MUDDY WATERS RESEARCH

AppLovin: Deep Data Analysis Shows APP is Just Another Scammy AdTech Company

Approximately 52% of e-commerce Sales is Retargeting, with Incrementality of Only ~25%-35%. We Estimate Q1 2025 Churn is ~23%. APP's Code Evidences its Business is Built on Systematically Violating Third Party Platforms' TOS.

March 27, 2025

As of the time and date of this report, Muddy Waters (defined below) is short the securities of, or derivatives linked to Approving Corporation (the "Covered Issuer"). Upon publication, we intend to begin covering a substantial majority – possibly all – of our short positions. As we elaborate below, our risk reduction is not a reflection of a lack of conviction in our opinions or the facts presented; rather, it has to do with managing risk in a manner that is prudent for a fiduciary of our investors' money.

This report has been published by Muddy Waters, LLC ("Muddy Waters Research" or "we" or "us"). Muddy Waters Research is under common control and affiliated with Muddy Waters Capital LLC ("Muddy Waters Capital"). Muddy Waters Research is an online research publication that produces due diligence-based reports on publicly traded securities, and Muddy Waters Capital LLC is an investment adviser registered with the U.S. Securities and Exchange Commission. This presentation is the property of Muddy Waters Research. Muddy Waters Research and Muddy Waters Capital, collectively their respective affiliates and related parties, including, but not limited to any principals, officers, directors, employees, members, clients, investors, consultants and agents, are referred herein to as "Muddy Waters".

Muddy Waters will continue transacting in the securities of Covered Issuer for an indefinite period after this report on the Covered Issuer, and we may be net short, net long or flat positions in the Covered Issuer's securities after the initial publication of this report, regardless of our initial position and views herein.

We are a "for profit" journalistic organization with a non-traditional revenue model – rather than accepting advertising money or subscriptions, we finance our journalism through taking positions in the securities of companies on which we report. This revenue model enables us to report in great depth on a limited number of investigations, and also entails our taking significant financial risk on behalf of ourselves and our clients. In order to manage risk, we must close open positions as we deem prudent. We do not provide "price targets", although we may express our opinion of what the security is worth. An opinion of the value of a security differs from a price target in that we do not purport to have any insight as to how the market as a whole might value a security – we can only speak for how we, ourselves, view its value. We therefore do not hold a position until it reaches a certain price target, nor do we hold positions until they reach the price at which we have expressed a valuation opinion. There are numerous factors that enter into investment decisions aside from opinions of the value of the security, including without limitation, the borrow cost of a shorted security, the potential for a "short squeeze", prudent risk sizing relative to capital and volatility, reduced information asymmetry, the opportunity cost of capital, client expectations, the ability to hedge market risk, our perception of the efficacy of market regulators and gatekeepers, our perception of the resource imbalance between us and Covered Issuers, and our moods and gut feelings. Therefore, you should assume that upon publication of this report, we will, or have begun to, close a substantial portion – possibly the entirety – of our positions in the Covered Issuer's securities.

We are not providing you with a recommendation to buy or sell securities of the Covered Issuer. We are articulating our reasons at the time of publication we have positions in the securities of the Covered Issuer.

We have no duty or obligation to update this report or update you on the size or direction of any position we hold in a Covered Issuer. We do not provide investment advice to any person, unless our affiliate has entered into an investment adviser-client relationship with that person in writing.

All information and opinions set forth herein are for informational purposes only. Under no circumstances should any information or opinions herein be construed as investment advice, as an offer to sell, or the solicitation of an offer to buy any securities or other financial instruments.

This report is opinion journalism. We are providing our journalistic opinions about issues of concern to the general public. The opinions, information, and reports set forth herein are solely attributable to Muddy Waters Research. Before making any investment decision, you should do your own research and due diligence before making any investment decision with respect to securities of or derivatives linked to the Covered Issuer.

This report represents the views of Muddy Waters Research only and is based on publicly available information. To the best of our knowledge, all information contained herein is accurate and reliable and has been obtained from publicly available sources that we believe to be accurate and reliable. The information presented herein is "as is," without warranty of any kind, whether express or implied. This report contains a large measure of analysis and opinion. All expressions of opinion are subject to change without notice.

By viewing and accessing this report, you further agree to the following terms of use:

Muddy Waters shall not be liable for any claims, losses, costs, or damages of any kind, including direct, indirect, punitive, exemplary, incidental, special or consequential damages, arising out of or in any way connected with this report. This limitation of liability applies regardless of any negligence or gross negligence of Muddy Waters. You accept all risks in relying on the information and opinions in this report.

You agree that any dispute between you and Muddy Waters arising from or related to this presentation shall be governed by the laws of the State of Texas, 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 Austin, Texas and waive your right to any other jurisdiction or applicable law, given that Muddy Waters are based in Austin, Texas.

The failure of Muddy Waters to exercise or enforce any right or provision herein shall not constitute a waiver of such right or provision. If any provision of these terms of use 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 other provisions set forth herein, in particular as to this governing law and jurisdiction provision.

You agree and understand that, by the time you read this report, we may be covering or have already covered (i.e., bought back) our short position, and we are unlikely to increase our short positions unless it is in our financial interest to do so. You should not make any investment decision based your interpreted view of our positioning in the Covered Issuer's securities.

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 presentation must be filed within one (1) year after the occurrence of the alleged harm that gave rise to such claim or cause of action, or such claim or cause of action be forever barred.

APP e-Commerce is Mostly Retargeting, Incrementality is Low, and it Clearly Violates Platforms' TOS

Muddy Waters is short APP. Web traffic analysis leads us to estimate that ~52% of APPs e-commerce conversions are retargeting and incrementality is only ~25%-35%. Code evidences that APP is collecting and structuring user IDs from its key platform partners, which appears to be a major violation of the platforms' terms of service (TOS). APP therefore, in our opinion, could be deplatformed, similar to Cheetah Mobile. If APP is not deplatformed, logically, numerous competitors will start copying APP's techniques because there is little technology involved. APP's advertising clients are likely sensitive to actual incrementality, which should frustrate APP's growth plans. We have already observed e-commerce client churn of ~23% in Q1.

To identify high value users, it appears that APP is impermissibly extracting proprietary IDs from Meta, Snap, Tiktok, Reddit, Google, and others. APP then combines that misappropriated data to create artificial and persistent user IDs (aka user graphs). This is an iteration of old-school fingerprinting schemes to target ads without user consent.[1] The user graph is augmented by Shopify events (e.g. items added to shoppers' carts, checkout initiation), which provides APP with a black edge in the ad auctions. The last critical step in this scheme involves the aggressive use of these Persistent Identity Graphs ("PIGs") to repeatedly target and retarget high value users, serving them with ads won at these auctions. In this way, APP claims the revenue from highly valuable last-click attributions. This subterfuge occurs outside of the platforms' servers, making it difficult to detect.

- Web traffic for **37 million unique users across five advertisers in Q1 2025** indicates that ~52% of e-commerce sales are retargeting. This data informs our estimate that only ~25% to ~35% of APP's sales are incremental. This is far below the CEO's claim that e-commerce customers were "experiencing nearly 100% incrementality."[1]
- APP's e-commerce beta advertisers appear to be churning. Our analysis of 776 advertisers active in early Q1 2025 indicates that the churn rate is ~23%. APP's CEO reportedly claims there has been almost no churn.[2]
- Data sent to APP servers by APP's pixels (JavaScript) installed on advertisers' websites contains proprietary user data belonging to third party (3P) platforms.
- APPs creation and use of PIGs appears to be a gross violation of 3P platforms TOS, which puts APP at risk of being deplatformed.

[1] APP CEO Adam Foroughi, Q3 2024 earnings call

[2] Recently reported by the CEO Adam Foroughi to a sell-side analyst.

APP is Unique for its Audacity—Not for its Technology

How is APP, a company that requires neither user email addresses or phone numbers to play its games, nor requires personal data sharing opt-in, able to target ads so precisely as to match – or beat – Meta and Google at their own game? There is a perception that APP's targeting outperforms Facebook's Return On Ad Spend (ROAS).[1]

Google and Meta use their troves of first party (1P) data from consenting users, including emails, phone numbers, and browsing history to dominate digital advertising. They match their 1P data to individual users with clear consumer intent and leverage armies of engineers to predict what someone will purchase next with a high degree of accuracy.

Starting in 2021, Apple implemented iOS14.5 privacy measures like App Tracking Transparency (ATT). Google followed with its own version, depriving other ad networks of the data needed to compete. Every ad network had to adjust to the loss of data access, and Google[2] and Meta's[3] market share expanded to capture half of the global digital ad market.[4]

In short, iOS14 (2021) prohibited fingerprinting, etc. on (or by) any Apple devices. Apple's policies remain in place today. This is significant because iOS maintains its dominant position with ~58% US market share.[5]

When APP moved into e-commerce, we believe it repurposed existing tools (specifically, Compass analytics and the App Graph) because it did not have a robust supply of fresh1P data. APP's primarily innovation appears to have been adapting these tools to avoid detection by the 3P platforms.

[1] https://www.northbeam.io/post/applovin-performance-unveiled-insights-from-northbeam-users

[2] Google processes 5.9 million searches per minute showing user intent. Its shopping graph includes >45 billion product listings. https://www.digitalinformationworld.com/2025/03/google-processes-158548-searches-every.html, https://www.hillwebcreations.com/google-shopping-results/

[3] A 2024 Consumer Reports study found Meta has approximately 2,230 data points on how each of its 3.35 billion users interact with other companies and services. https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/

[4] Google 38.1% (https://www.precedenceresearch.com/digital-ad-spending-market), Social media ads, dominated by Meta account for 40% (https://cropink.com/advertising-statistics)

[5] https://gs.statcounter.com/os-market-share/mobile/united-states-of-america

Table of Contents

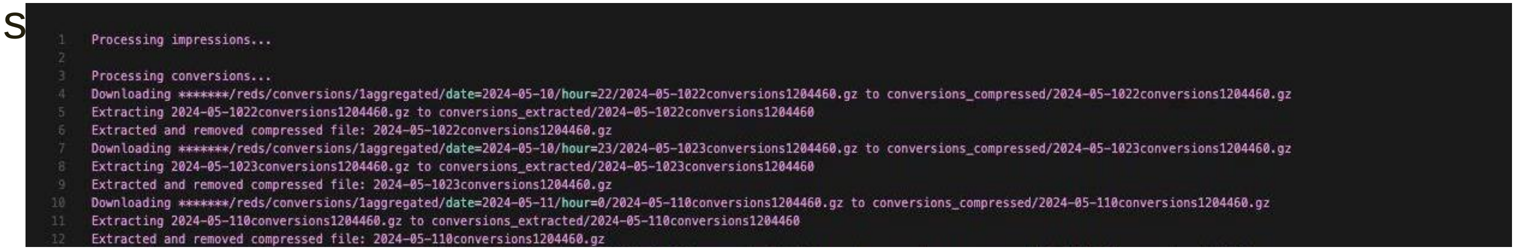
~52% of E-commerce Sales Are Retargeting, Only ~25-35% Incremental (Not ~100%)

E-Commerce Sales Are ~52% Retargeting

Approximately 52% of e-commerce sale appear to be retargeting based on analysis of conversion log-level files provided by a leading independent demand-side platform that covers over 37 million unique users from across five different advertisers' Shopify stores.

These 37 million unique users represent over $300 million in revenue over the apparel, beauty, healthcare, hobby and more verticals. Over seven weeks from YE 2024 into Q1 2025, approximately two-thirds to three-quarters of the ads were likely not attributable to APP's efforts. APP appears to have instead actively retargeted and / or jumped the last click attribution claim.[1]

- Only ~3.4% of users had any clicks from APP ads as indicated by URL level tracking by these advertisers
- For ~52% of the users who has a purchase event on the last click attribution, APP was not the first click to the webs



```
Processing impressions...

Processing conversions...
Downloading *******/reds/conversions/1aggregated/date=2024-05-10/hour=22/2024-05-1022conversions1204460.gz to conversions_compressed/2024-05-1022conversions1204460.gz
Extracting 2024-05-1022conversions1204460.gz to conversions_extracted/2024-05-1022conversions1204460
Extracted and removed compressed file: 2024-05-1022conversions1204460.gz
Downloading *******/reds/conversions/1aggregated/date=2024-05-10/hour=23/2024-05-1023conversions1204460.gz to conversions_compressed/2024-05-1023conversions1204460.gz
Extracting 2024-05-1023conversions1204460.gz to conversions_extracted/2024-05-1023conversions1204460
Extracted and removed compressed file: 2024-05-1023conversions1204460.gz
Downloading *******/reds/conversions/1aggregated/date=2024-05-11/hour=0/2024-05-110conversions1204460.gz to conversions_compressed/2024-05-110conversions1204460.gz
Extracting 2024-05-110conversions1204460.gz to conversions_extracted/2024-05-110conversions1204460
Extracted and removed compressed file: 2024-05-110conversions1204460.gz
```

[1] Study data provided by a Marking Tech company with APP customers. Weeks 12/30/24 to 2/16/25. This study achieved a statistical significance of 98% confidence interval with a ±2% margin of error.

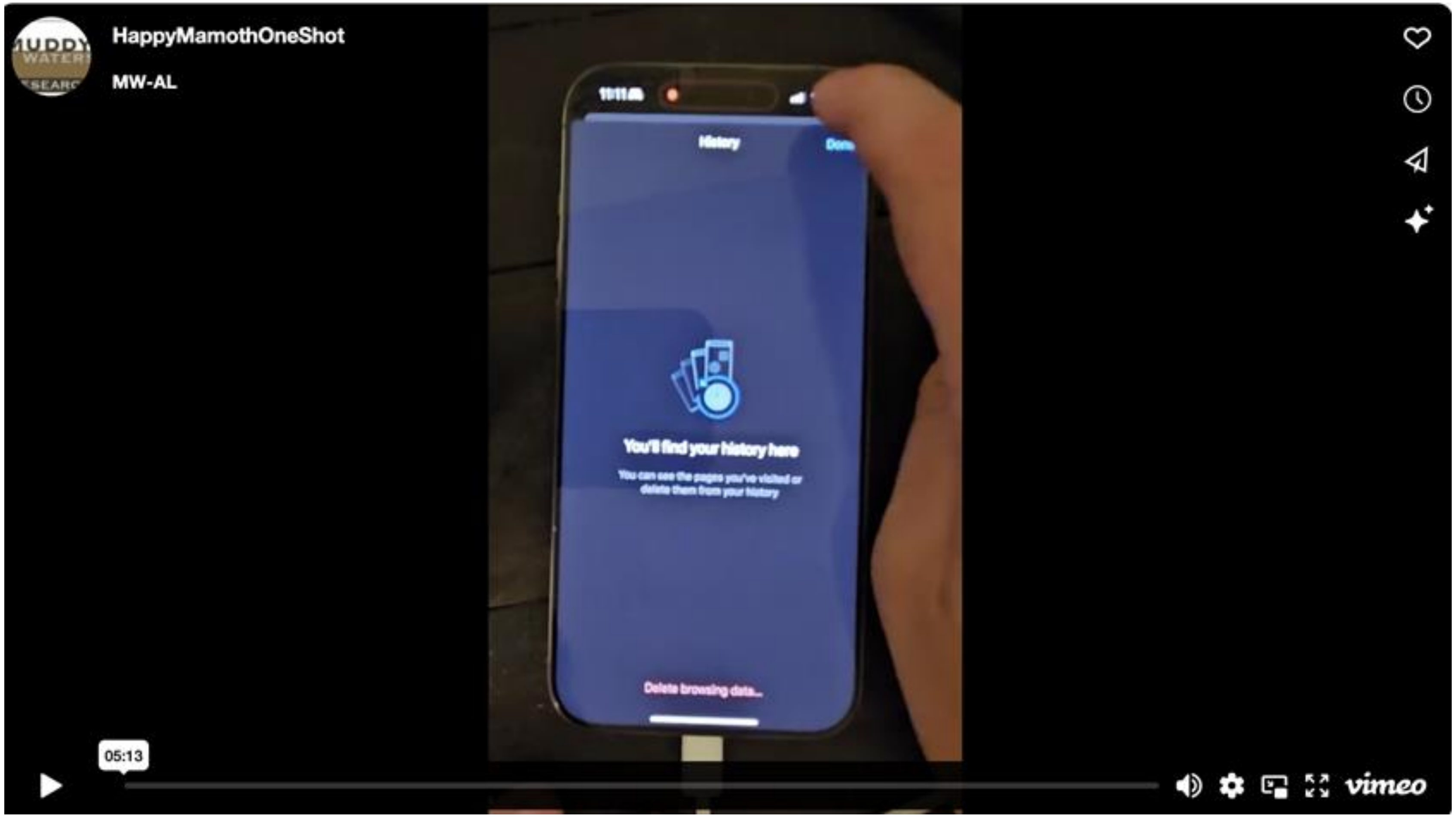
Example: Immediate Retargeting After Cart Abandonment

In this video, the user performs the following steps, which together provide behavioral evidence of fingerprinting and aggressive retargeting tactics:

- Clears all device browsers of cookies
- Newly installs the 3P app, Zynga's Words With Friends
- Signs in as a guest, asks not to be tracked, activates VPN
- Browses to the e-commerce store "Happy Mammoth"
- Adds an item to the Happy Mammoth cart, but does not complete the purchase
- After opening the game, the 2nd ad received from APP is for "Happy Mammoth"

Video URL:
https://www.youtube.com/watch?v=h9nd7oRgh9c

Below: Video of Happy Mammoth ad-to-cart followed by APP Ad for Happy Mammoth Product



You'll find your history here

You can see the pages you've visited or delete them from your history

Delete browsing data...

Sales Are Only ~25-35% Incremental, but APP's CEO Claims it's ~100%

Of the remaining ~48% of sales in which APP had the first click, ~29% show touch points from other ad networks. Therefore, we believe that likely only ~34% of purchases attributed to APP are incremental.[2] After adjusting for the typical e-commerce repeat customer rate of ~28%,[3] this number drops to ~25%.

