clickthrough rates >30% when typical ads were lucky to get 1%" and that "those same ads would have a low 0.1% click-to-install conversion rate, indicating that the initial click on the ad was bogus."

AppLovin Even FIRED Most of Adjust's Fraud Team

Formers told us that after buying Adjust AppLovin not only whitelisted themselves but also fired a majority of Adjust's anti-fraud team.

> "[AppLovin] overpaid for Adjust so they could whitelist themselves, **get rid of the fraud team**…**[AppLovin] took out the only people who pointed out how shady they were**."
>
> ~ Former Adjust Executive L

AppLovin Whitelisted Themselves After Buying Adjust – Suddenly 'No More Fraud' Reported

Adjust executives and former AppLovin employees told us that after the Adjust purchase AppLovin whitelisted all their own apps and then low and behold there was "no more ad fraud reported" by Adjust regarding AppLovin.

> "**I know for a fact that Applovin was whitelisted**. So no longer being called out for fraud within Adjust. … And now it was like, no, **there's no more fraud at Applovin**."
>
> ~Former Adjust Executive K

Is AppLovin Using Adjust to "Adjust" its Metrics?

Without Adjust policing the fraud, the former executives and engineers told us that it would be easy for AppLovin to inflate their metrics with the kinds of tricks that give mobile advertising a bad name.

> "Ultimately, AppLovin is really not telling you how transparent that is. In some ways, **they are kind of grading their own homework**, so they function very much like a walled garden."
>
> ~ Industry Executive A

> "You get to grade your own homework and in the case of AppLovin, they also get to grade everybody else's homework."
>
> ~ Former AppLovin Anti-Fraud Executive B

Former executives and engineers say that it is fair to suspect AppLovin is doing just that.

> "**Adjust is refereeing a game in which AppLovin is one of the main players**… people are right to raise their eyebrows considerably."
>
> ~ Former AppLovin Senior Engineer G

Those tricks could include:

- Ads that auto click without the user touching the screen – can also be click spamming
- Bad ad formats that force users to go to App Store and Play Store
- Injecting a fake ad click just before an installation to take credit for it.

DOJ Filed Charges Against PE Sponsor KKR for Hiding AppLovin-Adjust Deals from Regulators

The DOJ recently filed charges against KKR (AppLovin's PE Sponsor) in January 2025 for blatantly ignoring federal disclosure laws by failing to submit the required FTC premerger filings for AppLovin's acquisition of Adjust. KKR's investments in AppLovin and Adjust were specifically named in government complaint v. KKR as key examples of an alleged practice of hiding deals from government regulatory scrutiny.

The complaint states that KKR and AppLovin effectively shielded the deal from regulatory scrutiny, allowing AppLovin to acquire the mediation platform without any input from regulators.

C. For at Least Two Different Transactions, KKR Failed to Properly Notify a Merger or Acquisition at All

24. KKR's HSR Act violations go beyond failing to submit or altering Item 4 documents called for by the HSR Form. KKR violated the HSR Act twice by failing to make premerger HSR filings for at least two qualifying transactions.

25. In December 2021, KKR admitted to the FTC that it did not make premerger HSR filings before closing two acquisitions, Applovin and Adjust. When it submitted corrective filings more than seven months after it had completed those transactions, KKR assured the FTC these failures to file were merely "inadvertent[]" and "exceptional," resulting from "an unusual and unanticipated set of circumstances," and inconsistent with its "internal policies and procedures in place to ensure compliance with HSR." But in fact, KKR's failures to comply with the HSR Act requirements for the Applovin or Adjust acquisitions were not "exceptional"—they were of a piece with at least 14 other HSR Act violations committed before, during, and after the failures it admitted to with regard to Applovin and Adjust.

Source: DOJ v. KKR – Complaint — Case 1:25-cv-00343

PART V – Culper Exposes Direct Download Driving Revenue – Short AppLovin

Culper Research Blows the Lid Off AppLovin's Growth Story & Black Box – "Direct Downloads" Revealed

- Hidden "Direct Download" Code Discovered
- Secret Installation of Apps Began in Late 2022 – Right When Revenue Growth Took Off
- Employees & Gaming Executives Confirm It
- Report Details Sketchy History of AppLovin Executives

We asked a C-Level Mobile Gaming Executive at a private company if their games had experienced the automatic direct downloads that Culper Research disclosed in its research report.

The gaming executive who confirmed Culper's Research told us:

> "**Yes. We had the automatic downloads** happen with T-Mobile…they made the average quality of AppLovin installs worse."
>
> ~Mobile Gaming Executive

Culper Exposes Automatic Downloads Driving High Margin Growth

Culper's forensic code analysis and interviews with former AppLovin' employees revealed that AppLovin is forcing "direct downloads" by exploiting permissions granted by phone carriers and device makers, including Samsung, T-Mobile, Sprint, and OPPO (Indonesian-based phone OEM).

According to Culper's research, AppLovin has been able to force unwanted games potentially onto an estimated 1.4 billion DAUs. The direct downloads appear to be one of the main drivers behind AppLovin's high-margin revenue growth. Culper shows how the real secret of AppLovin's incredible revenue growth appears not to be rooted in Axon 2.0's AI, but in AppLovin's secret double D's – "Direct Downloads."

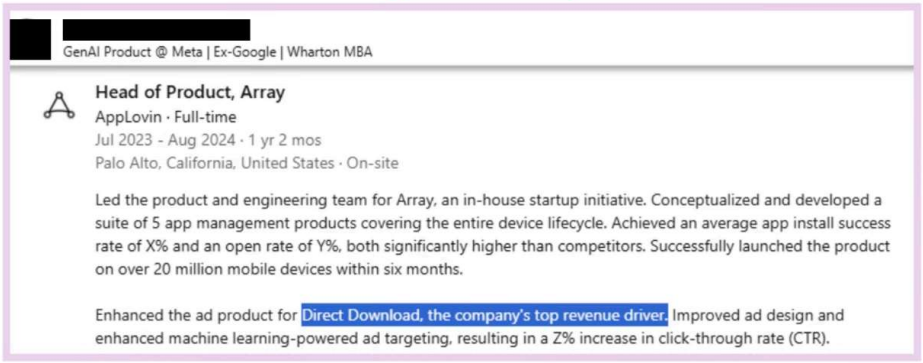
Culper shows that AppLovin began adding what it calls "direct download" permissions to its SDKs in late 2022 and 2023, and Culper even exposes how downloads spiked as games were updated with the new code.

Culper Uncovered AppLovin Employees Bragging About Direct Downloads as the Top Revenue Driver

We aren't sure if it is worse to force apps onto people's phones without their permission or to brag about doing that on LinkedIn. Culper discovered multiple employees confirming the importance of Direct Download on their resumes.

"Enhanced the ad product for Direct Download, the company's top revenue driver." (LinkedIn)

Direct Download = AppLovin's "Top Revenue Driver"



Other AppLovin employees even explained exactly what the direct download program

"Leading transformative partnership negotiation with Samsung, projected to significantly enhance the Direct Download feature on Samsung devices, allowing user to install mobile applications directly" (LinkedIn)

Management's Historical Connections to Spyware & Scammy Ads

Culper also uncovered that AppLovin's CEO, Adam Foroughi, previously was at Gator Corporation, which was "**Notorious as one of the first widespread spyware applications.**"

Adam Foroughi and AppLovin co-founder Andrew Karam also founded Social Hour, which was evidently banned by Facebook for showing "**scammy ads**" that "**trick Facebook users into clicking ads.**"

It appears that AppLovin has been employing management's same old tricks.

Code FPR Analyzed Appears to Confirm Direct Downloads

Fuzzy Panda Research purchased multiple T-mobile and Samsung phones and tested them. In our tech team's opinion, this "silent install" code appears to confirm the code that enables the direct downloads that Culper discovered.

Code Appears to Confirm Direct Downloads

AppTrackingEventInfo

```
1  package com.applovin.array.sdk.track;
2
3  import com.applovin.array.common.provider.C0871f;
4  import com.applovin.array.common.web.trigger.extension.AppMetricsExtension;
5  import java.util.ArrayList;
6  import java.util.HashMap;
7  import java.util.List;
8  import java.util.stream.Collectors;
9
10 /* loaded from: classes.dex */
11 public class AppTrackingEventInfo {
12     public static final String ACTIVATE = "activate";
13     public static final String CANCEL = "cancel";
14     public static final String CLICK = "click";
15     public static final String CLICK_OPEN_APP_NOTIFICATION = "click_open_app_notification";
16     public static final String CONTINUE_CLICK = "continue_button_click";
17     public static final String DOWNLOAD_FAILED = "download_failed";
18     public static final String DOWNLOAD_STARTED = "download_started";
19     public static final String IMPRESSION = "impression";
20     public static final String INSTALL_CLICK = "install_button_click";
21     public static final String INSTALL_FAILED = "install_failed";
22     public static final String INSTALL_STARTED = "install_started";
23     public static final String INSTALL_SUCCESS = "install_success";
24     public static final String SILENT_INSTALL_START_DOWNLOAD = "silent_install_start_download";
25     public static final String SILENT_PRELOAD_START_DOWNLOAD = "silent_preload_start_download";
26     public static final String THIRD_APP_FIRST_LAUNCH = "third_app_first_launch";
27     public static final String WIDGET_RECOMMENDATION_ICON_CLICKED = "widget_recommendation_icon_clicked";
28     long clientTimestamp = System.currentTimeMillis();
29     public String eventName;
30     List<AppTrackingEventExtraItem> extra;
```

Silent Install = Direct Download

Ad Fraud Researcher Ben Edelman Found References to Direct Downloads

> "**AppLovin's source code contains repeated references to 'direct download.'** That is a surprise: On Android, the standard way to install a new app is to send the user to Play Store where the user can press a button to download and install."
>
> "**The revelation of AppLovin installing games and apps without user consent is explosive.** Only very rarely has a company of their size ever been caught placing software on a user's device without the user agreeing. **This revelation would make AppLovin a pariah in many online advertising circles, for crossing a crucial line that's usually so easy to stay on the right side of.**"
>
> ~Ben Edelman

Fuzzy Panda Research Highly Respects Culper Research's Diligence & Track Record

We hold many short-sellers in high regard. We have often followed people for years, read their campaigns, and seen their long-term follow through.

Culper Research is an activist short-seller that when we read their work we say "Wow, how did they find that?" Culper has a very impressive track record as a result.

During the course of our own AppLovin research, we became aware via a mutual contact that Culper also had likely been doing extensive due diligence on the company. So rather than try to race and scoop Culper's story we decided to take a page from our history as a long-only investor. We decided to go with the route of being a "good human" and decided to choose trust over conspiracy. So we called Culper's founder on the phone and said, "Hello, I think we might both be working on the same company. What have you uncovered? We have found xyz so far." It felt like a risky move, especially in this short-seller world where we have seen countless friends backstab one another over the years or try to take credit for another's research.

It's a call we don't regret as we believe both Culper and us learned more about what is going on inside AppLovin's Black Box.

This goes back to the whole point of Fuzzy Panda sharing our independent research publicly (and in this case also with Culper Research). Great research makes everyone smarter.

Fuzzy Panda Research is an objectively terrible brand name (kind of like AppLovin'), but at least we admit our name is ridiculous. Our ridiculous brand name does one important thing: it strips our team's pedigree and egos from the work we publish. Our research has to stand for itself, and the only way you could possibly trust it is if you can replicate it.

We believe every researcher (long & short) sees or knows a different part of the puzzle that all investors are trying to figure out. So, a shout-out goes to other educated voices who have helped advance our own research: Congrats to Edwin Dorsey at BearCave for nailing the peak and especially Lauren Balik for furthering our own AppLovin diligence.

Our final thought is that when 2 long-only investors get together and share their ideas and diligence it's called a "lunch among friends." If 2 short-sellers get together and do the same thing, people accuse them of being a secret cabal. The reality is both scenarios are actually just 2 friends trusting the other with their own research.

Thanks for trusting us Culper.

Legal Note – Fuzzy Panda Research is responsible for their own research and own opinions. Culper Research is responsible for their own research and own opinions. Neither of us can vouch for the accuracy of the other's diligence or opinions.