APPs CEO stated the following:

> *"Early data has exceeded our expectations, with the advertisers in the pilot seeing substantial returns, often surpassing those from other media channels and, in many cases, experiencing nearly 100% incrementality from our traffic."*
>
> *– APP CEO Adam Foroughi, Q3 2024 earnings call*

[2] 52% - 100% = 48%. 48% - (29%*48%) = 34%

[3] A Shopify blog cites a study indicating an average of 28.2% (20.9% low ~ 36.2% high) of e-commerce customers are repeat customers, therefore it is possible or likely that some of those 34% were in fact returning customers, and true incrementality is even lower. Adjusting for the ~28% Shopify repeat customer rate, this figure could be as low as 25%. https://www.shopify.com/enterprise/blog/ecommerce-customer-retention, https://www.metrilo.com/blog/repeat-purchase-rate

~22.6% of APP’s E-commerce Customers Appear to Have Churned in Q1 2025

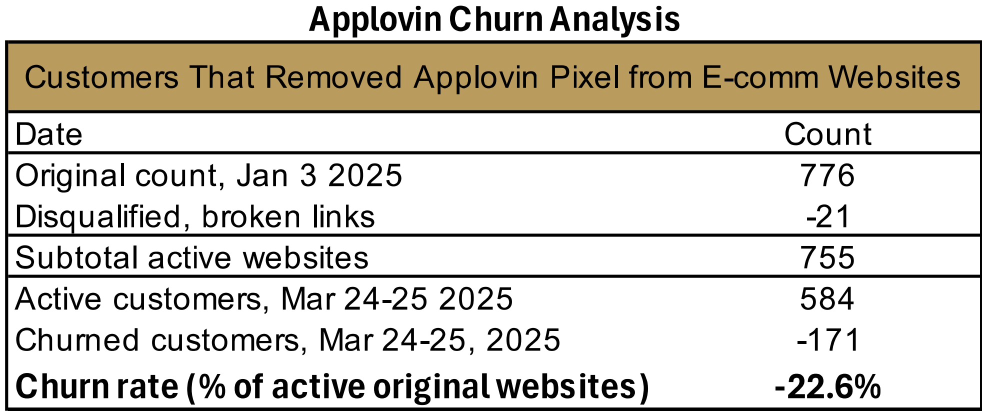
To understand churn, we scanned the web for e-commerce trial customers having APP’s Axon pixel. We originally conducted a search on Jan 3, 2025. To analyze churn, we re-ran checks on these same customers on March 24-26, 2025.

On Jan 3, we found 776 customers’ websites that contained the Axon pixel. In March, we found 21 sites with broken links, reducing the number of original active sites to 755. Of these, 171 no longer contained the pixel, indicating a churn rate of at least ~22.6%.[1]

This churn rate is based only on those customers who removed the pixel. We are aware of customers who stopped spending on APP, but who have not yet removed the pixel. This analysis would not detect customers who have significantly cut spend through APP.

APP’s CEO reportedly claimed APP experienced “no churn” among its e-commerce beta customers.[2]

See Appendix for additional details on methodology.



Applovin Churn Analysis

Customers That Removed Applovin Pixel from E-comm Websites	
Date	Count
Original count, Jan 3 2025	776
Disqualified, broken links	-21
Subtotal active websites	755
Active customers, Mar 24-25 2025	584
Churned customers, Mar 24-25, 2025	-171
Churn rate (% of active original websites)	**-22.6%**

[1] APP Note from our CEO: https://www.applovin.com/blog/note-from-our-ceo/ This number tracks with CEO’s statement that the number of e-commerce customers was ~600 (584 + 21 broken links = 605).
[2] March 2025 sell-side research report.

APP Systemically Violates TOS by Creating Persistent Identity Graphs (PIGs)

APP Systematically Violates TOS by Creating Persistent Identity Graphs (PIGs)

APPs Persistent Identity Graphs (PIGs) are digital collections of personal identifying information (PII). APP collects and stores this personal user data on its servers. APPs development and storage of PIG data are a type of "fingerprinting", a form of digital profiling of individual users without their knowledge or consent to track them across the web.

Fingerprinting aggregates various device and browser signals to create a unique identifier for users without relying on cookies. In addition to the 3P platform IDs collected, other shared information will commonly include the ip address, operating system, browser version, time zone, browser identifier, or device information (screen size, fonts installed, language). Unlike cookies, which users can delete or block, fingerprinting operates server-side, making it a persistent tracking mechanism that raises major privacy concerns.[1] Fingerprinting is often considered controversial and invasive because it does not require user consent. Regulatory bodies and major tech companies like Apple and Meta have taken measures to limit or regulate fingerprinting due to its potential ethical and legal implications.

Fingerprinting without consent generally violates key privacy rules and TOS with its major platform partners. Fingerprinting without consent is explicitly prohibited by Apple on its iOS devices. As a Meta Audience Network Partner[2] APP is subject to additional restrictions. Meta expressly prohibits the collecting or storage of any data obtained from any Ad or use of the Audience Network Service.

Code reveals APPs collection of Facebook, Google, Snap, Reddit, as well as other platforms IDs. These code IDs can be clearly traced to their platforms.

Proof of the collection of these data are clear and reproducible.

APPs CEO claims to have neither the means nor desire to look at other companies' user data, but the evidence in its code indicates the opposite – APP has the means and is engaging in collecting 3P platforms data to construct its PIGs.

[1] Because It is unlikely a user will regularly change their browser characteristics, operating system, or IP address, the fingerprints stay unchanged, or "persist".
[2] https://www.applovin.com/partners/

Example: APP Systematically Violates TOS by Creating Persistent Identity Graphs (PIGs)

Code from APP e-commerce client Hume Health’s website reveals APP is collecting IDs of partners such as Meta, Google, Snap, Tiktok, and others. APP’s code labels each of these IDs as a “key” and sends them to its own servers. These IDs are stitched together to create what we call a Persistent identity Graph (PIG).

Shopify events are also collected (e.g. cookies indicating an add to cart, checkout initiated, and/or Shopify’s own 1P “y_coo kie”) and added to the “PIG.”[1]

The collection of Shopify event data is critical to the success of the e-commerce launch because these behavioral actions inform APP’s ad auction bids. We infer that APP’s algorithm is specifically trained to target high-value users. Knowing which users are poised to make purchases, especially those with items in carts or who are in the checkout process, is extremely valuable information (i.e., a black edge).

APP’s PIGs Violate Apple’s TOS

Apple clearly states that fingerprinting without consent violates its Apple Developer Program License Agreement. Fingerprinting is explicitly prohibited by Apple on its iOS devices.[1] (Bold emphasis added)

> ***“Can I use App AdAttributionKit in conjunction with fingerprinting?***
>
> ***No. You may not derive data from a device for the purpose of uniquely identifying it, per the Apple Developer Program License Agreement.*** *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.”*

Apple’s rules about data collection and storage also clearly state that user consent is required for user data collection, even if the data is considered anonymous. Additionally, the collected data must be the minimum necessary and limited only to that which is legitimate interest and relevant to the core function of the app.[2] (Bold emphasis added)

> *“5.1.1 Data Collection and Storage*
> *(ii) Permission: Apps that collect user or usage data must secure* ***user consent for the collection, even if such data is considered to be anonymous****... Apps that collect data for a legitimate interest without consent by relying on the terms of the EU’s GDPR or similar statute must comply with all terms of that law.*
> ***(iii) Data Minimization: Apps should only request access to data relevant to the core functionality of the app and should only collect and use data that is required to accomplish the relevant task****…*
> *(iv) Access: Apps must respect the user’s permission settings and not attempt to manipulate, trick, or force people to consent to unnecessary data access.”*

[1] https://developer.apple.com/app-store/ad-attribution/
[2] https://developer.apple.com/app-store/review/guidelines/#data-collection-and-storage

Meta’s Audience Network Partner TOS Expressly Prohibits Collecting, Storing, or Using Data from Meta

As a Meta Audience Network Partner[2] APP is subject to additional restrictions. Meta expressly prohibits the collection or storage of any data obtained from any Ad or use of the Audience Network Service (Bold emphasis added).

“Meta Audience Network Terms: 3. Implementation.: Violations include “misusing or deriving data from the technology (e.g., the Audience Network SDK, Meta tags, or Meta APIs', as applicable) made available to Publisher by Meta (the "Audience Network Tools"). Meta may modify, suspend, or terminate Publisher’s access to, or discontinue the availability of, the Audience Network Tools at any time.”

Meta Audience Network Terms: 5. Privacy and Data. “…Publisher agrees that it will not (a) collect, store, or use any information about any user derived from the Ad served by Meta to such user on the Publisher Properties, including information derived from the content of the Ad creative, a user’s engagement with the Ad, or the content accessed by a user after navigating to the Ad landing page; (b) use (i) data from the Audience Network Service to categorize a user of Publisher Properties as a Meta user, (ii) identifiers provided by Meta to retarget users or deliver advertising based on user behaviors apart from the Audience Network Service, or (iii) any Meta Advertising Data to build or enhance profiles, including any profiles associated with any personally identifiable information, mobile device identifier, or other unique identifier that identifies any particular individual, user, browser, computer or device; …. In addition, with respect to Publisher Properties, Publisher will (y) deploy administrative, physical and technical safeguards that prevent unauthorized access to any Meta Advertising Data in its possession or control; and (z) provide Meta with reasonably prompt written notice as soon as it becomes aware that it has or is likely to breach any of the terms set forth in this Section.”

APP’s 2023 Disclosure Change Emphasizes the Risk of Being Deplatformed for Violating TOS

In 2023, APP added to its risk disclosure about its reliance on Apple and other 3P platforms. The new disclosure explains that Apple’s privacy controls compel advertisers to justify data received through certain APIs.[1] These apply to software companies operating on Apple devices. [2] We explain infra that fingerprinting occurs not via the APIs, but on its own servers, which Apple cannot directly monitor. We contend that APP engages in Fingerprinting 2.0 by creating user graphs composed of other platforms unique identifiers like the Facebook “fbp”, Google “ga”, etc. and importantly marrying this up with an e-commerce site like Shopify’s event data to recognize whether such users are high value. These actions, especially when considered in their totality, present as major violations of key partner platforms’ privacy policies. (Bold emphasis added)

> *Additionally, Apple implemented new requirements for consumer disclosures regarding privacy and data processing practices in December 2020, which has resulted in increased compliance requirements and could result in decreased usage of our Apps. Apple incorporated new SDK privacy controls into iOS 17, which was released in September 2023, including privacy manifests and signatures designed to allow app developers to outline the data practices for SDKs embedded in their apps, manage tracking domains within SDKs, and* ***curb device fingerprinting by requiring app developers to select allowed reasons for using data received through certain APIs.*** *Apple indicated that it expects privacy manifests and signatures to become part of the App Store review in Spring 2024.*

[1] APP 2023 10-K, p. 13

Big Tech Routinely Deplatforms App Developers that Violate their TOS

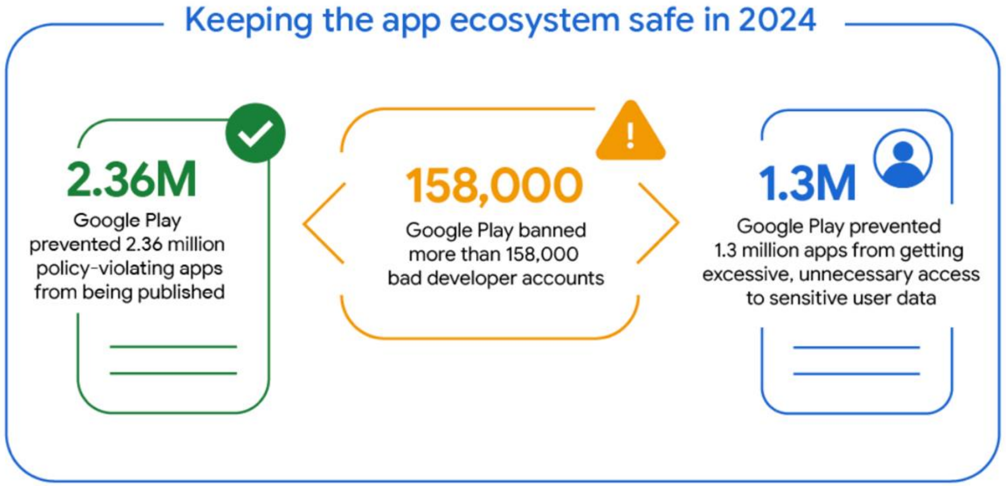
Big Tech blocks or removes over a million apps each year for TOS privacy violations. Cheetah Mobile is a prominent example of this.

In 2024, Google “prevented 1.3 million apps from getting excessive, unnecessary access to sensitive user data” and banned more than 158,000 bad developer accounts that attempted to publish harmful apps.[1]

In 2022 and 2023, Apple terminated over 500,000 developer accounts.[2]

Pixalate, a privacy and compliance analytics platform, reported that from Q1 2021 to Q4 2024, 1.89 million apps were delisted from the Apple App Store. In Q4 2024 alone, Apple reportedly deplatformed 336,500 apps with most coming at year end and being registered by US companies.[3,4]

Below: In 2024, Google Play blocked 1.3m apps from excessive, unnecessary access to sensitive user data



Keeping the app ecosystem safe in 2024

2.36M
Google Play prevented 2.36 million policy-violating apps from being published

158,000
Google Play banned more than 158,000 bad developer accounts

1.3M
Google Play prevented 1.3 million apps from getting excessive, unnecessary access to sensitive user data

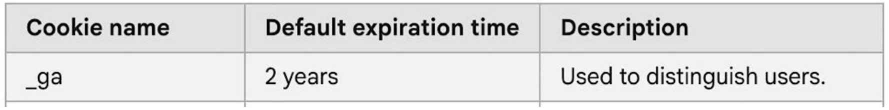
[1] https://security.googleblog.com/2025/01/how-we-kept-google-play-android-app-ecosystem-safe-2024.html
[2] https://www.apple.com/uk/newsroom/2024/05/app-store-stopped-over-7-billion-usd-in-potentially-fraudulent-transactions/
[3] Pixalate DELISTED MOBILE APPS Monthly Report Apple App Store, Dec 2024
[4] https://www.globenewswire.com/news-release/2025/01/17/3011681/0/en/Apple-Purges-Mobile-App-Store-Pixalate-s-December-2024-Delisted-Mobile-Apps-Report-Finds-400K-Apps-Delisted-Across-Apple-336-5K-Google-64K-App-Stores.html

APP Collects Proprietary 3P IDs

Code reveals APPs collection of Google, Facebook, Instagram, Snap, TikTok as well as other platforms' IDs. Most of these code IDs can easily be traced to their platforms where details of their properties and duration are commonly provided.

Google's "_ga", Ad-click identifier (typically stored in 1P cookies) with two-year duration. [1]

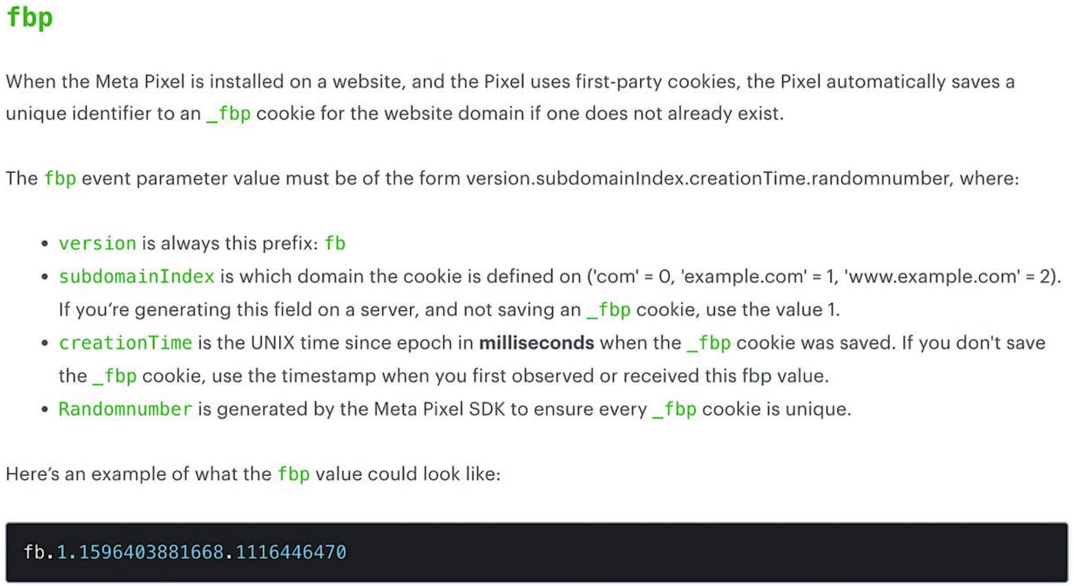
'_ga', the main cookie used by Google Analytics, enables the service to distinguish one visitor from another and lasts for 2 years. Any site that implements Google Analytics, including Google services, uses the '_ga' cookie. Each '_ga' cookie is unique to the specific property, so it cannot be used to track a given user or browser across unrelated websites.



Cookie name	Default expiration time	Description
_ga	2 years	Used to distinguish users.

Facebook's "fbp", a unique 1P browser cookie, with three months duration.[2]

When the Meta Pixel is installed on a website, and the Pixel uses first-party cookies, the Pixel automatically saves a unique identifier to an *_fbp* cookie for the website domain if one does not already exist.



fbp

When the Meta Pixel is installed on a website, and the Pixel uses first-party cookies, the Pixel automatically saves a unique identifier to an `_fbp` cookie for the website domain if one does not already exist.

The `fbp` event parameter value must be of the form version.subdomainIndex.creationTime.randomnumber, where:

- `version` is always this prefix: `fb`
- `subdomainIndex` is which domain the cookie is defined on ('com' = 0, 'example.com' = 1, 'www.example.com' = 2). If you're generating this field on a server, and not saving an `_fbp` cookie, use the value 1.
- `creationTime` is the UNIX time since epoch in **milliseconds** when the `_fbp` cookie was saved. If you don't save the `_fbp` cookie, use the timestamp when you first observed or received this fbp value.
- `Randomnumber` is generated by the Meta Pixel SDK to ensure every `_fbp` cookie is unique.