PART VI – What We Think Is Coming Next – Short AppLovin

Violating Apple Or Google's Rules = Kicked Out of App Stores

- Apps w/ AppLovin SDK Could Be Removed from Apple or Google App Stores
  - For Sketchy Ad Practices
  - For Serving Sexual Ads to Children
  - For Tracking Children
  - For Violating Privacy of "Do Not Track" Users
- Apple Banned Adjust SDK briefly in 2021

> "Apple and Google have rules…I kept sort of expecting the … **shoe to drop and crush our heads**."
>
> ~ Former AppLovin Senior Engineer G

Shorting AppLovin does not require an investor to hope that the FTC or California AG will intervene and stop the sketchy ad practices or enforce children privacy rights.

AppLovin's business depends on access to Apple's App Store and Google's Play Store. The reality is that AppLovin survives and thrives at the whims of Google and Apple.

AppLovin's business practices have provided both Apple and Google ample reasons to remove AppLovin Apps from the iOS and Android App Stores. Not only that, but any other apps with an AppLovin SDK found to be violating privacy rules could also be removed.

AppLovin's business could be destroyed overnight.

Why Now? Tech Monopolies Can Flex Their Muscle Again

We think this hasn't happened yet and Apple and Google allowed AppLovin to thrive as a result of the anti-trust pressure that had been put on major tech companies by the Biden Administration. They couldn't be seen as sanctioning a major competitor of theirs for ad spend or in the mediation business previously. Former AdMob employees even told us Google had to always fight with one hand tied behind it back, but now with a lax anti-trust Republican government they can finally fight back.

> **"Google [AdMob] is always fighting with one hand tied behind its back** … They **[AppLovin] were Fingerprinting users,** you know, with IP address and IDFA back when it was readily available"
>
> ~Former Google AdMob Employee

AppLovin Appears to Have Violated Multiple of the Apple iOS Rules

- Using Apple's IDFV for Non-Analytics Purposes
- Fingerprinting Users

AppLovin Appears to Have Violated Multiple Android Store Policies:

- Device and Network Abuse for Causing the Reported Automatic Downloads
- Automatically Generating Clicks on Ads which Google Play describes as "Ad Fraud"
- Inappropriate Content – for Promoting Sexual Content via Depictions of Sex Acts to Minors

This has actually happened before, and the company that was sanctioned in that case was…Adjust (now owned by AppLovin).

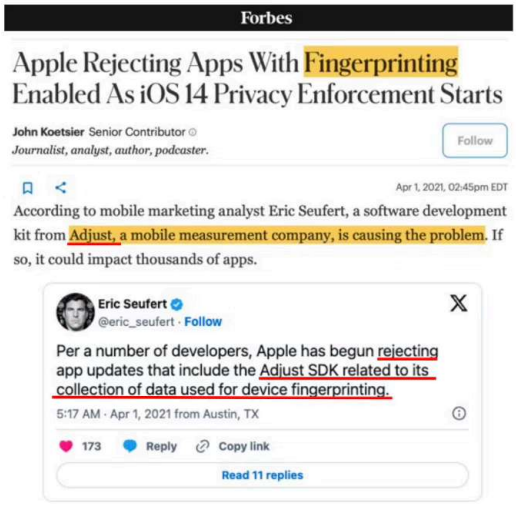
Apple Briefly Banned AppLovin's Adjust SDK in 2021 Over Fingerprinting

In 2021, AppLovin's Adjust mediation platform was briefly banned for "fingerprinting."

Apple started rejecting all apps with the Adjust SDK when Apple tightened its privacy protections, and the ban was only lifted after Adjust tweaked its SDK.

We think this could happen again.

Adjust SDK Banned for Fingerprinting



Forbes

Apple Rejecting Apps With Fingerprinting Enabled As iOS 14 Privacy Enforcement Starts

John Koetsier Senior Contributor
Journalist, analyst, author, podcaster.

Follow

Apr 1, 2021, 02:45pm EDT

According to mobile marketing analyst Eric Seufert, a software development kit from Adjust, a mobile measurement company, is causing the problem. If so, it could impact thousands of apps.

Eric Seufert
@eric_seufert · Follow

Per a number of developers, Apple has begun rejecting app updates that include the Adjust SDK related to its collection of data used for device fingerprinting.

5:17 AM · Apr 1, 2021 from Austin, TX

173 Reply Copy link

Read 11 replies

A Case Study = Tiny Labs Kicked Out of Google Play Store & Went Bankrupt

We found a case study of what happens if a gaming company is removed from the Google & Apple App Store for privacy violations alleged in a lawsuit by the State of New Mexico vs. Tiny Lab & AppLovin for collecting personal data from children and not obtaining proper parental consent.

WHEREAS, as a result of the conduct alleged in the Complaint, Google removed Tiny Lab from the Google Play Store, which substantially limited its ability to publish online games and to profit from them.

WHEREAS, upon investigation of undersigned counsel, Tiny Lab ceased as a going concern.

Source: State of New Mexico v. Tiny Lab Productions Case 1:18-cv-00854-MV-JFR – Stipulated Order of Dismissal

Government Regulator's Response?

- COPPA Violations Could Lead to Massive FTC Fines
- California Privacy Violations = More Potential Large Fines

Let's be realistic, the idea of the FTC enforcing any large fines against a company seems far-fetched in today's political environment. However, if there were one exception to this, it would be for systematically violating the privacy of children. We think that NOT tracking children and NOT showing children sexually inappropriate ads is an issue that even Republicans & Democrats can agree on.

We believe that inappropriate ads like the ones we were shown in our tests are "deceptive and harmful" and that the FTC should actively protect American boys and girls by looking into AppLovin.

US Law Bans Tracking Children – Fines For AppLovin Tracking Children Could be Massive

The Children's Online Privacy Protection Act (COPPA) from 1998 is not ambiguous: **Tech companies cannot collect data on or track children under the age of 13 without "verifiable parental consent."**

Violating the law, known as COPPA, has led to massive fines for app developers and platforms.

The FTC has levied huge fines for COPPA violations on Epic Games, Google/YouTube, TikTok and others.

AppLovin's COPPA violations could be widespread – tens of millions of children play apps that use their advertising platform.

Epic Games was fined >$500 million for COPPA Child Privacy Violations:

Google/YouTube was fined $170 million for COPPA Child Privacy Violations:

Below are possible child privacy violations that other media companies have been accused of that we believe could be precedent for charges brought against AppLovin.

AppLovin Potential FTC Violations

Possible Violation	Case Precedence	Defendant's Violation	Fine Paid
Sexual & Violent Ads to Children	FTC v Epic	Exposed children to dangerous and psychologically traumatizing issues, such as suicide	$520 million
Shifting Onus to Parents	FTC v Epic	Epic's weak privacy policy put the burden on parents to report violations	$520 million
Unknowingly Targeting Kids & No Parental Consent	FTC v YouTube	YouTube failed to obtain verifiable parental consent	$170 million
No "Actual Knowledge" of Child Data Collection	FTC v YouTube	YouTube claimed to be a general-audience network, allowing them not to request parental consent to track children	$170 million
Sharing Unique Tracking ID with 3rd parties – Not For Internal Purposes	FTC v TikTok	TikTok shared info they collected from children with 3rd parties for reasons other than internal operations	$5.7 million

FTC Previously Named Both AppLovin & MoPub For Receiving Personal Information on Kids in Lawsuit

Both AppLovin and MoPub were named by the FTC for receiving personal information on children in a 2019 lawsuit vs Google. The FTC complaint was regarding unfair and deceptive practices in marketing apps for children.

FTC Names AppLovin & MoPub For Receiving Kids Personal Info

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20584

In the Matter of	)
	)
Request to Investigate Google's Unfair and Deceptive Practices in Marketing Apps for Children	)
	)
	)

Examples of third parties receiving personal information from apps in the Family section

AppLovin describes its business as a comprehensive platform to help app developers grow and monetize games. Its privacy policy states that it may collect "device information across mobile apps and websites over time" and combine it with other information. It claims that it does not knowingly collect personal information from children under 13 except to provide support for internal operations or other exceptions in the COPPA Rule. https://applovin.com/privacy/	*Design It Girl –Fashion Salon*, by TabTale, (ages 6-12) *The Fixies Quest: Kids Riddles*, by DEVGAME KIDS, ((ages 6-8))
MoPub is owned by Twitter, and is a defendant in the New Mexico COPPA complaint. Its privacy policy states that if you use an app integrated with MoPub services, it will collect personal information about you, including device identifiers and precise geolocation. It uses this and other information to serve interest-based advertising. It says it does not permit MoPub services to be used to collect information from apps directed to children under 13 for personalized advertising. It does collect information from for serving contextual ad and other purposes. https://www.mopub.com/legal/privacy/	*Design It Girl –Fashion Salon*, by TabTale, (ages 6-12) *The Fixies Quest: Kids Riddles*, by DEVGAME KIDS, (ages 6-8)

California Privacy Violations Could Lead to Large Fines for AppLovin

The Mitchell v. AppLovin lawsuit alleges AppLovin violates California Invasion of Privacy Act, the California Computer Data Access and Fraud Act, and other California laws every time a person uses apps on its network.

Aside from the lawsuit, the violations could also lead to legal action by California authorities. AppLovin could face criminal penalties and massive fines. Each CIPA violation alone can result in a $5,000 fine, and AppLovin could face millions of violations.

PART VII – Is APP the Next APPS – Short AppLovin

Is APP The Next APPS?

- Will AppLovin (APP) Be the Next Digital Turbine (APPS)?

AppLovin and Digital Turbine don't just only share a similar ticker—we realized there are a remarkable number of similarities between AppLovin and Digital Turbine, the mobile ad darling of Wall Street from 2020-2021. Digital Turbine imploded and has fallen by >95% since.

Is AppLovin next?

	Digital Turbine (APPS)	AppLovin (APP)
Wall Street Darling at Peak Valuation	✓	✓
Stock Price Up >500% from IPO to Peak	✓	✓
Labeled a "Category Leader" in Mobile AdTech	✓	✓
Aggressive M&A-Driven Growth Strategy	✓	✓
Shift to End-to-End Software Model	✓	✓
Opaque Revenue Recognition	✓	✓
Divestiture of Underperforming Publisher Assets	✓	✓
TAM Expansion Bull Story (Internet TV, E-Commerce, etc)	✓	✓
Significant Executive Compensation & Insider Selling	✓	✓
Shady Ad Practices (deceptive redirects, forced installs, etc.)	✓	✓
Major Platform Dependencies (Google, OEMs, Meta, etc.)	✓	✓
Intense Decline in Revenue & Margins	✓	?
Regulatory & Legal Scrutiny (Google, Apple, Meta, etc.)	✓	?
Extreme Stock Price Decline	✓	?

Conclusion – Short AppLovin

> **"[App Lovin] have been fraudsters since they started in the industry** and they have learned and they have improved **and they have become the best fraudsters that are in this market"**
>
> ~ Former AppLovin Anti-Fraud Executive B

To short AppLovin you don't have to believe that CMOs or the even the FTC will intervene to stop what former employees describe is "Ad Fraud."

All you need to believe is that any of the 3 major tech powerhouses will intervene to protect their own users and reputations.

AppLovin has pushed the envelope too far and pulled too many shady ad tricks. We believe Apple and Google will remove games and SDKs that are:

- Violating COPPA Laws by:
  - Assigning Unique Identification Numbers to Children
  - Pulling Identifying Device & Tracking Attributes from Kids' Devices
  - Serving Sexually Explicit Ads to Kids
- Violating Privacy Restrictions by allegedly Fingerprinting "Do Not Track" Users
- Consistently Engaging in "Manipulative End Card Practices"

We think Google has no choice but to take action against the AppLovin SDKs that appear to be exploiting a "Direct Download" weakness in order to boost their own revenue by automatically install apps without user consent. The "Direct Download" program that Former AppLovin employees claim has been "the top revenue driver" is set up to be eliminated.

META will destroy the E-commerce bull thesis.

Experts have told us APP has gotten away with "copying" Meta's homework. This has lasted for a little over 6 months. Meta formers & current employees told us that Meta won't put up with it, so investors should expect them to fight back.

We are short AppLovin because we think Apple, Google, Meta are going to fight back. They are going to punch AppLovin right in their ROAS!