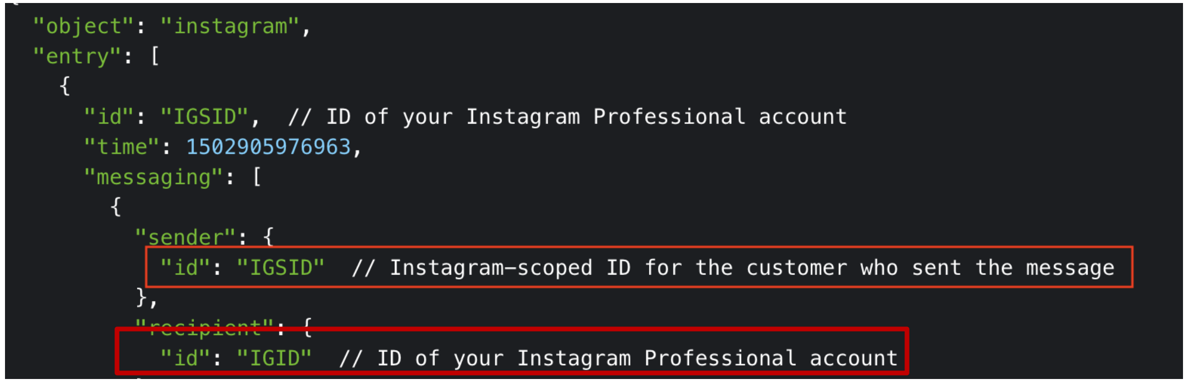
Here's an example of what the `fbp` value could look like:

```
fb.1.1596403881668.1116446470
```

[1] https://policies.google.com/technologies/cookies?hl=en-US , https://support.google.com/analytics/answer/11397207
[2] https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/

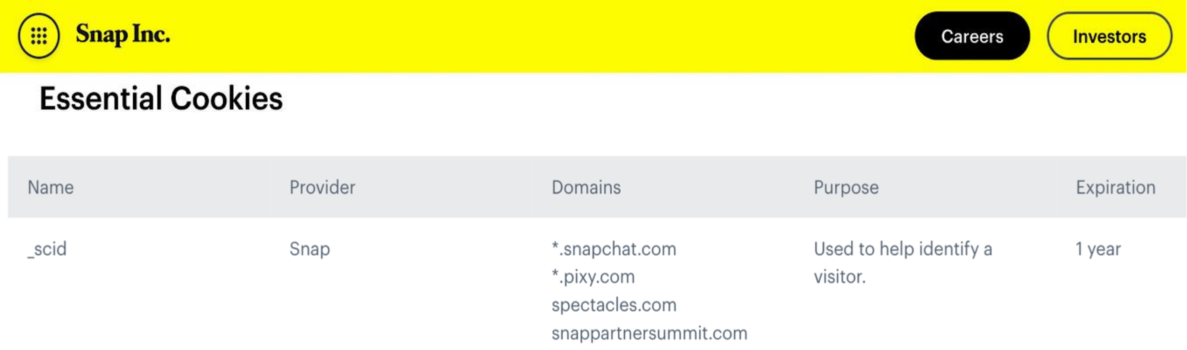
APP Collects Proprietary 3P IDs (2)

Instagram's “igID” is an ID for an Instagram Professional account [1]



```
  "object": "instagram",
  "entry": [
    {
      "id": "IGSID",  // ID of your Instagram Professional account
      "time": 1502905976963,
      "messaging": [
        {
          "sender": {
            "id": "IGSID"  // Instagram-scoped ID for the customer who sent the message
          },
          "recipient": {
            "id": "IGID"  // ID of your Instagram Professional account
```

Snap’s “scid” is used to help identify a visitor. It has a one-year expiration.[2]



Essential Cookies

Name	Provider	Domains	Purpose	Expiration
_scid	Snap	*.snapchat.com *.pixy.com spectacles.com snappartnersummit.com	Used to help identify a visitor.	1 year

[1] https://developers.facebook.com/docs/messenger-platform/instagram/features/webhook/
[2] https://www.snap.com/privacy/cookie-information

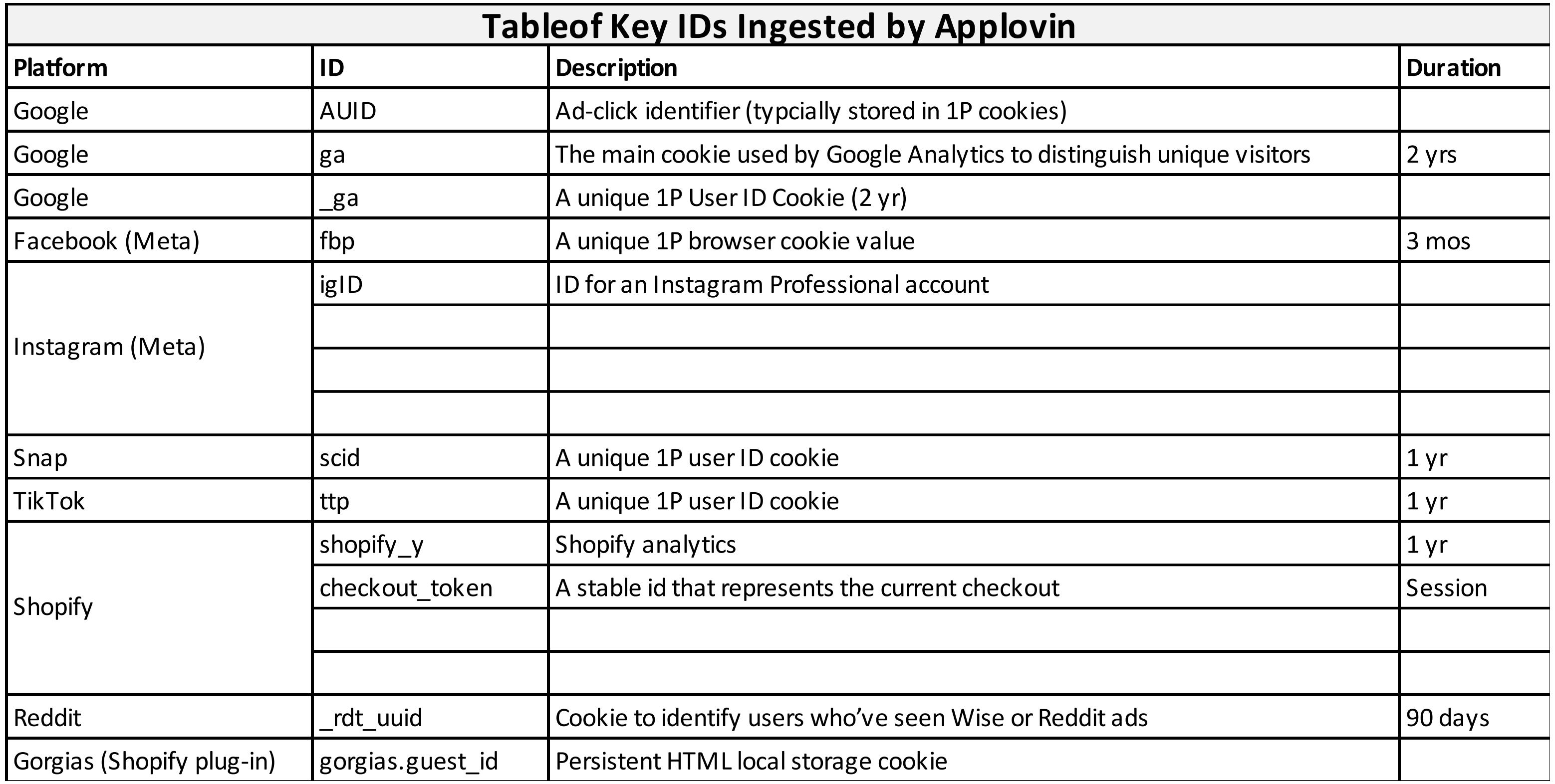
APP Collects Proprietary 3P IDs (3)

The table at right provide a list identifiers we observed being collected by APP. APP collects and structures these IDs in its code's payload (e.g., it uses the common naming convention "key" to preface these IDs).

As shown in the following examples, the data is collected from the advertisers' websites. In most cases, these collected identifiers are persistent, with durations up to one or two years.

In addition to this sensitive data, our team also observed other important and sensitive being ingested, including: telemetry, ip addresses, device data, as well as other Shopify plug-ins, such as Fondue cart, Recart, etc.

Below: The table lists the data our tech team observed APP identifying as "key" 3P IDs, ingesting, and sending to itself.



Tableof Key IDs Ingested by Applovin

Platform	ID	Description	Duration
Google	AUID	Ad-click identifier (typcially stored in 1P cookies)	
Google	ga	The main cookie used by Google Analytics to distinguish unique visitors	2 yrs
Google	_ga	A unique 1P User ID Cookie (2 yr)	
Facebook (Meta)	fbp	A unique 1P browser cookie value	3 mos
Instagram (Meta)	igID	ID for an Instagram Professional account	
Snap	scid	A unique 1P user ID cookie	1 yr
TikTok	ttp	A unique 1P user ID cookie	1 yr
Shopify	shopify_y	Shopify analytics	1 yr
	checkout_token	A stable id that represents the current checkout	Session
Reddit	_rdt_uuid	Cookie to identify users who've seen Wise or Reddit ads	90 days
Gorgias (Shopify plug-in)	gorgias.guest_id	Persistent HTML local storage cookie	

Example: APP Client Website Contains Numerous 3Ps' Proprietary User Data

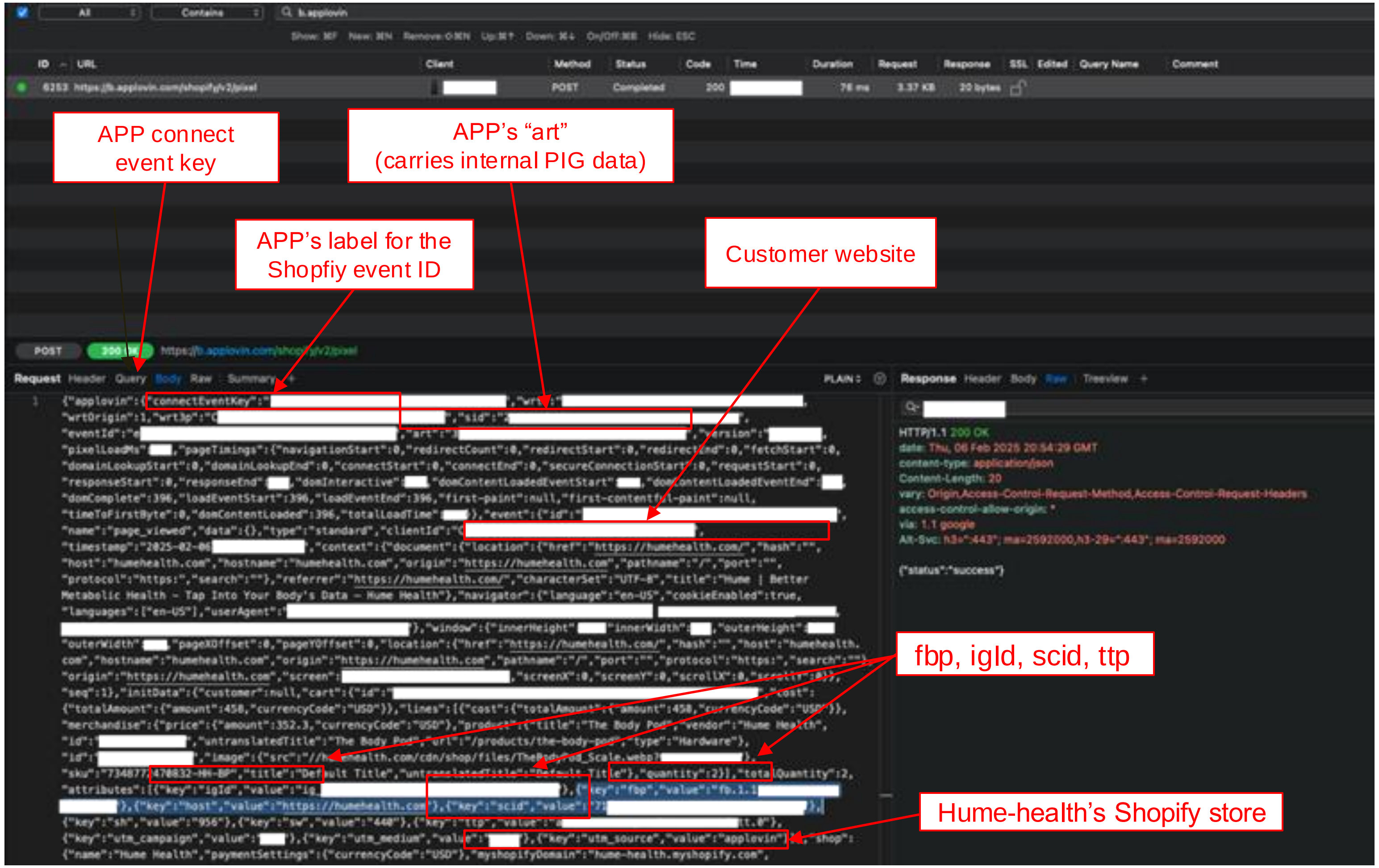
APP claims to be able to deliver performance targeting without PII. However, its code collects and structures IDs and other information from across many major platforms including Shopify, Google, Facebook, Snap, Instagram, TikTok, etc.

The 3P IDs are being collected, structured, and labelled as "key" by APP on its advertising clients' websites.

The image at right is data being sent to the APP server from the Hume Health website (PII redacted). It includes:

- Facebook's ID: fbp
- Instagram's ID: igid
- Snap's ID: scid
- TikTok's ID: ttp
- Shopify store address
- Shopify event ID[1]

Below: the b.applovin tag (pixel) is ingesting multiple platforms' key IDs from the Hume Health webpage



```
All    Contains    b.applovin
Show: ⌘F  New: ⌘N  Remove:⇧⌘N  Up:⌘↑  Down: ⌘↓  On/Off:⌘B  Hide: ESC
ID  URL                                          Client      Method  Status     Code  Time        Duration  Request  Response  SSL  Edited  Query Name  Comment
6253 https://b.applovin.com/shopify/v2/pixel    [redacted]  POST    Completed  200   [redacted]  76 ms     3.37 KB  20 bytes
```

APP connect event key

APP's "art" (carries internal PIG data)

APP's label for the Shopfiy event ID

Customer website

```
POST  200 OK  https://b.applovin.com/shopify/v2/pixel
Request  Header  Query  Body  Raw  Summary  +                                   PLAIN
```

```
{"applovin":{"connectEventKey":"[redacted]","wrt":"[redacted],
"wrtOrigin":1,"wrt3p":"C[redacted]","sid":"2[redacted],
"eventId":"e[redacted]","art":"1[redacted]","version":"[redacted],
"pixelLoadMs"[redacted],"pageTimings":{"navigationStart":0,"redirectCount":0,"redirectStart":0,"redirectEnd":0,"fetchStart":0,
"domainLookupStart":0,"domainLookupEnd":0,"connectStart":0,"connectEnd":0,"secureConnectionStart":0,"requestStart":0,
"responseStart":0,"responseEnd"[redacted],"domInteractive"[redacted],"domContentLoadedEventStart"[redacted],"domContentLoadedEventEnd":[redacted],
"domComplete":396,"loadEventStart":396,"loadEventEnd":396,"first-paint":null,"first-contentful-paint":null,
"timeToFirstByte":0,"domContentLoaded":396,"totalLoadTime"[redacted]},"event":{"id":"[redacted]",
"name":"page_viewed","data":{},"type":"standard","clientId":"C[redacted],
"timestamp":"2025-02-06[redacted]","context":{"document":{"location":{"href":"https://humehealth.com/","hash":"",
"host":"humehealth.com","hostname":"humehealth.com","origin":"https://humehealth.com","pathname":"/","port":"",
"protocol":"https:","search":""},"referrer":"https://humehealth.com/","characterSet":"UTF-8","title":"Hume | Better
Metabolic Health - Tap Into Your Body's Data - Hume Health"},"navigator":{"language":"en-US","cookieEnabled":true,
"languages":["en-US"],"userAgent":"[redacted]
[redacted]"},"window":{"innerHeight"[redacted]"innerWidth":[redacted],"outerHeight":[redacted]
"outerWidth"[redacted],"pageXOffset":0,"pageYOffset":0,"location":{"href":"https://humehealth.com/","hash":"","host":"humehealth.
com","hostname":"humehealth.com","origin":"https://humehealth.com","pathname":"/","port":"","protocol":"https:","search":""},
"origin":"https://humehealth.com","screen":[redacted],"screenX":0,"screenY":0,"scrollX":0,"scrollY":0}},
"seq":1},"initData":{"customer":null,"cart":{"id":"[redacted]","cost":
{"totalAmount":{"amount":458,"currencyCode":"USD"}},"lines":[{"cost":{"totalAmount":{"amount":458,"currencyCode":"USD"}},
"merchandise":{"price":{"amount":352.3,"currencyCode":"USD"},"product":{"title":"The Body Pod","vendor":"Hume Health",
"id":"[redacted]","untranslatedTitle":"The Body Pod","url":"/products/the-body-pod","type":"Hardware"},
"id":"[redacted]","image":{"src":"//humehealth.com/cdn/shop/files/TheBodyPod_Scale.webp?[redacted]},
"sku":"734877470832-HH-BP","title":"Default Title","untranslatedTitle":"Default Title"},"quantity":2}],"totalQuantity":2,
"attributes":[{"key":"igId","value":"ig[redacted]},{"key":"fbp","value":"fb.1.1[redacted]
[redacted]},{"key":"host","value":"https://humehealth.com"},{"key":"scid","value":"7[redacted]},
{"key":"sh","value":"956"},{"key":"sw","value":"440"},{"key":"ttp","value":"a[redacted]tt.0"},
{"key":"utm_campaign","value":"[redacted]},{"key":"utm_medium","value":"[redacted]},{"key":"utm_source","value":"applovin"},"shop":
{"name":"Hume Health","paymentSettings":{"currencyCode":"USD"},"myshopifyDomain":"hume-health.myshopify.com",
```

```
Response  Header  Body  Raw  Treeview  +
[redacted]
HTTP/1.1 200 OK
date: Thu, 06 Feb 2025 20:54:29 GMT
content-type: application/json
Content-Length: 20
vary: Origin,Access-Control-Request-Method,Access-Control-Request-Headers
access-control-allow-origin: *
via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"status":"success"}
```

fbp, igId, scid, ttp

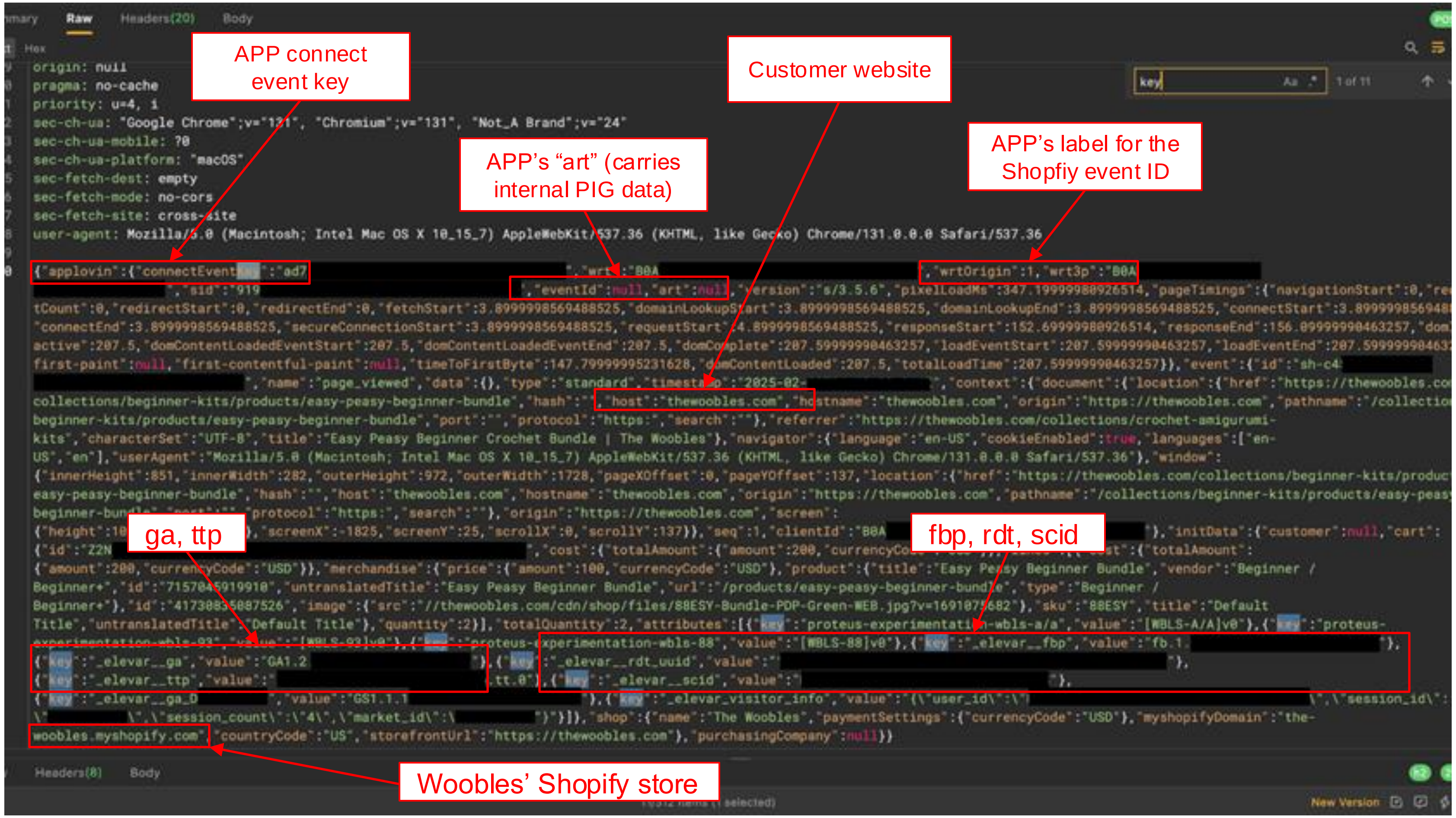
Hume-health's Shopify store

[1] APP associates the Shopify y cookie with the wrt3p function in its code, See Appendix.