Fuzzy Panda Research is Short AppLovin (APP)

McLovin' Note – We discovered in our research that AppLovin actually is named after McLovin. (See this old interview with the AppLovin CEO where he admits it.)

So why does the company feel the need to lie about a small & silly fact? Especially when it turns out AppLovin had so much else to hide in their black box.

Appendix A – Reality of Games Studio Sale – A Non-Binding, Seller Financed, Partial Sale

- Sale is Non-Binding
- Sale is Only of 5/9 of Business
- APP Providing 50% of the Cash

AppLovin has been trying to divest their games studio business since 2022. On the Q4-24 earnings call, AppLovin announced that they finally had a deal to sell the stagnant/declining business whose revenue has declined 16% over the last 2 years. Management said they would sell the business for $900 million which immediately increased APP's market cap by another ~$20 billion!

But the reality of this deal is buried in the details:

- AppLovin will still own 44% of the business
- Acquirer can borrow ½ the cash from…AppLovin!
- Term sheet is non-binding
- Unknown Buyer but subject to regulatory approval – Is it a Chinese buyer again?

The reality is that AppLovin has a non-binding term sheet to sell only 55.6% of the Apps business…AND AppLovin has offered to provide the financing for half of that 55%.

Sale of Gaming Studios = Taking a Big Loss?

AppLovin began restructuring their Apps business in 2022 and have repeatedly indicated interest in selling their gaming studios, but over two years, they were unable to find a buyer.

AppLovin hasn't disclosed details of each gaming studio purchase they've made nor have they disclosed the cost of developing Lion Studios from scratch. However, we have acquisition data on 4/10 they currently own, and we can see AppLovin paid ~$773 million for them. It's unclear what APP paid or spent to develop the remaining studios, but selling 55% of them for $900 million sounds like it could represent a large loss for AppLovin.

Studio	Cost ($ Million)	Important Games
Lion Studios	developed	
PeopleFun	100.7	1
Magic Tavern	undisclosed	2
Belka Games	undisclosed	
Clipwire	undisclosed	
Machine Zone	328.6	
Zenlife Games	173.3	
Athena Studio	170.7	
Leyi	undisclosed	
Zeroo Gravity	undisclosed	
Total	**773.3**	

Chinese Buyer Again?

While discussing the Q2 2025 target closing of the sale, APP's CFO mentioned the transaction "may be subject to regulatory approval, so that timing may change slightly." Back in 2016, APP was supposed to be acquired by Orient Hontai Capital – a Chinese PE firm – for $1.4 billion. The deal was blocked by the US government's CFIUS (Committee on Foreign Investment in the US).

Is it a Chinese buyer again?

If it isn't then would a non-Chinese buyer still be interested when they know APP's gaming studios have likely been key in collecting children's data? And likely were serving children sexual graphic ads?

Appendix B = Copying Meta's Homework – A Take-Home Test for PMs

A 12-Step program to see AppLovin mimic Meta IRL

1. Use a clean device (new or reset mobile device).
2. Install a VPN that will change your IP Address and block requests sent to AppLovin (and Adjust). Do this BEFORE searching on a Meta app or installing an AppLovin app.
    1. The reason why is that e-commerce companies often put an AppLovin Pixel on their websites which allows easy retargeting. So, unless you block the pixel sending the data back to AppLovin, you will get a false positive based on retargeting.
3. Go to Facebook or Instagram.
4. Search for a product like "Ridge wallets" — a Meta and AppLovin e-commerce customer. Navigate to the Ridge store and add items to cart but don't purchase.
5. Behind the scenes, Meta will see this and bid to show you a Ridge ad on AppLovin's auction platform. AppLovin will see the bid and essentially copy Meta's targeting.
6. Download an AppLovin mobile game, like Happy Glass.

7. Disable the VPN.
8. Hit "allow" when it asks if you want to be tracked across apps.
9. Begin playing!
10. If AppLovin hits you with Ridge wallet ad, guess what? You just caught AppLovin copying Meta's homework.
11. The ads will continue to follow you across other AppLovin games if AppLovin has "fingerprinted" your device.
12. Now, as you wait for your beautiful new wallet to arrive, sit back and ponder, "How did AppLovin know something you only told Meta?"

Appendix C – Download the Apps to do Basic AppLovin Research

It's easy. You don't need to intercept the data transmitted or decode a black box SDK to figure out what is going on.

Here are the basic steps a PM or analyst needs to do diligence on AppLovin.

- Own a mobile phone
- Download an AppLovin game
- Play mobile game 10-15 minutes
- Get mad at Ads
  - Ads that don't close;
  - Ads that auto open the App Store;
  - Ads that appear to click themselves.

We believe the ven diagram of free mobile gamers and hedge fund managers = ZERO People. Those two groups have likely never met one another. So go spend 10-15 min on an AppLovin game and experience what we think is a key part of AppLovin's secret sauce – fake clicks and accidental downloads.

PM's that still own APP after this miraculous run in the stock must have their head stuck in the Sensor Tower data and are blind to what is really going on.

Appendix D – Disappearing Subsidiaries Signal Something Sketchy? Or Old Fashioned Un-American Tax Avoidance?

- 58 Subsidiaries Have Vanished Since 2021

The number of subsidiaries listed in AppLovin's financials dropped from 67 in 2021, the year it went public, to just 9 in 2023. Yet we found that most of the 58 disappeared companies remain active and owned by AppLovin, including subsidiaries in Cyprus and the Cayman Islands.

AppLovin has told investors that it reorganized its subsidiaries and restructured them into Singapore to lower its tax burden. They also warned in its most recent financials that the structure could be challenged by U.S. or "foreign tax authorities." And hey, maybe that is the real reason since AppLovin is only paid a ridiculously low 2% LTM tax rate.

But to us, disappearing subsidiaries is a huge red flag. Unfortunately, we have done a deep dive and still have not yet found satisfactory answers. Thus, we will shortly be posting all of the relevant missing subsidiary documents so hopefully another enterprising investor can figure out the mystery of "AppLovin's Disappearing Subsidiaries."

On February 25, 2025, Sakura Research seems to have begun solving part of the mystery discovering 3 undisclosed subsidiaries in China and Singapore.