Example: APP Client Website Contains Numerous 3Ps' Proprietary User Data

At right is an example of code being sent to APP's server from thewoobles.com. It contains structured proprietary 3P user data, including:

- Google id: ga
- Reddit id: rdt
- Facebook id: fbp
- Snap id: scid
- Tiktok id: ttp
- Shopify store address
- Shopify event ID[1]



```
origin: null
pragma: no-cache
priority: u=4, i
sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
sec-fetch-dest: empty
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

{"applovin":{"connectEventKey":"ad7[redacted]","wrt":"B0A[redacted]","wrtOrigin":1,"wrt3p":"B0A[redacted]
[redacted]","sid":"919[redacted]","eventId":null,"art":null,"version":"s/3.5.6","pixelLoadMs":347.19999980926514,"pageTimings":{"navigationStart":0,"re
tCount":0,"redirectStart":0,"redirectEnd":0,"fetchStart":3.8999998569488525,"domainLookupStart":3.8999998569488525,"domainLookupEnd":3.8999998569488525,"connectStart":3.89999985694
"connectEnd":3.8999998569488525,"secureConnectionStart":3.8999998569488525,"requestStart":4.8999998569488525,"responseStart":152.69999980926514,"responseEnd":156.09999990463257,"dom
active":207.5,"domContentLoadedEventStart":207.5,"domContentLoadedEventEnd":207.5,"domComplete":207.59999990463257,"loadEventStart":207.59999990463257,"loadEventEnd":207.599999904632
first-paint":null,"first-contentful-paint":null,"timeToFirstByte":147.79999995231628,"domContentLoaded":207.5,"totalLoadTime":207.59999990463257}},"event":{"id":"sh-c4[redacted]
[redacted]","name":"page_viewed","data":{},"type":"standard","timestamp":"2025-02-[redacted]","context":{"document":{"location":{"href":"https://thewoobles.co
collections/beginner-kits/products/easy-peasy-beginner-bundle","hash":"","host":"thewoobles.com","hostname":"thewoobles.com","origin":"https://thewoobles.com","pathname":"/collectio
beginner-kits/products/easy-peasy-beginner-bundle","port":"","protocol":"https:","search":""},"referrer":"https://thewoobles.com/collections/crochet-amigurumi-
kits","characterSet":"UTF-8","title":"Easy Peasy Beginner Crochet Bundle | The Woobles"},"navigator":{"language":"en-US","cookieEnabled":true,"languages":["en-
US","en"],"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"},"window":
{"innerHeight":851,"innerWidth":282,"outerHeight":972,"outerWidth":1728,"pageXOffset":0,"pageYOffset":137,"location":{"href":"https://thewoobles.com/collections/beginner-kits/produc
easy-peasy-beginner-bundle","hash":"","host":"thewoobles.com","hostname":"thewoobles.com","origin":"https://thewoobles.com","pathname":"/collections/beginner-kits/products/easy-peas
beginner-bun                ,"protocol":"https:","search":""},"origin":"https://thewoobles.com","screen":
{"height":10                },"screenX":-1825,"screenY":25,"scrollX":0,"scrollY":137}},"seq":1,"clientId":"B0A[redacted]"},"initData":{"customer":null,"cart":
{"id":"Z2N[redacted]","cost":{"totalAmount":{"amount":200,"currencyCo                st":{"totalAmount":
{"amount":200,"currencyCode":"USD"}},"merchandise":{"price":{"amount":100,"currencyCode":"USD"},"product":{"title":"Easy Peasy Beginner Bundle","vendor":"Beginner /
Beginner+","id":"7157045919910","untranslatedTitle":"Easy Peasy Beginner Bundle","url":"/products/easy-peasy-beginner-bundle","type":"Beginner /
Beginner+"},"id":"41730835887526","image":{"src":"//thewoobles.com/cdn/shop/files/88ESY-Bundle-PDP-Green-WEB.jpg?v=1691075682"},"sku":"88ESY","title":"Default
Title","untranslatedTitle":"Default Title"},"quantity":2}],"totalQuantity":2,"attributes":[{"key":"proteus-experimentation-wbls-a/a","value":"[WBLS-A/A]v0"},{"key":"proteus-
experimentation-wbls-93","value":"[WBLS-93]v0"},{"key":"proteus-experimentation-wbls-88","value":"[WBLS-88]v0"},{"key":"_elevar__fbp","value":"fb.1.[redacted]"},
{"key":"_elevar__ga","value":"GA1.2[redacted]"},{"key":"_elevar__rdt_uuid","value":"[redacted]"},
{"key":"_elevar__ttp","value":"[redacted].tt.0"},{"key":"_elevar__scid","value":"[redacted]"},
{"key":"_elevar__ga_D[redacted]","value":"GS1.1.1[redacted]"},{"key":"_elevar_visitor_info","value":"{\"user_id\":\"[redacted]\",\"session_id\":
\"[redacted]\",\"session_count\":\"4\",\"market_id\":\[redacted]\"}"}]},"shop":{"name":"The Woobles","paymentSettings":{"currencyCode":"USD"},"myshopifyDomain":"the-
woobles.myshopify.com","countryCode":"US","storefrontUrl":"https://thewoobles.com"},"purchasingCompany":null}}
```

APP connect event key

Customer website

APP's "art" (carries internal PIG data)

APP's label for the Shopfiy event ID

ga, ttp

fbp, rdt, scid

Woobles' Shopify store

How to Verify APP's Data Collection

To see how APP collects identities fingerprints to create its PIGs follow the steps below (best results in US).[1]

Note: This process is to be carried out on a laptop (widows or Mac). An accompanying guide with screen shots is provided in the Appendix.[2]

1. Go to one of APP's customer websites, e.g.: trueclassictees.com
2. Right-click → select "Inspect" to open "Chrome DevTools"
3. Add any item to cart, then click "Checkout"
4. In DevTools, go to the "Network" tab
5. In the search bar, type: b.applovin.com
6. Click the top successfully loaded requests in the list. Successful requests are denoted as {:} pixel.
7. Go to the "Payload" tab, then → Expand initData (open the arrow) → select "cart" → select "attributes"
8. Look for entries with a "key" and "value" structure*

*what "keys" are being collected will vary from user to user, but there will most likely be a 3 to 10 key items being collected.

- These are labeled identifiers, like "igID", "_isApplePay" enabled,
- The "wrt3p" field is normally Shopify event, the event type can vary.
- "gorgias.guest_id", "RecartSessionId", etc.

Note: subsequent to the publication by other recent short reports, we observed changes in the data APP is collecting, potentially collecting a smaller number of 3P IDs on Hume Health's. This appears to be APP attempting to cover its tracks.

[1] We have seen high reproducibility in the US, but found other countries (such as Canada) may be blocked - even with a VPN set to a US ip address. In some cases where the user is on an unusual IP address (i.e. not where the user commonly resides or frequents) the ad retargeting may be delayed. We posit that this may be due to the algorithm's uncertainty of the user's identity in the new environment (as indicated by a new ip address).

[2] See Appendix Guide to Desktop Checking on Fingerprinting.

APP’s CEO Claims APP Does not Have, nor Desires, 3P User Data

In Adam Foroughi’s February 26 response to two short sellers’ reports, he claimed (emphasis added):

> *“…we obtain data from our partners solely in the context of providing them with advertising services; we do not work separately with data brokers. Adjust and MAX operations are entirely independent and transparent, with no conflicts or house bias. We also do not have any means or desire to look at other company’s bid or user data; our models use solely behavioral data, ad engagement data, win/loss notifications from mediation (same data shared to any bidder on our platform), and advertiser data to generate predictions* ***.”*** [1]

[1] APP, Note from our CEO, Adam Foroughi, Feb 26, 2025 (emphasis added) https://www.applovin.com/?p=37771

APP's Fingerprinting Scheme is Designed to Avoid Detection

How APP Avoids Detection by Platforms and Partners

APP's impropriety occurs outside the MAX mediation stack. It happens on advertisers' websites and APP's own servers – **where Google, Meta, and other partners and platforms can't see it**.

To avoid detection, APP performs its fingerprinting by collecting and structuring other platforms' pixels as they interact **with advertisers' websites**. This is outside the space which the platforms or its partners monitory.

APP passes this information to its own servers where we deduce it is associated with its compass tokens (CT) and recombines the data to create its PIG. **This is outside the spaces that the platforms or its partners monitor**.

To further obfuscate, the CT token value is labeled with different prefix codes, one for each move. These numerical IDs begin with APP's own "compass_random_token."[2]

- When the user downloads the game, a token value is generated. At this time, it's the "compass random token". This data is stored locally on the user's mobile device, inside each app the APP MAX mediation SDK installed on the device.
- When an in-game ad is requested, the CT's value is added to the URL and moved.
- The CT is re-labelled as the "alart" value.
- When the user reaches the advertiser's website, the CT's value is again changed to the "art" value and sent to b.applovin.com along with any detected platforms' IDs and any other "key" collected data.

Coming full circle, when the ad auction/mediation begins, the CT is called upon again, and if the associated PIG is big, APP knows to bid to win. Because this process of collection and matching occur outside the usual suspect areas, to date, APP's scheme has avoided detection.

We note that the Compass token appears to be a code associated with APP's Compass Analytics software. This is software calculates users' long-term value. It is software that APP has considered a key technology since its IPO, however it has removed mention of this technology from its two most recent 10-Ks.

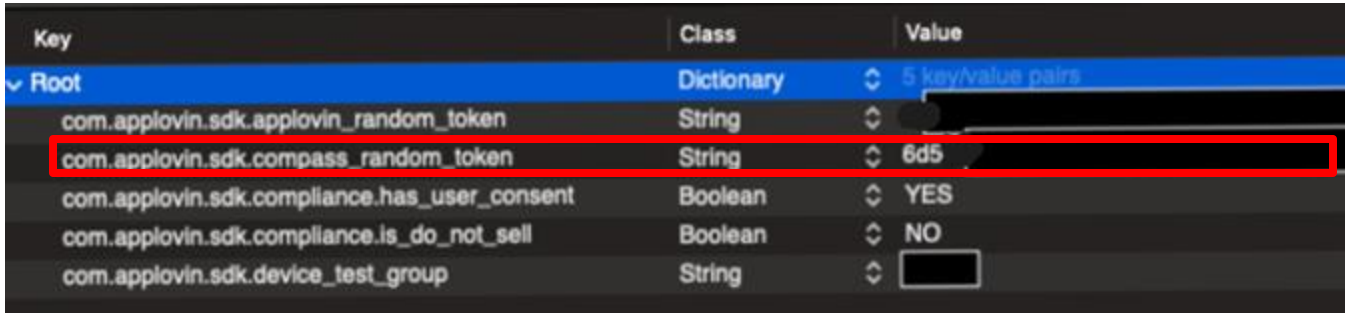
For a more technical explanation, see the Appendix.

[1] 2020 IPO Prospectus 424B4 p. 125 .

Example: The Compass Token Value Moves Across Environments Under Changing Names

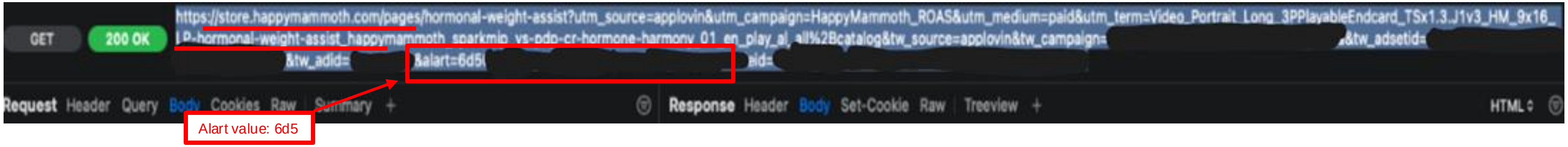
APP’s name changing process appears intended to obfuscate its collection and transmission of 3P user data.

Below: The “compass_random_token” is created with a value of “6d5…” is stored locally on the device



Key	Class	Value
Root	Dictionary	5 key/value pairs
com.applovin.sdk.applovin_random_token	String	[redacted]
com.applovin.sdk.compass_random_token	String	6d5 [redacted]
com.applovin.sdk.compliance.has_user_consent	Boolean	YES
com.applovin.sdk.compliance.is_do_not_sell	Boolean	NO
com.applovin.sdk.device_test_group	String	[redacted]

Below: In a new environment, the Happy Mammoth ad page, the value “6d5…” <u>appears persistently maintained</u> but given the new prefix “alart.”



```
https://store.happymammoth.com/pages/hormonal-weight-assist?utm_source=applovin&utm_campaign=HappyMammoth_ROAS&utm_medium=paid&utm_term=Video_Portrait_Long_3PPlayableEndcard_TSx1.3.J1v3_HM_9x16_
LP-hormonal-weight-assist_happymammoth_sparkmip_vs-pdp-cr-hormone-harmony_01_en_play_al_all%2Bcatalog&tw_source=applovin&tw_campaign=[redacted]&tw_adsetid=[redacted]
[redacted]&tw_adid=[redacted]&alart=6d5[redacted]eid=[redacted]
```

GET
200 OK
Request Header Query Body Cookies Raw Summary +
Response Header Body Set-Cookie Raw Treeview +
HTML ⇕

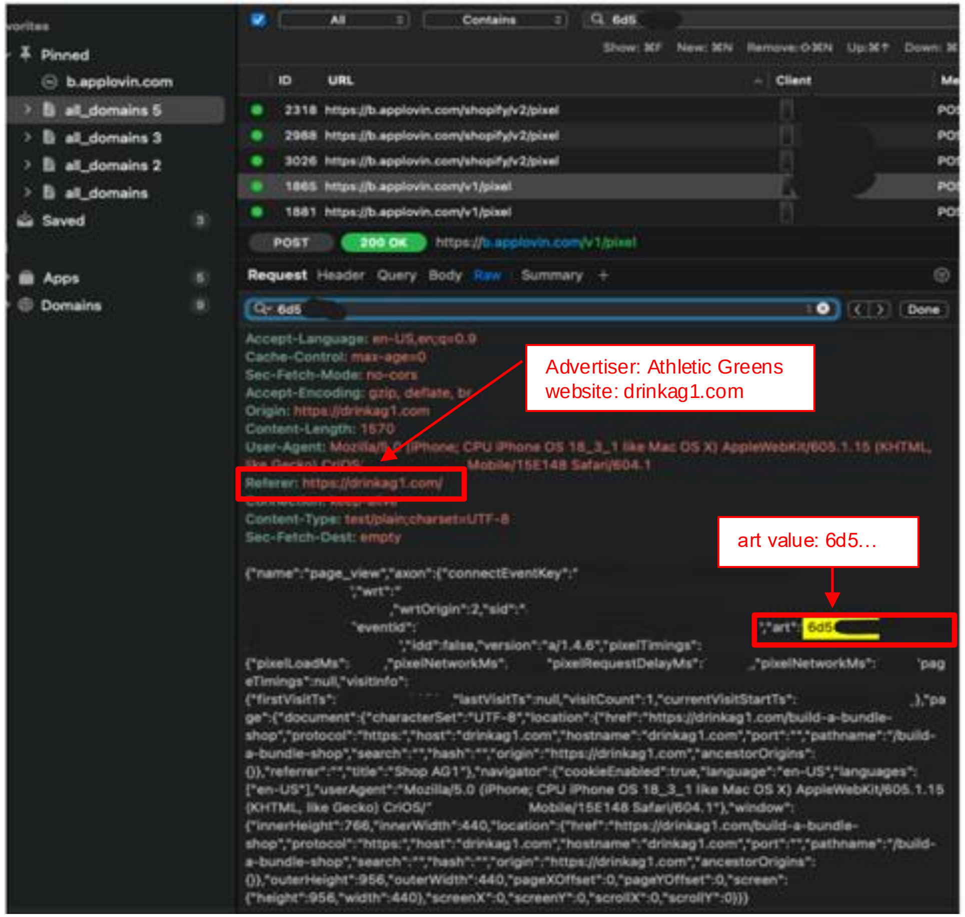
Alart value: 6d5

The User opted out of iOS tracking.
This token is considered a unique and persistent identifier, so all but the first three characters “6d5” have been redacted.

Example: Alart is Persistent but Re-Labeled "Art" as it Again Crosses Environments

In the screen shots below the same art values (6d5….) are passed between or across two different advertisers' websites.