Sakura Research discovered three missing subsidiaries: Apravi (Beijing) Technology Development Co, AppLovin (Singapore) Technologies I Pte Ltd, and AppLovin (Singapore) Technologies II Pte Ltd.

AppLovin's Disappearing Subsidiaries

Fiscal Year 2021: 67 Subsidiaries	Country
AppLovin Corporation	USA
7 Minute Games Corporation	USA
Acquired IO LLC	USA
Adeven Israel Ltd	Israel
Adjust Brasil Licenciamento do Software Ltda	Brazil
Adjust France SARL	France
Adjust GmbH	Germany
Adjust Gmbh Co. Ltd.	China
Adjust Inc	USA
Adjust Software India LLP	India
Adjust International Holding GmbH	Germany
Adjust K.K.	Japan
Adjust Korea Ltd	Korea
Adjust Singapore Pte Ltd	Singapore
Adjust Software Limited	England
AL HK Ltd (AppLovin Hong Kong)	Hong Kong
AL Rewards, LLC (aka OpenVessel Technologies)	USA
AppLovin Business Consulting	China
AppLovin Active Holdings, LLC	USA
AppLovin Canada Corporation	Canada
AppLovin Cayman Limited	Cayman Islands
AppLovin Corporate Limited	Cayman Islands
AppLovin Cypress Limited	Cyprus
AppLovin Games, LLC	USA
AppLovin GmbH	Germany
AppLovin KK	Japan
AppLovin Limited	Ireland
AppLovin Studios, LLC	USA
Arena of Stars LLC	USA
Belka Games, LLC	USA
Better Life Productions, LLC	USA
Bubblegum Games, LLC	USA
Clipwire Games Inc	Canada
Cognant LLC	USA
DD Games, LLC	USA
Epic Action LLC	USA
Epic War LLC	USA
Firecraft Studios Limited Corp	Cayman Islands
Fractional Media, Inc	USA
Geewa a.s.	Czech Republic
HippoTap, LLC	USA
Lion Studios, LLC	USA
Machine Zone KK	Japan
Machine Zone Germany GmbH	Germany
Machine Zone, Inc.	USA
Magic Tavern, Inc.	USA
MagicAnt, Inc	Japan
MagicAnt, LLC	Japan
Mobile War LLC	USA
Morocco, Inc	USA
MZ IP Holdings LLC	USA
PeopleFun CG, LLC	USA
PeopleFun, Inc.	USA
Poetic Cloud, LLC	USA
Redemption Games, Inc	USA
SafeDK Mobile Ltd	Israel
Samfinaco Limited	Cyprus
Satori Worldwide, LLC	USA
Spinx Studios LLC	USA
Supreme City Games LLC	USA
Tetris IP Holdings, LLC	USA
Thrive Games, LLC	USA
Unbotify Ltd	Israel
Word and Sudoku Games LLC	USA
ZenLife Games Limited	Cyprus
Zenlife Games Pte. Ltd	Singapore
Zerpo Gravity Games LLC	USA

Fiscal Year 2022: 12 Subsidiaries	Country
Adjust GmbH	Germany
AppLovin Active Holdings	USA
AppLovin Cyprus Limited	Cyprus
Clipwire Games Inc	Canada
Lion Studios, LLC	USA
Machine Zone, Inc	USA
Magic Tavern, Inc	USA
Morocco, Inc	USA
PeopleFun, Inc	USA
WURL, LLC	USA
ZenLife Games Limited	Cyprus
ZenLife Games Pte Ltd	Singapore

Fiscal Year 2023: 9 Subsidiaries	Country
Adjust GmbH	Germany
AppLovin Active Holdings	USA
AppLovin (Singapore) Pte Ltd	Singapore
Lion Studios, LLC	USA
Machine Zone, Inc	USA
Magic Tavern, Inc	USA
Morocco, Inc	USA
PeopleFun, Inc	USA
Zerpo Gravity Games LLC	USA

[List of Documents for AppLovin's "Disappearing" Subsidiaries]

Happy Hunting!

We'd suggest starting with Cyprus and the Cayman Islands, or maybe the solution lies in Singapore.

AppLovin has a Big Future Tax Bill Coming Due

AppLovin has historically paid very low taxes with a TTM effective tax rate of ~2%.

Regardless of the Singapore restructure, AppLovin will likely see its taxes jump at the end of FY 2025 because their net income is on pace to surpass a three-year average of $1 billion. That will trigger the 15% Corporate Alternative MinimumTax rule.

A good problem to have, for sure, but long investors should consider that AppLovin's tax rate is basically going to go from 2% to 15%.

Appendix E – Insiders Selling Way More Stock Than The Company Buys Back

Insiders and Chinese investors have cashed out of an est >$8.6 billion in stock while AppLovin has spent ~$2.17 billion repurchasing shares since 2023.

Not a Single Insider Has Purchased Shares in 3 Years.

Notably:

- Vasily Shikin (CTO), who is "The Man Inside the BlackBox," has reduced his shares by ~60%.
- Adam Foroughi CEO has even sold >$37 million. And that's just in the past week.
- In Q4 2024 stock buy backs were a mere $625,000, so management must clearly agree that the stock is overvalued.

Insiders & Key Investors Have Sold 4x More Than APP Has Repurchased

2023 - Present			
Insider	**Position**	**Est Sale Amount**	**% Change in Shares Held***
KKR	Private Equity Investor	$ (5,778,332,014)	-100%
Vasily Shikin	CTO	$ (357,449,621)	-60%
Adam Foroughi	CEO	$ (134,056,741)	-64%
Herald Chen	Former CFO	$ (239,993,891)	-27%
Eduardo Vivas	Director	$ (138,438,841)	-30%
Victoria Valenzuela	CLO	$ (44,191,737)	-62%
Matthew Stumpf	CFO	$ (12,022,100)	-29%
Katie Jansen	CMO	$ (66,125,414)	-47%

Significant Shareholders	**Investor Name**	**Est Sale Amount****	**% Change in Shares Held**
Midterm Success Limited	Hao Tang	$ (911,805,095)	-57%
Angel Pride Holdings	Tang Ling	$ (955,027,514)	-32%