Below: Athletic green's website (drinkag1.com) shows the art value 6d5…



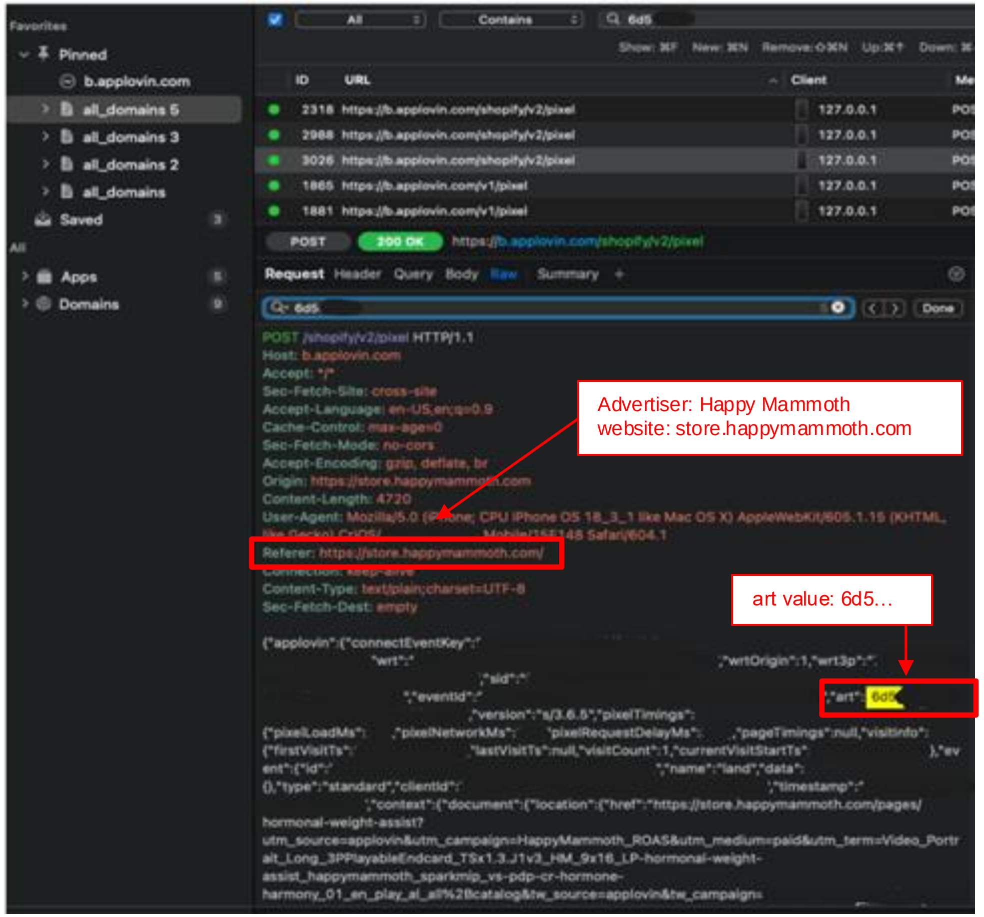
```
vorites
Pinned
  b.applovin.com
  all_domains 5
  all_domains 3
  all_domains 2
  all_domains
Saved                3

Apps                 5
Domains              9
```

```
All   Contains   6d5[redacted]
Show: ⌘F   New: ⌘N   Remove: ⇧⌘N   Up: ⌘↑   Down: ⌘

ID    URL                                             Client   Me
2318  https://b.applovin.com/shopify/v2/pixel        [redacted]  POS
2988  https://b.applovin.com/shopify/v2/pixel                    POS
3026  https://b.applovin.com/shopify/v2/pixel                    POS
1865  https://b.applovin.com/v1/pixel                            POS
1881  https://b.applovin.com/v1/pixel                            POS

POST   200 OK   https://b.applovin.com/v1/pixel

Request  Header  Query  Body  Raw  Summary  +
6d5[redacted]                                   Done

Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Sec-Fetch-Mode: no-cors
Accept-Encoding: gzip, deflate, br
Origin: https://drinkag1.com
Content-Length: 1570
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML,
like Gecko) CriOS/[redacted] Mobile/15E148 Safari/604.1
Referer: https://drinkag1.com/
Connection: keep-alive
Content-Type: text/plain;charset=UTF-8
Sec-Fetch-Dest: empty

{"name":"page_view","axon":{"connectEventKey":"[redacted]
[redacted]","wrt":"[redacted]
[redacted]","wrtOrigin":2,"sid":"[redacted]
[redacted]"eventId":[redacted]                                     ","art":"6d5[redacted]
[redacted]","idd":false,"version":"a/1.4.6","pixelTimings":
{"pixelLoadMs":[redacted],"pixelNetworkMs":[redacted]"pixelRequestDelayMs":[redacted],"pixelNetworkMs":[redacted]'pag
eTimings":null,"visitInfo":
{"firstVisitTs":[redacted]"lastVisitTs":null,"visitCount":1,"currentVisitStartTs":[redacted]},"pa
ge":{"document":{"characterSet":"UTF-8","location":{"href":"https://drinkag1.com/build-a-bundle-
shop","protocol":"https:","host":"drinkag1.com","hostname":"drinkag1.com","port":"","pathname":"/build-
a-bundle-shop","search":"","hash":"","origin":"https://drinkag1.com","ancestorOrigins":
{}},"referrer":"","title":"Shop AG1"},"navigator":{"cookieEnabled":true,"language":"en-US","languages":
["en-US"],"userAgent":"Mozilla/5.0 (iPhone; CPU iPhone OS 18_3_1 like Mac OS X) AppleWebKit/605.1.15
(KHTML, like Gecko) CriOS/"[redacted] Mobile/15E148 Safari/604.1"},"window":
{"innerHeight":766,"innerWidth":440,"location":{"href":"https://drinkag1.com/build-a-bundle-
shop","protocol":"https:","host":"drinkag1.com","hostname":"drinkag1.com","port":"","pathname":"/build-
a-bundle-shop","search":"","hash":"","origin":"https://drinkag1.com","ancestorOrigins":
{}},"outerHeight":956,"outerWidth":440,"pageXOffset":0,"pageYOffset":0,"screen":
{"height":956,"width":440},"screenX":0,"screenY":0,"scrollX":0,"scrollY":0}}}
```

Advertiser: Athletic Greens
website: drinkag1.com

art value: 6d5…

Below: HappyMammoth.com website shows the art value 6d5…



```
Favorites
Pinned
  b.applovin.com
  all_domains 5
  all_domains 3
  all_domains 2
  all_domains
Saved                3
All
Apps                 5
Domains              9
```

```
All   Contains   6d5[redacted]
Show: ⌘F   New: ⌘N   Remove: ⇧⌘N   Up: ⌘↑   Down: ⌘

ID    URL                                             Client      Me
2318  https://b.applovin.com/shopify/v2/pixel        127.0.0.1   POS
2988  https://b.applovin.com/shopify/v2/pixel        127.0.0.1   POS
3026  https://b.applovin.com/shopify/v2/pixel        127.0.0.1   POS
1865  https://b.applovin.com/v1/pixel                127.0.0.1   POS
1881  https://b.applovin.com/v1/pixel                127.0.0.1   POS

POST   200 OK   https://b.applovin.com/shopify/v2/pixel

Request  Header  Query  Body  Raw  Summary  +
6d5[redacted]                                   Done

POST /shopify/v2/pixel HTTP/1.1
Host: b.applovin.com
Accept: */*
Sec-Fetch-Site: cross-site
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Sec-Fetch-Mode: no-cors
Accept-Encoding: gzip, deflate, br
Origin: https://store.happymammoth.com
Content-Length: 4720
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML,
like Gecko) CriOS/[redacted] Mobile/15E148 Safari/604.1
Referer: https://store.happymammoth.com/
Connection: keep-alive
Content-Type: text/plain;charset=UTF-8
Sec-Fetch-Dest: empty

{"applovin":{"connectEventKey":"[redacted]
"wrt":"[redacted]","wrtOrigin":1,"wrt3p":"[redacted]
[redacted]","sid":"[redacted]
[redacted]","eventId":"[redacted]                                  ","art":"6d5[redacted]
[redacted]","version":"s/3.6.5","pixelTimings":
{"pixelLoadMs":[redacted],"pixelNetworkMs":[redacted]'pixelRequestDelayMs":[redacted],"pageTimings":null,"visitInfo":
{"firstVisitTs":[redacted],"lastVisitTs":null,"visitCount":1,"currentVisitStartTs"[redacted]},"ev
ent":{"id":"[redacted]","name":"land","data":
{},"type":"standard","clientId":"[redacted]","timestamp":"[redacted]
[redacted]","context":{"document":{"location":{"href":"https://store.happymammoth.com/pages/
hormonal-weight-assist?
utm_source=applovin&utm_campaign=HappyMammoth_ROAS&utm_medium=paid&utm_term=Video_Portr
alt_Long_3PPlayableEndcard_TSx1.3.J1v3_HM_9x16_LP-hormonal-weight-
assist_happymammoth_sparkmip_vs-pdp-cr-hormone-
harmony_01_en_play_al_all%2Bcatalog&tw_source=applovin&tw_campaign=
```

Advertiser: Happy Mammoth
website: store.happymammoth.com

art value: 6d5…

APP’s Unauthorized Use of PIG Data Gives It A Black Edge in Ad Auctions

APP’s Unauthorized Use of PIG Data Gives it a Black Edge in Ad Auctions

APP’s impermissibly collected 3P user data enables it to gain attribution for last clicks by telling it when to bid aggressively in ad auctions. Most industry standard Mobile Measurement Partners (MMPs), the ad auction referees, use a “last click” attribution model: the last ad shown before purchase gets full credit.

Because of the persistence of the 3P and Shopify event data, APP knows which users have recently abandoned their shopping carts. These users have a high probability of completing their purchases if retargeted by ads, particularly when the ad shows the brand or product presently in the user’s cart. Even if APP loses an initial bid (often against META or Google), if the item is still in the cart, APP can try to win the next auction.

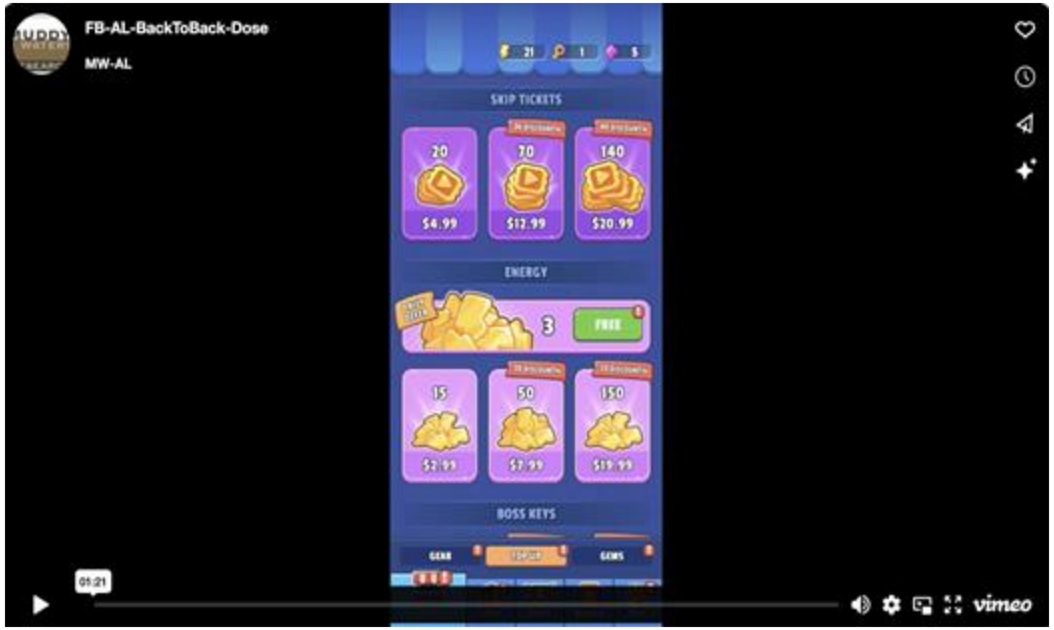
During our research, we repeatedly experienced “carpet bombing” of retargeted ads served dozens of times by APP in a single day after we had placed items from those advertisers in our carts.

We hypothesize that APP blends these high probability ad wins with low probability, low-cost ads to create the appearance of a high ROAS advertising platform while generating a high margin for APP.

Example: APP's Black Edge in Ad Auctions Increases Competition for 1P User Data Ad Networks

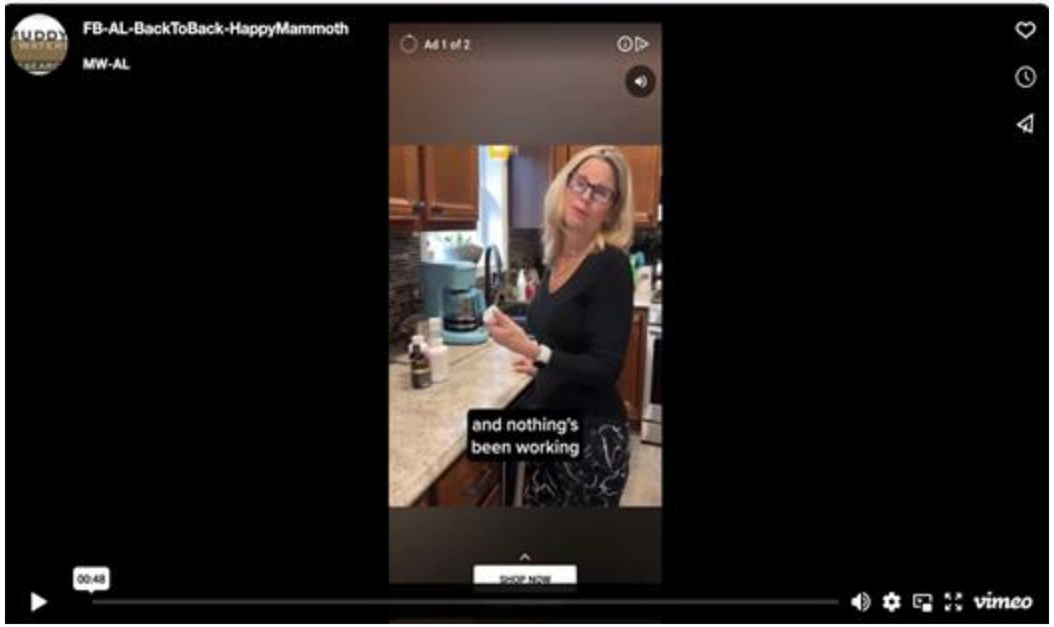
We repeatedly observed Facebook and APP ads for the same advertiser running back-to-back. This appears to reflect a bidding war between APP and Facebook, which seemingly place similar values on the user but should have vastly different amounts of data. APP doesn't overcome the information asymmetry through "AI", but rather through misappropriated 3P user data.

1st ad served: Dose for your liver ad by APP,
2nd ad served: another Dose ad by Facebook



https://www.youtube.com/watch?v=7tu7VlTNREY

1st ad served: a Happy Mammoth Ad by Facebook,
2nd ad served: another Happy Mammoth ad by APP



https://www.youtube.com/watch?v=ac8QL7dXMGA

App's Management Actively Misleads Both Investors and Customers

A Sample of APP’s Misleading Claims

APP is driving incremental sales: APP is driving real users who really click the ads and actually buy products. Some of the sales probably are incremental to the ad networks driving the original traffic. APP’s ads just aren’t the original source of most so-called incremental sales; rather it’s mainly claim jumping, taking the last click attribution credit. And to the extent these are retargeting sales, the value is further diminished.

APP has ad targeting and optimization: Likely it does to some degree. It’s just optimizing to show users ads right before users purchase to win credit for a sales it didn’t actually or solely generate.

APP’s doesn’t use PII: APP produces its PIGs from its partners’ unique IDs, synthetically building user profiles without having to touch PII directly. But, through this combination, these profiles effectively become a form of PII.

APP doesn’t specifically target Meta: APP’s PIGs aren’t specific to Meta. They include data from numerous platforms.

Materiality of Issues to APP's Business

Possible Consequences Range from Client Abandonment to Deplatforming

We believe that APP is at real risk of deplatforming. We understand that platforms' TOS prohibit fingerprinting without consent because the platforms are concerned about being to honor user opt-outs and deletion requests as required by various laws.

However, should the platforms not act against APP, we expect that APP will face significant competition because these techniques, if seemingly tolerated by the platforms, should be easy to duplicate. The key matching technology involved in APP's e-commerce business appears to lack a moat.

Putting aside the probability of margin-eroding competition should the platforms tolerate APP's approach, given the core of its product appears to be retargeting and has low apparent incrementality, we doubt many advertisers will countenance paying a premium for APP.

Appendix

Cheetah Mobile’s Click Injection Fraud Leads to Ban from Google & Meta – Share Price Collapses in Stages

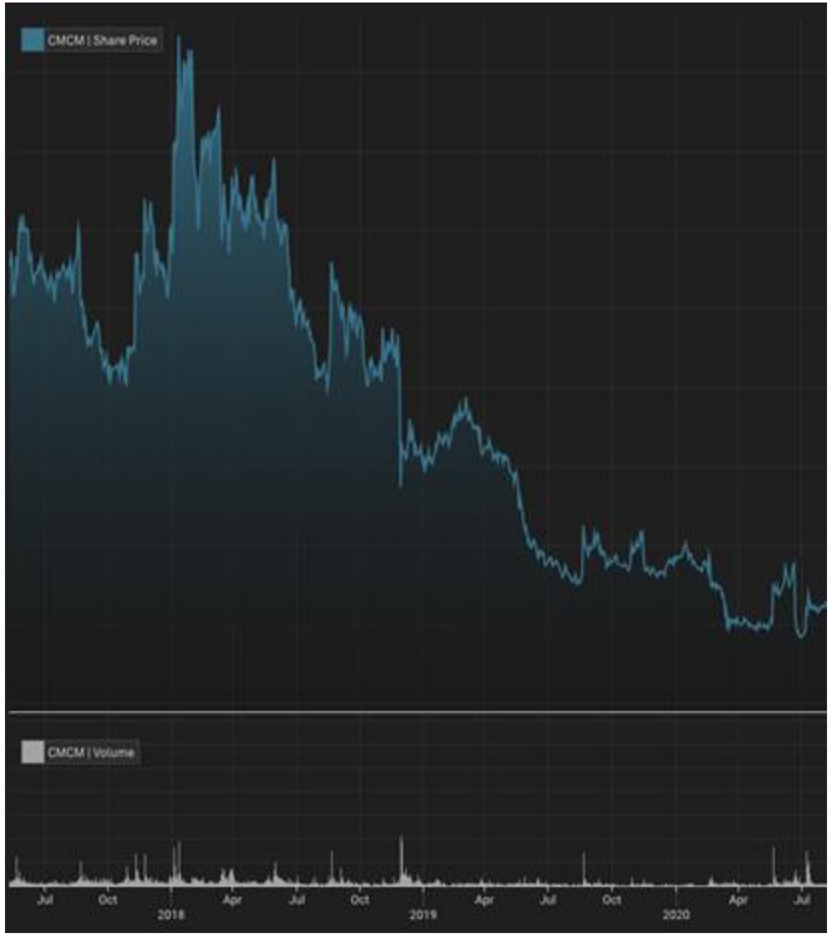
Cheetah Mobile was engaged in a "click injection" scheme to fraudulently claim referral bonuses from ad networks like Google and Facebook. A November 2018 BuzzFeed investigation reported the scheme citing findings from the analytics firm Kochava.[1] This investigation was spurred by a short seller investigation.[2]

The “Click Injection” scheme: Seven Cheetah apps injected fake clicks to falsely attribute organic downloads and collect unearned "install bounties.” Cheetah denied responsibility blaming third-party SDKs, but evidence showed the fraud was tied to its proprietary code. A cybersecurity research found four Cheetah apps had been “collecting all manner of private user data, including users’ browsing history, search engine queries, and Wi-Fi access point names.” Google and Meta were apparently unaware for years.[1,3,4,5,6]

Misleading Disclosures: Like, APP, the company made technically truthful but deceptive statements about revenue sources and app functionality, omitting risks posed by the click fraud scheme.[7]

Impact: Google and Facebook severed ties crippling Cheetah’s ad-driven revenue model.[3] Shares plummeted in stages from a high of $76 in Jan 2018 to $9 at YE 2020. Cheetah never recovered. CMCM currently trades at ~$5.

Below: Cheetah’s share price collapse, -87% from peak in Jan ‘18 to YE ‘20.



Source: CapIQ

[1] https://www.buzzfeednews.com/article/craigsilverman/android-apps-cheetah-mobile-kika-kochava-ad-fraud

[2] https://www.presciencepoint.com/research/research-archives/cheetah_mobile-cmcm/

[3] https://technode.com/2020/03/26/whats-to-blame-for-cheetah-mobile-downfall/

[4] https://www.androidpolice.com/2020/02/27/cheetah-mobile-apps-disappeared-play-store/

[5] https://www.forbes.com/sites/thomasbrewster/2020/03/03/warning-an-android-security-app-with-1-billion-downloads-is-recording-users-web-browsing/#6378cb5f2149

[6] https://lawprofessors.typepad.com/business_law/2020/07/rumpelstiltskin-and-the-securities-laws.html

Facebook (Meta) Embargoed Zynga, FarmVille Suffers a Drought – Share Price Falls 84%

Zynga's rise and its 2011 IPO was fueled by an online gaming app launched in Facebook (FB), tapping into FB's huge userbase, selling virtual goods and flooding FB's platform with endless streams of message requests, and most problematically for FB, driving traffic away from its platform to its Zynga's non-Facebook games.[1,2]

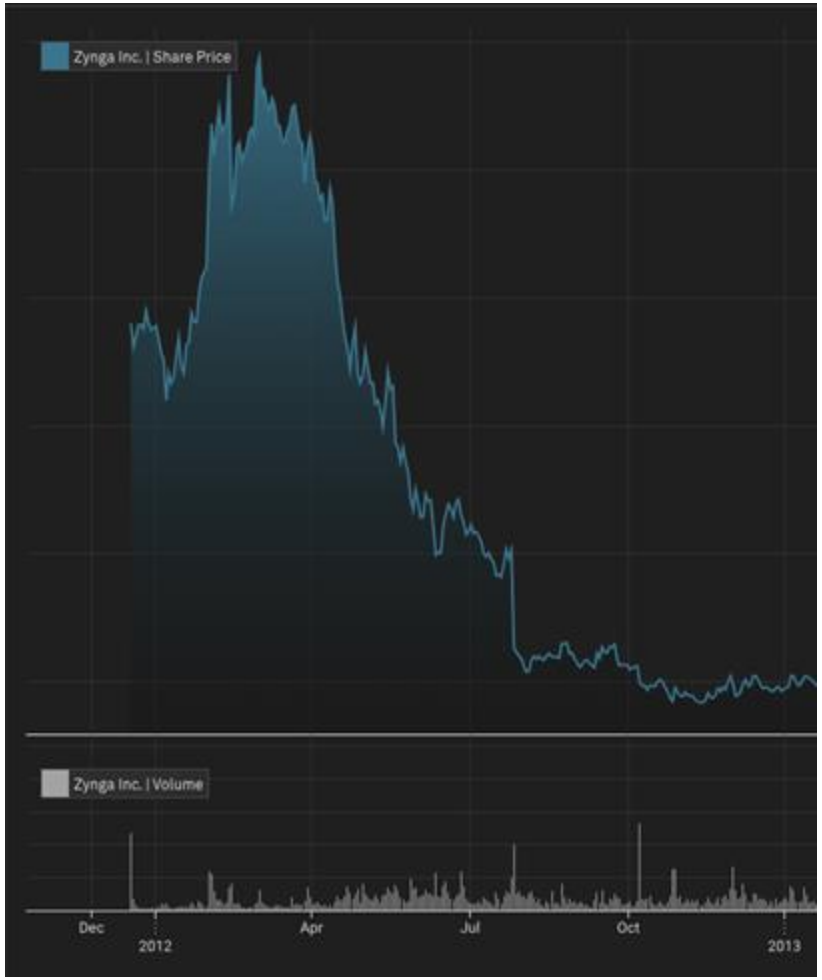
Zynga's reliance on FB proved to be a vulnerability. In 2012, Facebook changed its terms of service (TOS). This change was not due to a TOS violation but intended to eliminate an upstart who was siphoning off traffic and revenues.

Facebook embargoed Zynga from preferential treatments associated with its special relationship, turned off notifications, cross-promotions, viral calls, and eventually in 2013 algorithmically deprioritized games by moving them to a separate "Games Feed", all of which hamstrung Zynga and contributed to it's share price collapse and sustained low valuation.

In July 2012 Zynga posted disappointing earnings, blaming "a faster decline in existing Web games due in part to a more challenging environment on the Facebook Web platform." Zynga's shares immediately fell 41%. By year end 2012, Zynga's shares had collapsed from its peak of $14.75 in on March 2, 2012 to just $2.36 at the Dec 31, 2012.[1,2,3,4]

Impact: APP also enjoys special status as a Facebook ad mediation platform. Our tech team found that APP has jumping in to hijack ad attribution – including from Meta - and been making extensive use of Meta's user identifiers to do so. As Meta did with Zynga, Meta could change its TOS, its code, or both, and APP would be embargoed from its key (albeit improperly obtained) user data as well as ad revenue from Meta ads. We believe the impact would, again, be enormous.

Below: Zynga's 2012 Share price collapse, 84% fall from peak to year end



Source: CapIQ (Note: Zynga was taken over by TTWO in 2022)

[1] https://toppandigital.com/us/blog-usa/rise-fall-zynga-cautionary-tale-game-developers/

[2] https://lloydmelnick.com/2012/11/30/what-does-the-change-in-zyngas-agreement-with-facebook-mean-to-other-game-companies/

[3] https://www.gamesindustry.biz/zynga-no-longer-leashed-to-facebook

[4] https://www.latimes.com/business/la-xpm-2012-jul-25-la-fi-ct-zynga-nintendo-earnings-20120726-story.html

Churn Verification – Automated Tools & Manual Checks Deployed for Pixel Hunting

Analysts utilized both automated scanning technologies and manual checks to ascertain which websites retained the presence of the Axon and/or APP-specific tracking pixels.

URLScan.io was used in the final pass, which provides a publicly accessible, and verifiable source for all of the tests. URLScan.io uses a full browser to browse to the target website, and then monitor that browser for all HTTP requests, cookies, console (error or logging messages) information along with statistics for each domain that was contacted. After the automated scan, the churn list was double checked by means of manual inspection utilizing Chrome DevTools.

To determine whether the AXON/APP system was present, analysts tested for the "axcrt" AXON cookie being present, various page-specific global variables that the AXON tracking pixel sets, and for the presence of HTTP communication between the URLScan.iobrowser and axon.ai [axon.ai] and/or b.applovin.com [applovin.com].

Criteria:

- The presence of *any one* of these criteria would be judged as an *active website*, i.e. NOT churned.*
- If none of the above criteria was present in the URLScan data, then the website was considered to have churned.

This assumes that the ecommerce customer is using the AXON data meaningfully and does not take into account e-commerce websites that may have incorrectly configured the AXON/APP pixels. Incorrectly configured websites which are not functioning properly which do present an APP pixel will be deemed to have NOT churned. This is considered a company-favorable methodology.

APP associates the Shopify_y cookie with the wrt prefix

In APP's code, a shopify event (such as the shopify_y cookie) is an essential element.

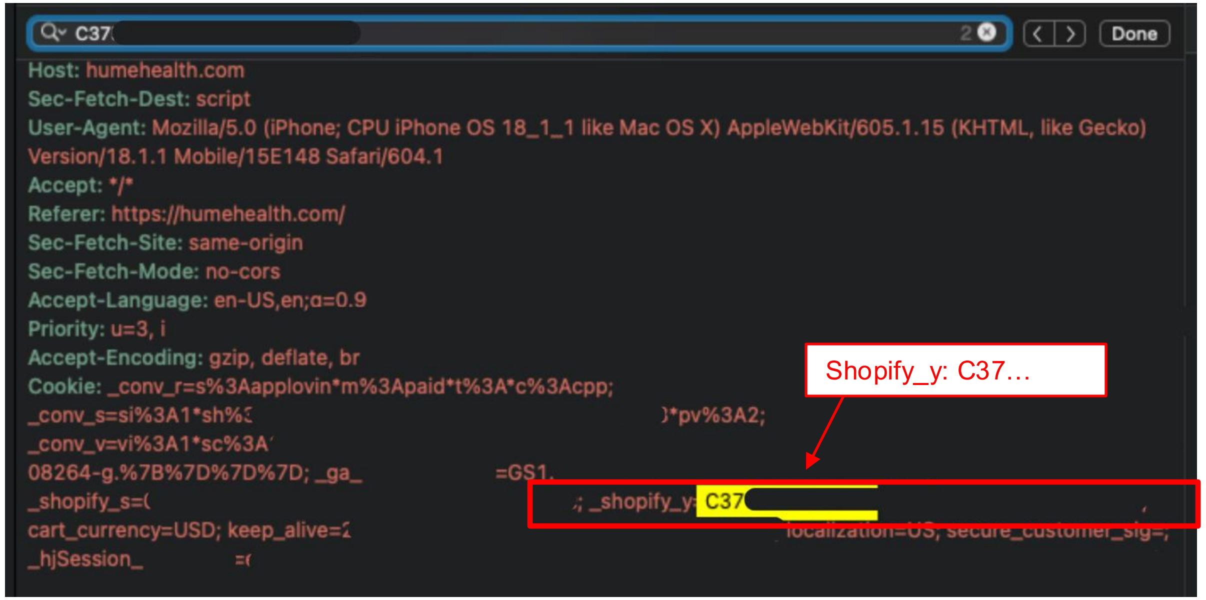
The shopify_y cookie is a particularly useful data point to collect because it is a persistent identifier with a duration of 1 year.

Its value is normally presented with the "_wrt" or "_wrt3p" prefix.

The image at the upper right is from Shopify and shows the Shopify_y cookie value: C37…

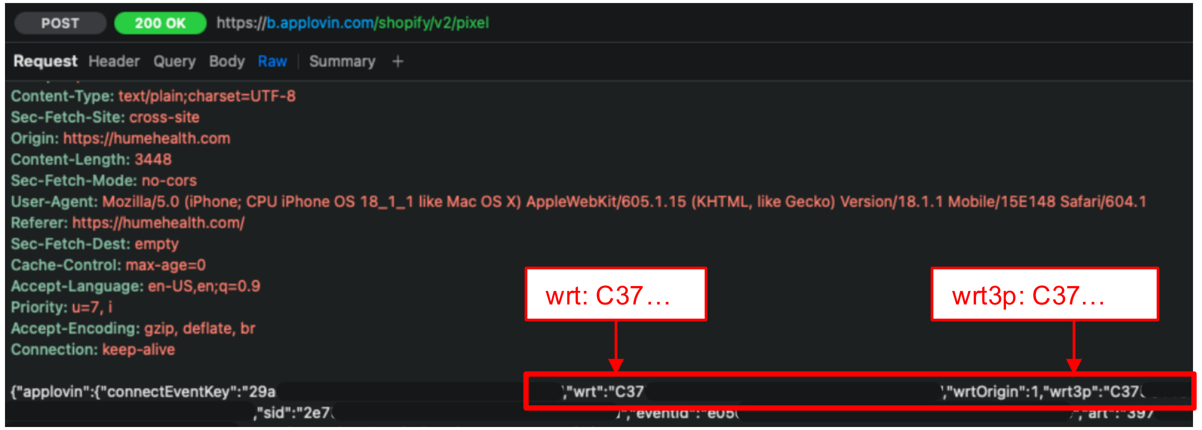
The image at the lower right is from Approving and shows the Shopify_y cookie value with the wrt and the wrt3p prefix C37…

Note: to protect the originators PII only the initial characters in the full sting value are shown. The rest have been redacted.



```
Host: humehealth.com
Sec-Fetch-Dest: script
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/18.1.1 Mobile/15E148 Safari/604.1
Accept: */*
Referer: https://humehealth.com/
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Accept-Language: en-US,en;q=0.9
Priority: u=3, i
Accept-Encoding: gzip, deflate, br
Cookie: _conv_r=s%3Aapplovin*m%3Apaid*t%3A*c%3Acpp;
_conv_s=si%3A1*sh%3 [redacted] )*pv%3A2;
_conv_v=vi%3A1*sc%3A [redacted]
08264-g.%7B%7D%7D%7D; _ga_ [redacted] =GS1. [redacted]
_shopify_s=( [redacted] ; _shopify_y: C37 [redacted]
cart_currency=USD; keep_alive=2 [redacted] localization=US; secure_customer_sig=;
_hjSession_ [redacted] =( [redacted]
```

Shopify_y: C37…



```
https://b.applovin.com/shopify/v2/pixel
Content-Type: text/plain;charset=UTF-8
Sec-Fetch-Site: cross-site
Origin: https://humehealth.com
Content-Length: 3448
Sec-Fetch-Mode: no-cors
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.1.1 Mobile/15E148 Safari/604.1
Referer: https://humehealth.com/
Sec-Fetch-Dest: empty
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Priority: u=7, i
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{"applovin":{"connectEventKey":"29a [redacted] ","wrt":"C37 [redacted] ","wrtOrigin":1,"wrt3p":"C37 [redacted]
,"sid":"2e7 [redacted] ","eventId":"e05 [redacted] ","art":"397
```

wrt: C37…

wrt3p: C37…

Technical Explanation of How PIGing Gives APP Black Edge

Based on our research and understanding of the ad behavior and code, we outline the ad rigging process:

- Trigger: A user goes to an e-commerce site that has the pixel installed, takes a triggering action such as adding an item to a cart and beginning a purchase process, then pauses leaving items stranded in the cart (which is extremely common).
- Data Theft: Pixels often ingest three distinct types of data: a third-party ID such as (Google, Meta, Tiktok, Snap, etc.) or other data such as link UTMs,[1] and other Shopify settings labeling them as a "key". A Shopify event items such as its "Y Cookie", purchase token, checkout token, etc. are labeling as "wrt" or "wrt3p" and finally associated with APP's hidden Compass Tokens (CT). The CT is used in the Ad mediation and Ad auction process.
- Obfuscation: Multiple pixels mask tracking; IDs are linked between pixels via an event ID (the "connectEventKey") before being sent to APP's servers.
- Persistent Identity Graph (PIG): APP's algorithm ingests and stitches together user IDs and users' data to create the PIG ID. By associating multiple 3rd party IDs with behavioral signals from Shopify and its own Compass Token, along with the typical fingerprinting data such as location, telemetry, hardware information, etc. APP has functionally de-anonymized these anonymous IDs and built a profile of a user without technically directly using PII (Personally Identify Information); instead, APP is building a synthetic representation of that user, the PIG.
- APP's Max Auction: The in-app ad auction wherein an app calls up for an ad and a competitive auction is held. The APP network installed CT is called on. The algorithm uses the PIG data, estimates a user's value, and delivers a bid via the CT to the MAX Mediation auction.
- Targeting/Retargeting: After identifying the highest value users, APP bids aggressively, and when victorious aggressively shows ads for the product the user was just looking at, often dozens of times a day.
- Tracking: If the user clicks an ad for that product, the exact same value of the CT is relabeled as "alart" and added to the URL. The user is identified and tracked across web e-commerce sites and also across mobile games, which we believe is a violation of privacy TOS.
- Coming full circle: The process begins again however with "alart" value taken from the URL and is relabeled for a 3rd time as the "art" value.
- This PIG tech is unprecedented for ads—but it isn't unprecedented for AI models where synthetic data is often utilized to train models.
- The end result is APP uses the PIG ID to win auctions and win a number of clicks for users that were already poised to purchase.

A set of diagrams mapping this process are in Appendix.

[1] UTMs (Urchin Tracking Modules) are custom tags that can be added to a URL. They provide additional information to analytics tools like Google Analytics, and provide an understanding of traffic sources. When a URL with UTM parameter is clicked, the tags are sent back to the analytics tool which then logs data about the visitor and their behavior. admetrics.io/en/post/utm-parameters-for-ad-tracking
[2] The CTs were found by our team when searching "the shared plist file" stored locally in the gaming apps and on the device.