Total Insiders	$ (6,770,610,360)
Total Insiders + Key Chinese Investors	$ (8,637,442,969)
Total Repurchases	$ 2,166,233,210

*calculated using share count as of 12/31/2022 or as of 3/13/2023. Mr. Shikin & Mr. Foroughi received RSU/PRSUs that day

**We used an est sales price of $50/share & $219/share for Angel Pride Holdings's decrease in share count as of 12/31/2023 13G & 12/31/2024 13G, respetively

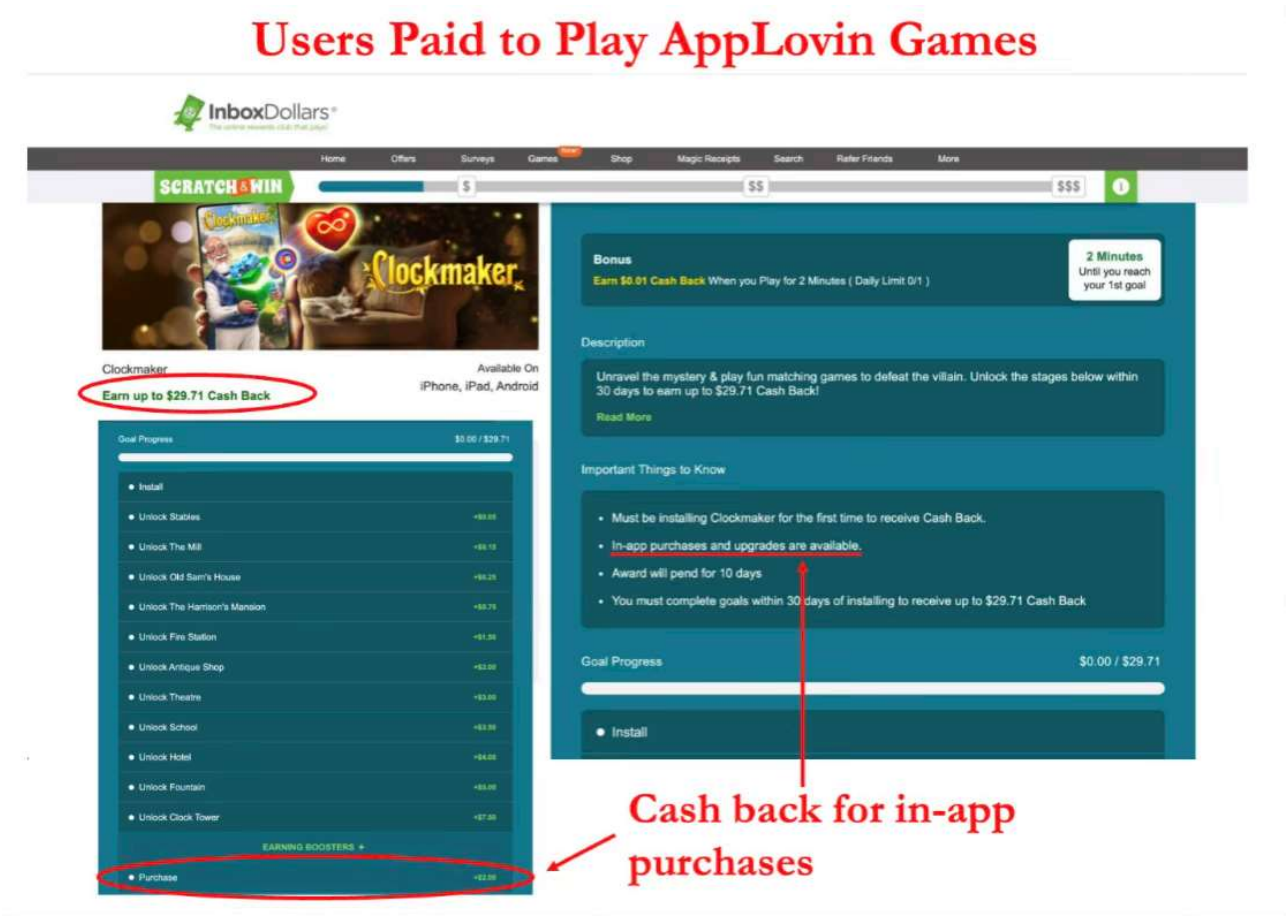
**We used an est sales price of $15/share & $85/share for Midterm Success Limited's decrease in share count as of 4/23/2024 Proxy & 12/31/2024 13G, respectively

Appendix F – Swagbucks Appears to Be a Pay-to-Play Roundtrip of Revenue

Recent reporting by Lauren Balik, a finance blogger, has detailed how AppLovin partners with third-party companies that "pay" users via PayPal and gift cards to play its games, incentivizing them to make in-app purchases.

One of those companies, Prodege, which AppLovin describes as a "performance-based user acquisition partner," owns and operates swagbucks.com and inboxdollars.com. We found multiple offers on the two sites advertising cash rewards for playing AppLovin mobile games, including a current promotion on inboxdollars.com to get "cash back" for playing Clockmaker.

AppLovin appears to be engaged in a method that we believe is round-tripping of revenue. Money is cycled from users to the company and then back to the users and it in essence artificially inflates revenue. You can read Lauren's work on AppLovin here, here, here and here.



Appendix G – AppLovin's Child Privacy Policies Appear Insufficient

We believe that AppLovin's children's privacy policies appear to be insufficient. They attempt to shift the onus of responsibility to other app developers and even onto parents. Saying things like "If you are under 13, do not use or provide any information on this Website…or features" is not sufficient.

Adjust's Child Privacy Policy

MAX's Child Privacy Policy

Meantime, AppLovin removed COPPA support from their SDK in September 2024 to try to push the responsibility to others for not collecting kids' data.

But the legal precedent is clear: Ignoring a problem doesn't absolve a company of responsibility.