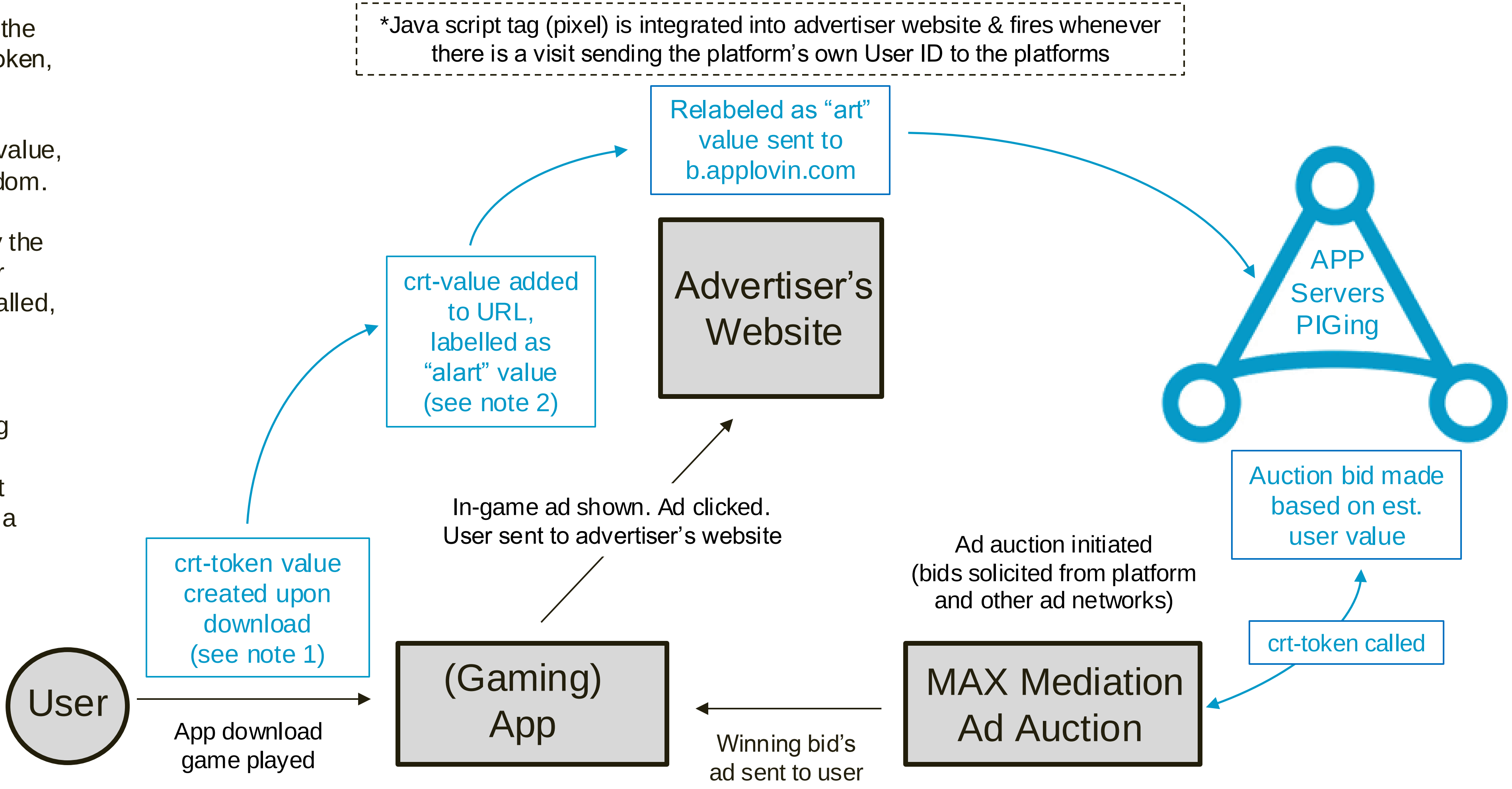
Fingerprinting Machine Step 1 - APP's Tokens Movements Are Relabeled and Transfer Data

This diagram shows the movement of the "compas_random_token", the "alart" token, and "art".

These tokens are given an persistent value, a string of numbers which are not random.

These persistent values are carried by the tokens from stage to stage as the user engages with the game and ads are called, ad auctions run, and ads shown.

Notes:
1. A bid token should not leave bidding environment.
2. The alart should not be persistent. It should be unique each time, not carry a repeating value.



*Java script tag (pixel) is integrated into advertiser website & fires whenever there is a visit sending the platform's own User ID to the platforms

User
App download
game played
crt-token value created upon download (see note 1)
(Gaming) App
crt-value added to URL, labelled as "alart" value (see note 2)
Relabeled as "art" value sent to b.applovin.com
Advertiser's Website
In-game ad shown. Ad clicked. User sent to advertiser's website
APP Servers PIGing
Auction bid made based on est. user value
crt-token called
Ad auction initiated (bids solicited from platform and other ad networks)
MAX Mediation Ad Auction
Winning bid's ad sent to user

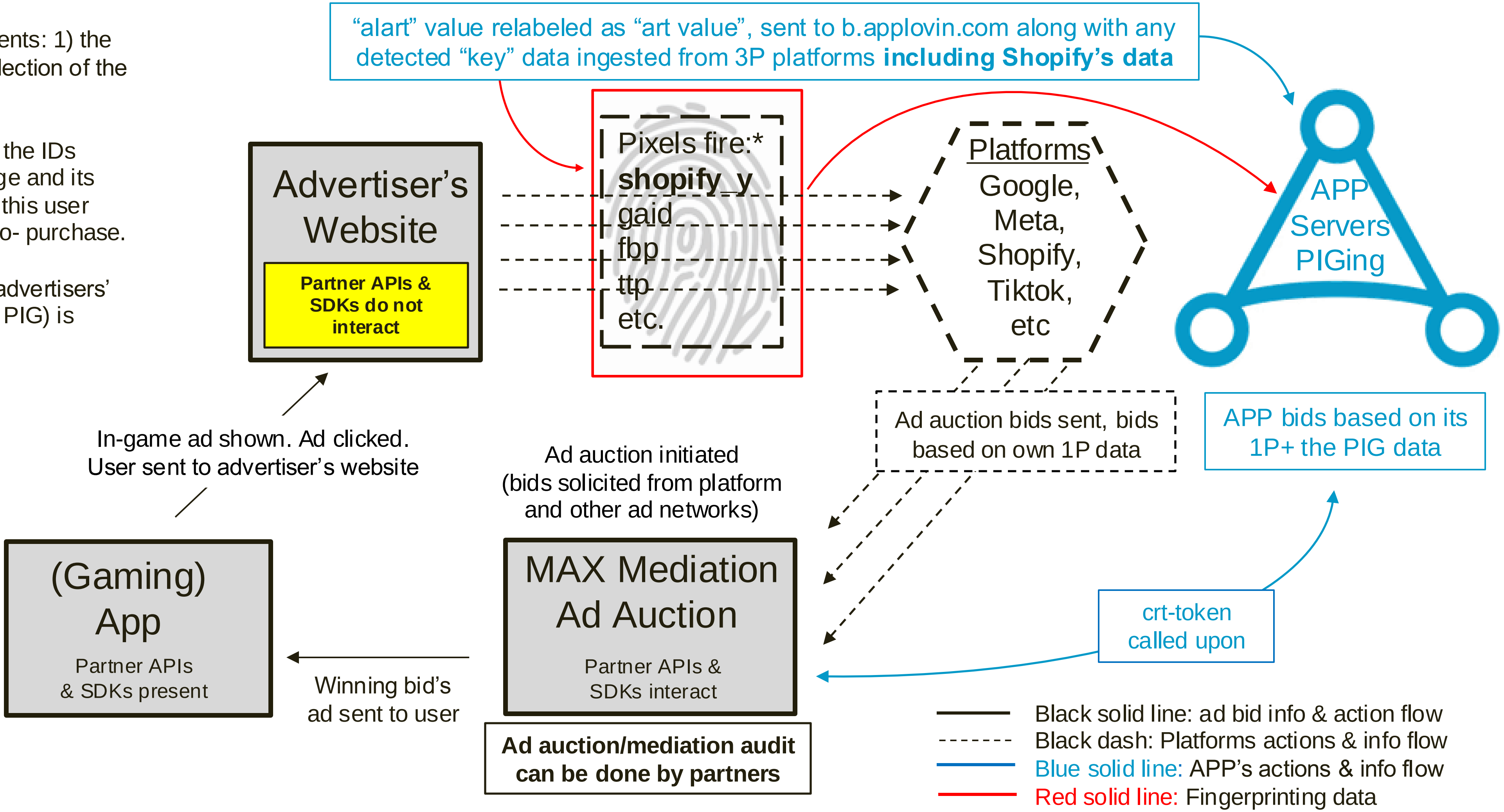
APP’s Fingerprinting Machine Step 2 – Ingesting “Key” Data To Inform APP’s Bid

This diagram adds two significant components: 1) the 3P platforms pixels/data, and 2) APP’s collection of the same data.

APP sidesteps the typical flow by stitching the IDs together and leveraging local device storage and its servers to achieve this process of building this user graphs and targets bids for users poised-to- purchase.

APP’s fingerprint signals are collected on advertisers’ websites, while probabilistic matching (the PIG) is on its own servers outside the controlled environments where Apple, Google, and Meta enforce detection policies, bypassing their ability to monitor cross-platform tracking.

Platforms could do the same, but their own TOS prohibits monitoring other networks’ activities.



“alart” value relabeled as “art value”, sent to b.applovin.com along with any detected “key” data ingested from 3P platforms **including Shopify’s data**

Advertiser’s Website

Partner APIs & SDKs do not interact

Pixels fire:*
shopify_y
gaid
fbp
ttp
etc.

Platforms
Google,
Meta,
Shopify,
Tiktok,
etc

APP Servers PIGing

Ad auction bids sent, bids based on own 1P data

APP bids based on its 1P+ the PIG data

In-game ad shown. Ad clicked. User sent to advertiser’s website

Ad auction initiated (bids solicited from platform and other ad networks)

crt-token called upon

(Gaming) App

Partner APIs & SDKs present

Winning bid’s ad sent to user

MAX Mediation Ad Auction

Partner APIs & SDKs interact

Ad auction/mediation audit can be done by partners

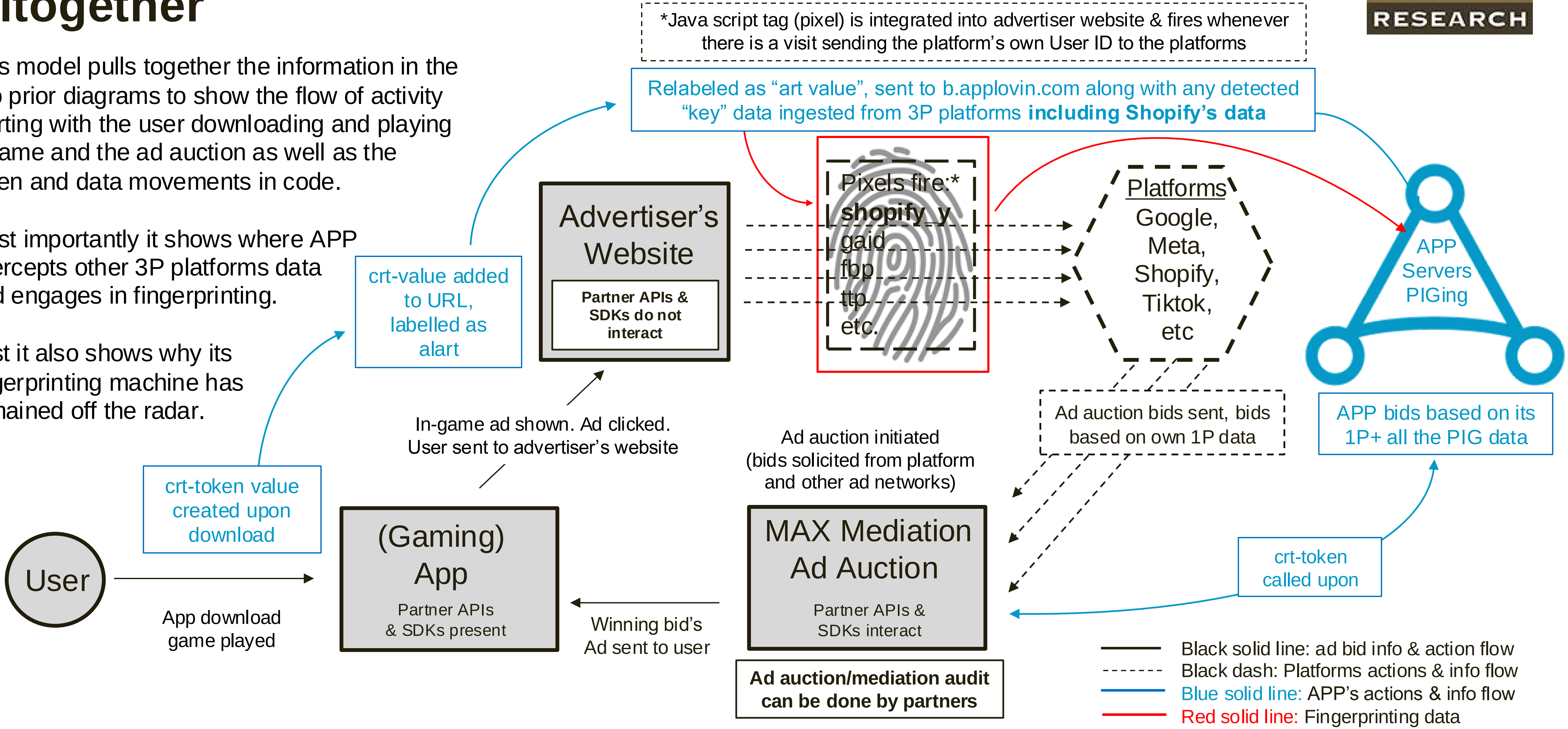
Black solid line: ad bid info & action flow
Black dash: Platforms actions & info flow
Blue solid line: APP’s actions & info flow
Red solid line: Fingerprinting data

APP's Fingerprinting Machine – Step 3: Pulling it Altogether

This model pulls together the information in the two prior diagrams to show the flow of activity starting with the user downloading and playing a game and the ad auction as well as the token and data movements in code.

Most importantly it shows where APP intercepts other 3P platforms data and engages in fingerprinting.

Last it also shows why its fingerprinting machine has remained off the radar.



*Java script tag (pixel) is integrated into advertiser website & fires whenever there is a visit sending the platform's own User ID to the platforms

Relabeled as "art value", sent to b.applovin.com along with any detected "key" data ingested from 3P platforms **including Shopify's data**

Advertiser's Website

Partner APIs & SDKs do not interact

Pixels fire:*
shopify_y
gaid
fbp
ttp
etc.

Platforms
Google, Meta, Shopify, Tiktok, etc

APP Servers PIGing

crt-value added to URL, labelled as alart

In-game ad shown. Ad clicked. User sent to advertiser's website

Ad auction initiated (bids solicited from platform and other ad networks)

Ad auction bids sent, bids based on own 1P data

APP bids based on its 1P+ all the PIG data

crt-token value created upon download

User

App download game played

(Gaming) App

Partner APIs & SDKs present

Winning bid's Ad sent to user

MAX Mediation Ad Auction

Partner APIs & SDKs interact

Ad auction/mediation audit can be done by partners

crt-token called upon

Black solid line: ad bid info & action flow
Black dash: Platforms actions & info flow
Blue solid line: APP's actions & info flow
Red solid line: Fingerprinting data

Guide to Desktop Checking on Fingerprinting

To see how APP collects identities fingerprints to create its PIGs follow the steps below (best results in US).[1]

Note: This process is to be carried out on a laptop (widows or Mac). An accompanying guide with screen shots is provided in the Appendix.[2]

1. Go to one of APP's customer websites, e.g.: trueclassictees.com
2. Right-click → select "Inspect" to open "Chrome DevTools"
3. Add any item to cart, then click "Checkout"
4. In DevTools, go to the "Network" tab
5. In the search bar, type: b.applovin.com
6. Click the top successfully loaded requests in the list. Successful requests are denoted as {:} pixel.
7. Go to the "Payload" tab, then → Expand initData (open the arrow) → select "cart" → select "attributes"
8. Look for entries with a "key" and "value" structure*

What "keys" are being collected will vary from user to user, but there will most likely be a 3 to 10 key items being collected.

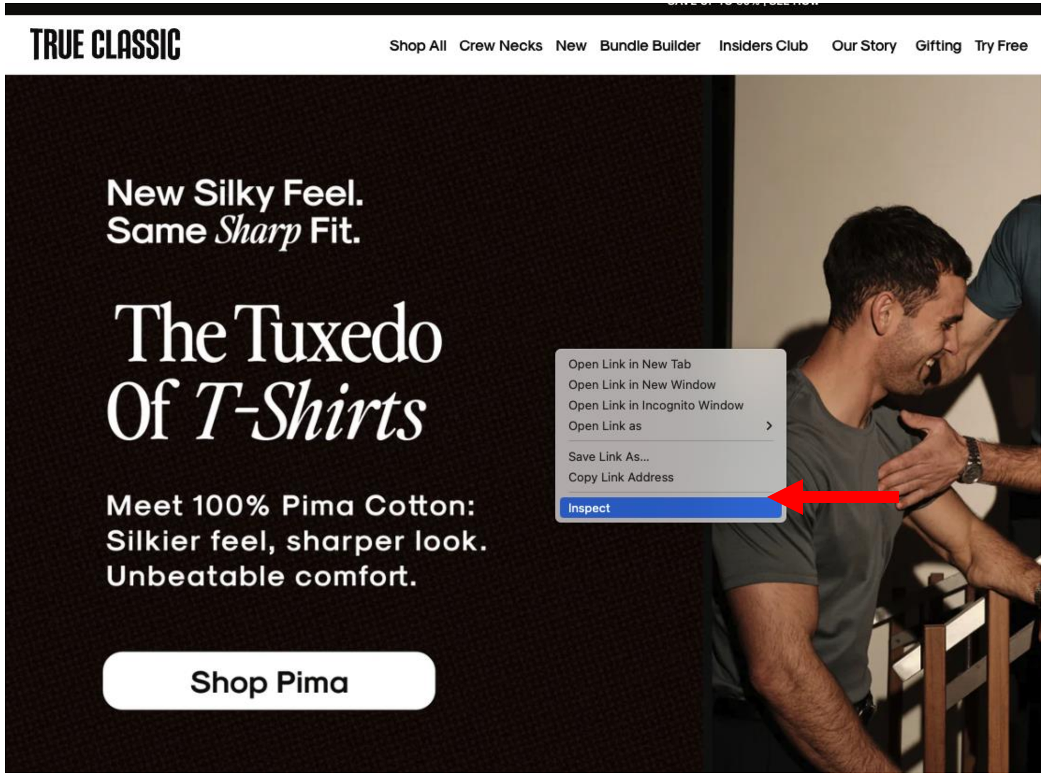
In this case, the following key data is picked up. Note "fondue cart" and "novel" are shopify plug ins as tracking an ApplePay signal.