If you solve the mystery then please email us at fuzzypandaresearch@protonmail.com

Fuzzy Panda Research Disclosures, Disclaimer and Terms of Service:

By downloading from or viewing material on this website and/or by reading this report, you agree to the following Terms of Service. You agree that any use of the research in this report or on this website is at your own risk. In no event will you hold Fuzzy Panda or any affiliated party, including officers, directors, employees, consultants, and agents of Fuzzy Panda or any companies affiliated with any of them, liable for any direct or indirect losses caused by your use of or reliance on information on this site or in this report. You further agree that you will not rely on any information in this report or on this website, to do your own research and due diligence before making any investment decision with respect to companies or securities mentioned herein, and that you will consult with your own investment professionals prior to any investment decisions. You represent that you have sufficient investment sophistication to critically assess the information, analysis and opinions in this report or on this site. You further agree that you will not communicate the contents this report or other materials on this site to any other person unless that person has agreed to be bound by these same Terms of Service. If you accessed, download, or receive this report or the contents of other materials on this site as an agent for any other person, you are binding your principal to these same Terms of Service.

As of the publication date of this report, Fuzzy Panda, and possibly any companies affiliated with it or its members, partners, employees, consultants, clients and/or investors (the "Fuzzy Panda Affiliates"), have a short position in the stock (and/or options, swaps, and other derivatives related to the stock) and bonds of the company covered in this report (the "Covered Company"). Fuzzy Panda and the Fuzzy Panda Affiliates therefore stand to realize significant gains in the event that the prices of either equity or debt securities of the Covered Company declines. There are many factors that can go into a decision to cover the short position(s) in the Covered Company's securities and it is not possible to predict exactly when or for exactly what reasons Fuzzy Panda and the Fuzzy Panda Affiliates may cover their positions, in whole or part, or otherwise change their investment holdings. As a general matter, Fuzzy Panda and the Fuzzy Panda Affiliates intend to cover some or all of their positions at a time that the price of the Covered Company's securities are lower than when they were sold short or otherwise invested in. Fuzzy Panda and the Fuzzy Panda Affiliates may cover some or all of their short positions immediately after the publication of this report or an indefinite period after its publication. Similarly, Fuzzy Panda and the Fuzzy Panda Affiliates may cover some or all of their short positions if the price of the Covered Company's securities move a small amount or after moving a larger amount. Fuzzy Panda and the Fuzzy Panda Affiliates intend to continue transactions in the Covered Company's securities for an indefinite period after the publication of this report, and they may be short, neutral, or long at any time after the publication of this report regardless of any opinions, possible stock prices or valuations, or other views stated in the report. Fuzzy Panda will not update any report or information on this website to reflect any changes in the investments of Fuzzy Panda or the Fuzzy Panda Affiliates that existed at the time of the publication of this report, or any new positions in any securities of the Covered Company.

During the course of performing research Fuzzy Panda endeavors to speak with as many information sources as it can in an effort to produce better and more accurate reports. Fuzzy Panda occasionally speaks with other short sellers who are performing their own independent research on companies Fuzzy Panda is researching. In the course of researching APP, Fuzzy Panda and Culper Research shared some of the information they discovered in their respective independent research. Fuzzy Panda believes that Culper Research likely has a short position in APP and therefore Culper Research could also stand to benefit financially if the price of APP's securities declines.

This report and the Fuzzy Panda website is informational and describes the opinions of Fuzzy Panda. This report is not an offer to sell or a solicitation of an offer to buy any security, and Fuzzy Panda does not offer, sell or buy any security to or from any person through this report or the Fuzzy Panda website. This report is not a recommendation or advice to short or otherwise invest in or trade any security. Fuzzy Panda does not render investment advice to anyone unless it has an investment adviser-client relationship with that person evidenced by a formal written agreement. You understand and agree that Fuzzy Panda does not have any investment advisory relationship with you, or owe any fiduciary or other duties to you. Giving investment advice requires knowledge of your financial situation, investment objectives, and risk tolerance, and Fuzzy Panda has no such knowledge or information about you.

If you are in the United Kingdom, you confirm that you are accessing research and materials as or on behalf of: (a) an investment professional falling within Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); or (b) high net worth entity falling within Article 49 of the FPO.

Fuzzy Panda's research and reports express the opinions of Fuzzy Panda, which are based upon generally available information, field and online research, and inferences and deductions through due diligence and the analytical process. Fuzzy Panda believes that all information contained in this report has been obtained from accurate and reliable public sources, and no material nonpublic information was obtained from any person who had a duty to keep information confidential. However, Fuzzy Panda cannot be certain that the information it has relied upon in this report is accurate. The information and opinions in this report are therefore presented "as is," without warranty of any kind, whether express or implied. Fuzzy Panda 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. This report also contains forward looking statements about what may occur in the future. The future cannot be predicted with certainty and any of the forward-looking statements about projections, beliefs, estimates, assumptions, outcomes, or any other future event may be incorrect. Among other things, any forward-looking statements may be rendered inaccurate by incorrect assumptions, incorrect methodologies, unforeseen risks and events, or other variables. Any opinions about the possible future stock price of the Covered Company or fair value of its securities is not a price target and does not mean or imply that Fuzzy Panda or the Fuzzy Panda Associates will hold any investment until such price or valuation is met. Further, all expressions of opinion, including any conclusions drawn from Fuzzy Panda's analysis, are subject to change without notice, and Fuzzy Panda does not undertake to, and will not, update or supplement any reports or any of the information, analysis and opinion contained in them.

You agree that the expressions of information in this report are copyrighted and owned by Fuzzy Panda Research, and you therefore agree not to distribute this report, any excerpts from it, or information from the Fuzzy Panda website (whether the downloaded file, copies / images / reproductions, or the link to these files) in any manner other than by providing the following link: www.fuzzypandaresearch.com. If you have obtained Fuzzy Panda's research in any manner other than by accessing or downloading from that link, you may not read such research without going to that link and agreeing to the Terms of Service. You further agree that any dispute between you and Fuzzy Panda and/or any of the Fuzzy Panda Affiliates arising from or related to the material on their website shall be governed by the laws of the State of California, without regard to any conflict of law provisions. You knowingly and independently agree to submit to the personal and exclusive jurisdiction of the state and federal courts located in California and waive your right to any other jurisdiction or applicable law. The failure of Fuzzy Panda to exercise or enforce any right or provision of these Terms of Service shall not constitute a waiver of such 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 this report or the material on this website must be filed within one (1) year after such claim or cause of action arose or be forever barred.