- `{key: "igId", value: "ig_e86b73aa40d1933de4328f62a3b026983ada"},…]`
- `{key: "__fondue_cart_id", value: "314dd843-315a-4246-9343-c7ce5d3dc204-1743090589588"}`
- `{key: "novel_min_balance", value: "0"}`
- `{key: "GE_isApplePay", value: "false"}`

See: https://www.youtube.com/watch?v=g4DJArXAGTA

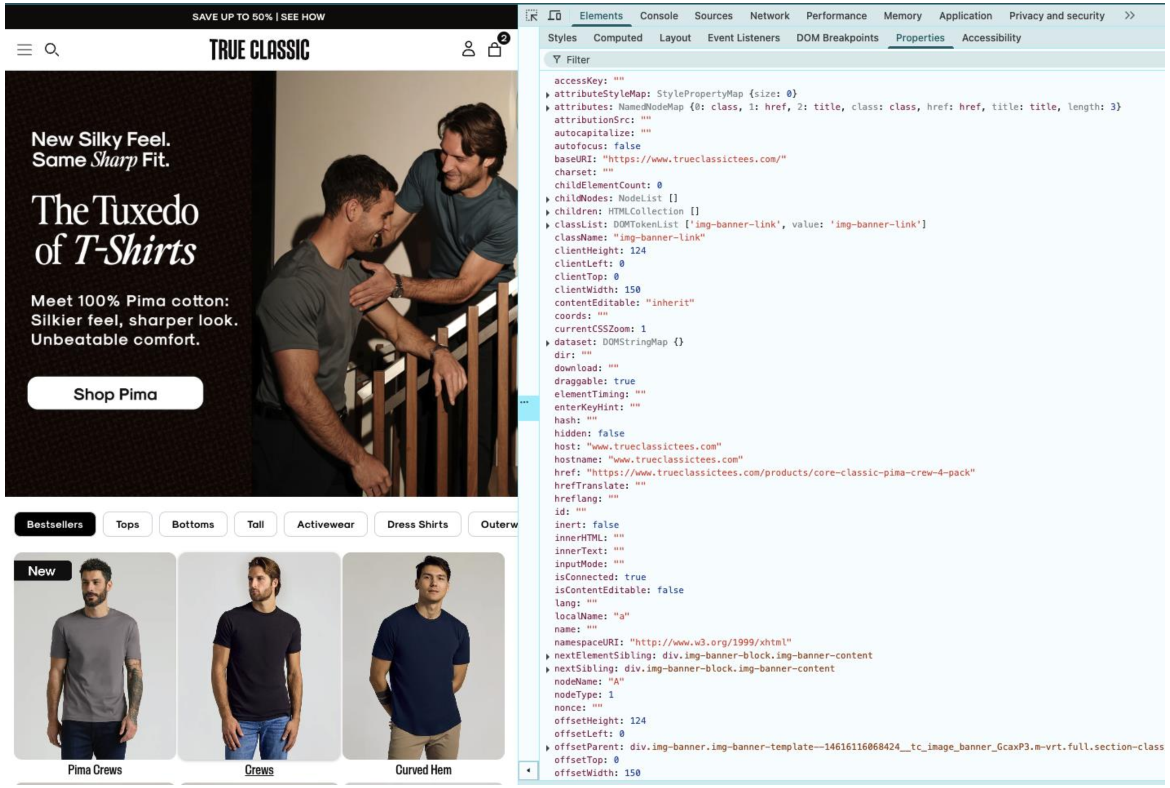
Guide to Desktop Checking on Fingerprinting

1. Go to one of APP’s customer websites, e.g.: trueclassictees.com



2. Right-click → select “Inspect” to open “Chrome DevTools”

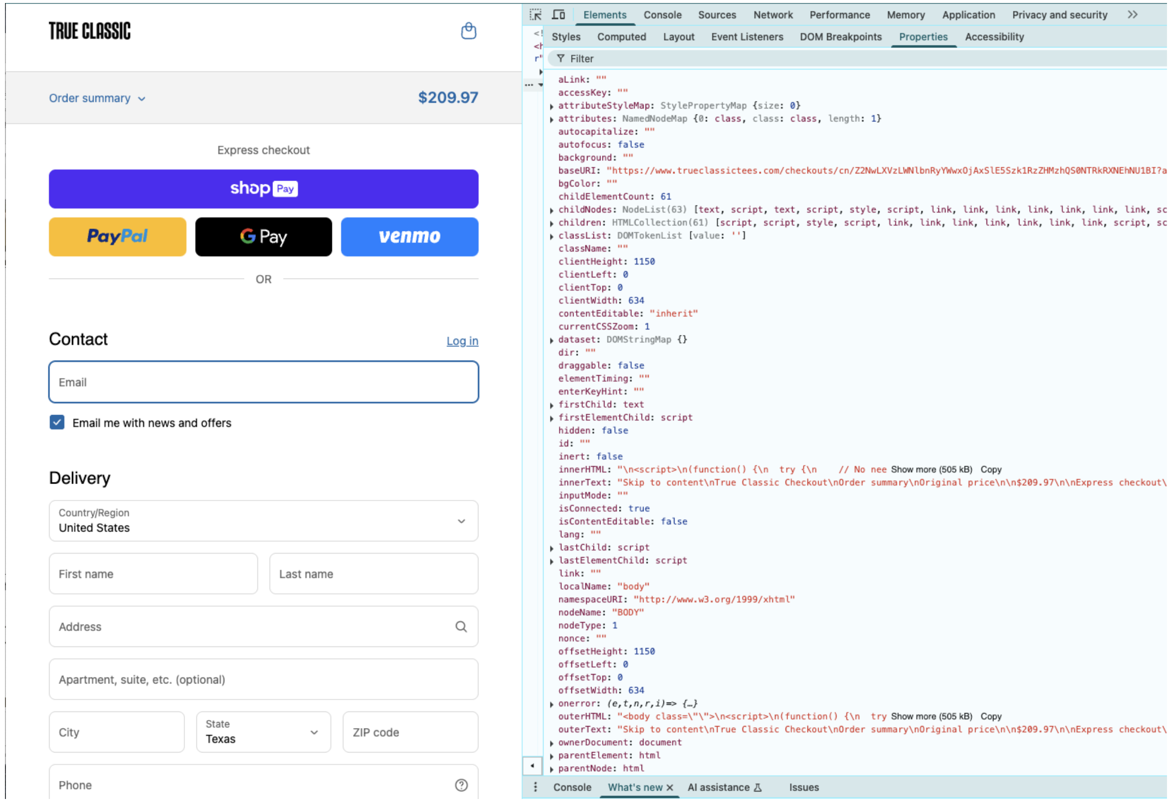
Image below shows Dev Tools after being opened



```
  accessKey: ""
▸ attributeStyleMap: StylePropertyMap {size: 0}
▸ attributes: NamedNodeMap {0: class, 1: href, 2: title, class: class, href: href, title: title, length: 3}
  attributionSrc: ""
  autocapitalize: ""
  autofocus: false
  baseURI: "https://www.trueclassictees.com/"
  charset: ""
  childElementCount: 0
▸ childNodes: NodeList []
▸ children: HTMLCollection []
▸ classList: DOMTokenList ['img-banner-link', value: 'img-banner-link']
  className: "img-banner-link"
  clientHeight: 124
  clientLeft: 0
  clientTop: 0
  clientWidth: 150
  contentEditable: "inherit"
  coords: ""
  currentCSSZoom: 1
▸ dataset: DOMStringMap {}
  dir: ""
  download: ""
  draggable: true
  elementTiming: ""
  enterKeyHint: ""
  hash: ""
  hidden: false
  host: "www.trueclassictees.com"
  hostname: "www.trueclassictees.com"
  href: "https://www.trueclassictees.com/products/core-classic-pima-crew-4-pack"
  hrefTranslate: ""
  hreflang: ""
  id: ""
  inert: false
  innerHTML: ""
  innerText: ""
  inputMode: ""
  isConnected: true
  isContentEditable: false
  lang: ""
  localName: "a"
  name: ""
  namespaceURI: "http://www.w3.org/1999/xhtml"
▸ nextElementSibling: div.img-banner-block.img-banner-content
▸ nextSibling: div.img-banner-block.img-banner-content
  nodeName: "A"
  nodeType: 1
  nonce: ""
  offsetHeight: 124
  offsetLeft: 0
▸ offsetParent: div.img-banner.img-banner-template--14616116068424__tc_image_banner_GcaxP3.m-vrt.full.section-class
  offsetTop: 0
  offsetWidth: 150
```

Guide to Desktop Checking on Fingerprinting

3. Add any item to cart, then click “Checkout”



TRUE CLASSIC

Order summary ⌄ $209.97

Express checkout

Contact Log in

Email

☑ Email me with news and offers

Delivery

Country/Region
United States

First name | Last name

Address

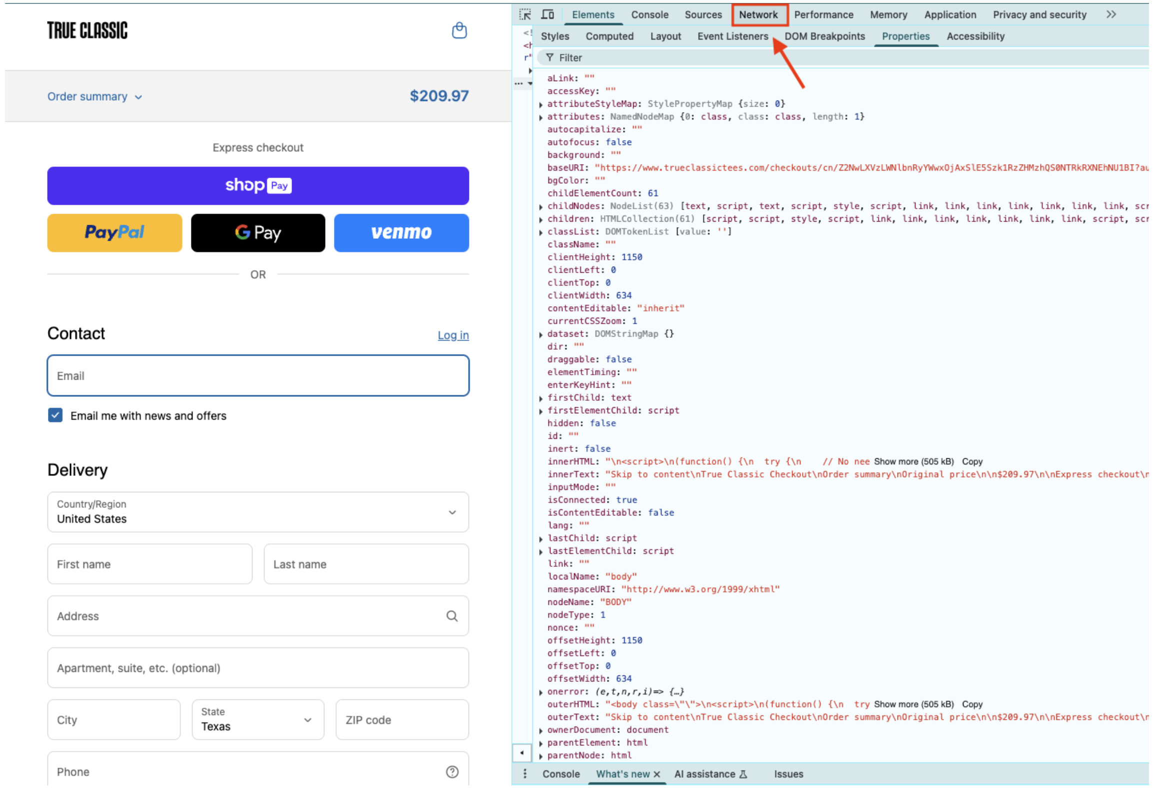
Apartment, suite, etc. (optional)

City | State Texas | ZIP code

Phone

```
  aLink: ""
  accessKey: ""
▸ attributeStyleMap: StylePropertyMap {size: 0}
▸ attributes: NamedNodeMap {0: class, class: class, length: 1}
  autocapitalize: ""
  autofocus: false
  background: ""
  baseURI: "https://www.trueclassictees.com/checkouts/cn/Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI?a
  bgColor: ""
  childElementCount: 61
▸ childNodes: NodeList(63) [text, script, text, script, style, script, link, link, link, link, link, link, link, sc
▸ children: HTMLCollection(61) [script, script, style, script, link, link, link, link, link, link, link, script, sc
▸ classList: DOMTokenList [value: '']
  className: ""
  clientHeight: 1150
  clientLeft: 0
  clientTop: 0
  clientWidth: 634
  contentEditable: "inherit"
  currentCSSZoom: 1
▸ dataset: DOMStringMap {}
  dir: ""
  draggable: false
  elementTiming: ""
  enterKeyHint: ""
▸ firstChild: text
▸ firstElementChild: script
  hidden: false
  id: ""
  inert: false
  innerHTML: "\n<script>\n(function() {\n  try {\n    // No nee Show more (505 kB)  Copy
  innerText: "Skip to content\nTrue Classic Checkout\nOrder summary\nOriginal price\n\n$209.97\n\nExpress checkout\
  inputMode: ""
  isConnected: true
  isContentEditable: false
  lang: ""
▸ lastChild: script
▸ lastElementChild: script
  link: ""
  localName: "body"
  namespaceURI: "http://www.w3.org/1999/xhtml"
  nodeName: "BODY"
  nodeType: 1
  nonce: ""
  offsetHeight: 1150
  offsetLeft: 0
  offsetTop: 0
  offsetWidth: 634
▸ onerror: (e,t,n,r,i)=> {…}
  outerHTML: "<body class=\"\">\n<script>\n(function() {\n  try Show more (505 kB)  Copy
  outerText: "Skip to content\nTrue Classic Checkout\nOrder summary\nOriginal price\n\n$209.97\n\nExpress checkout\
▸ ownerDocument: document
▸ parentElement: html
▸ parentNode: html
```

4. In DevTools, go to the “Network” tab



TRUE CLASSIC

Order summary ⌄ $209.97

Express checkout

Contact Log in

Email

☑ Email me with news and offers

Delivery

Country/Region
United States

First name | Last name

Address

Apartment, suite, etc. (optional)

City | State Texas | ZIP code

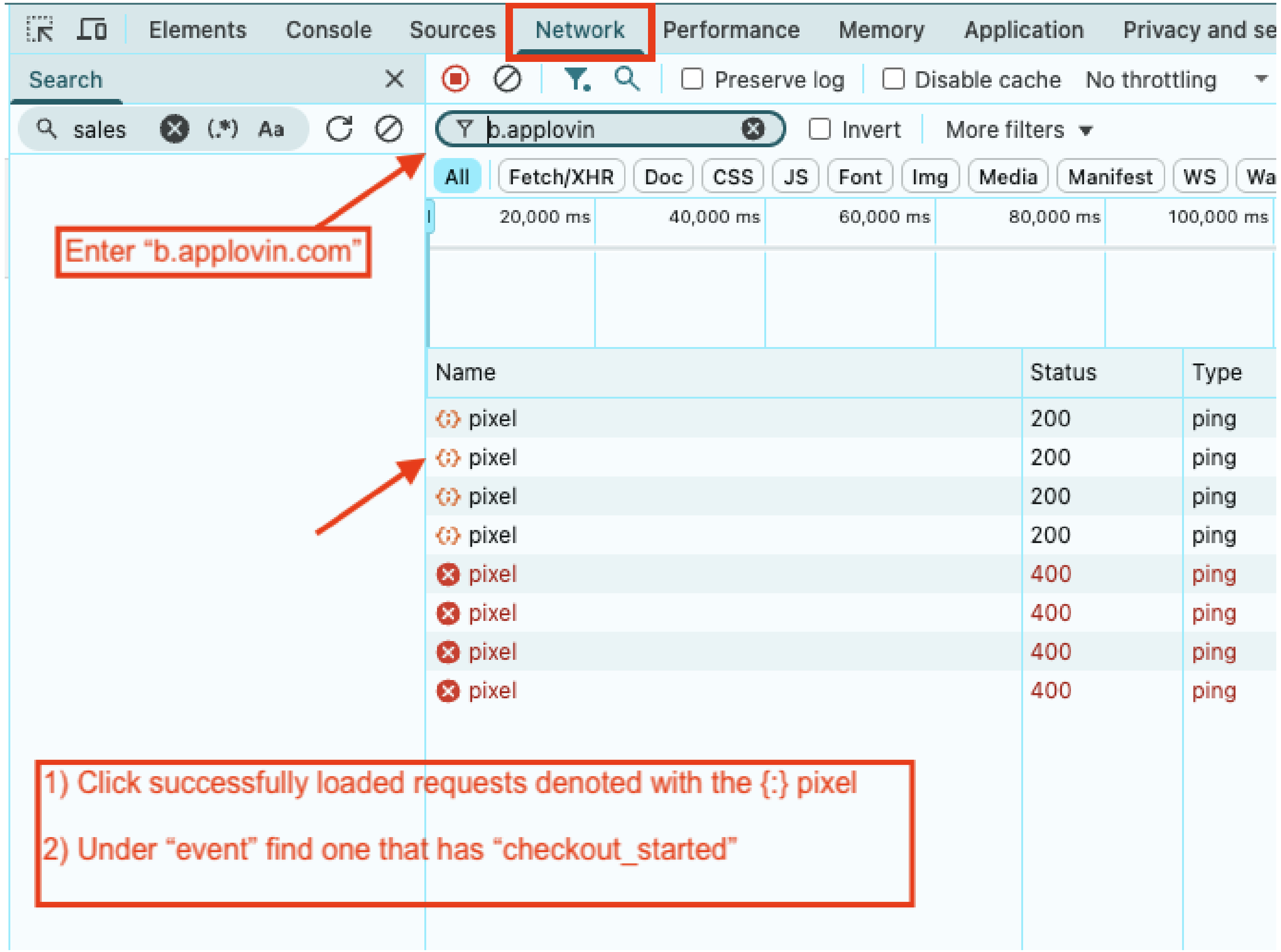
Phone

```
  aLink: ""
  accessKey: ""
▸ attributeStyleMap: StylePropertyMap {size: 0}
▸ attributes: NamedNodeMap {0: class, class: class, length: 1}
  autocapitalize: ""
  autofocus: false
  background: ""
  baseURI: "https://www.trueclassictees.com/checkouts/cn/Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI?au
  bgColor: ""
  childElementCount: 61
▸ childNodes: NodeList(63) [text, script, text, script, style, script, link, link, link, link, link, link, link, scr
▸ children: HTMLCollection(61) [script, script, style, script, link, link, link, link, link, link, link, script, scr
▸ classList: DOMTokenList [value: '']
  className: ""
  clientHeight: 1150
  clientLeft: 0
  clientTop: 0
  clientWidth: 634
  contentEditable: "inherit"
  currentCSSZoom: 1
▸ dataset: DOMStringMap {}
  dir: ""
  draggable: false
  elementTiming: ""
  enterKeyHint: ""
▸ firstChild: text
▸ firstElementChild: script
  hidden: false
  id: ""
  inert: false
  innerHTML: "\n<script>\n(function() {\n  try {\n    // No nee Show more (505 kB)  Copy
  innerText: "Skip to content\nTrue Classic Checkout\nOrder summary\nOriginal price\n\n$209.97\n\nExpress checkout\r
  inputMode: ""
  isConnected: true
  isContentEditable: false
  lang: ""
▸ lastChild: script
▸ lastElementChild: script
  link: ""
  localName: "body"
  namespaceURI: "http://www.w3.org/1999/xhtml"
  nodeName: "BODY"
  nodeType: 1
  nonce: ""
  offsetHeight: 1150
  offsetLeft: 0
  offsetTop: 0
  offsetWidth: 634
▸ onerror: (e,t,n,r,i)=> {…}
  outerHTML: "<body class=\"\">\n<script>\n(function() {\n  try Show more (505 kB)  Copy
  outerText: "Skip to content\nTrue Classic Checkout\nOrder summary\nOriginal price\n\n$209.97\n\nExpress checkout\r
▸ ownerDocument: document
▸ parentElement: html
▸ parentNode: html
```

Guide to Desktop Checking on Fingerprinting

5. In the search bar, type: b.applovin.com

6. Click the top successfully loaded requests in the list. Successful requests are denoted as {:} pixel.



Name	Status	Type
{:} pixel	200	ping
{:} pixel	200	ping
{:} pixel	200	ping
{:} pixel	200	ping
☒ pixel	400	ping
☒ pixel	400	ping
☒ pixel	400	ping
☒ pixel	400	ping

Enter “b.applovin.com”

1) Click successfully loaded requests denoted with the {:} pixel

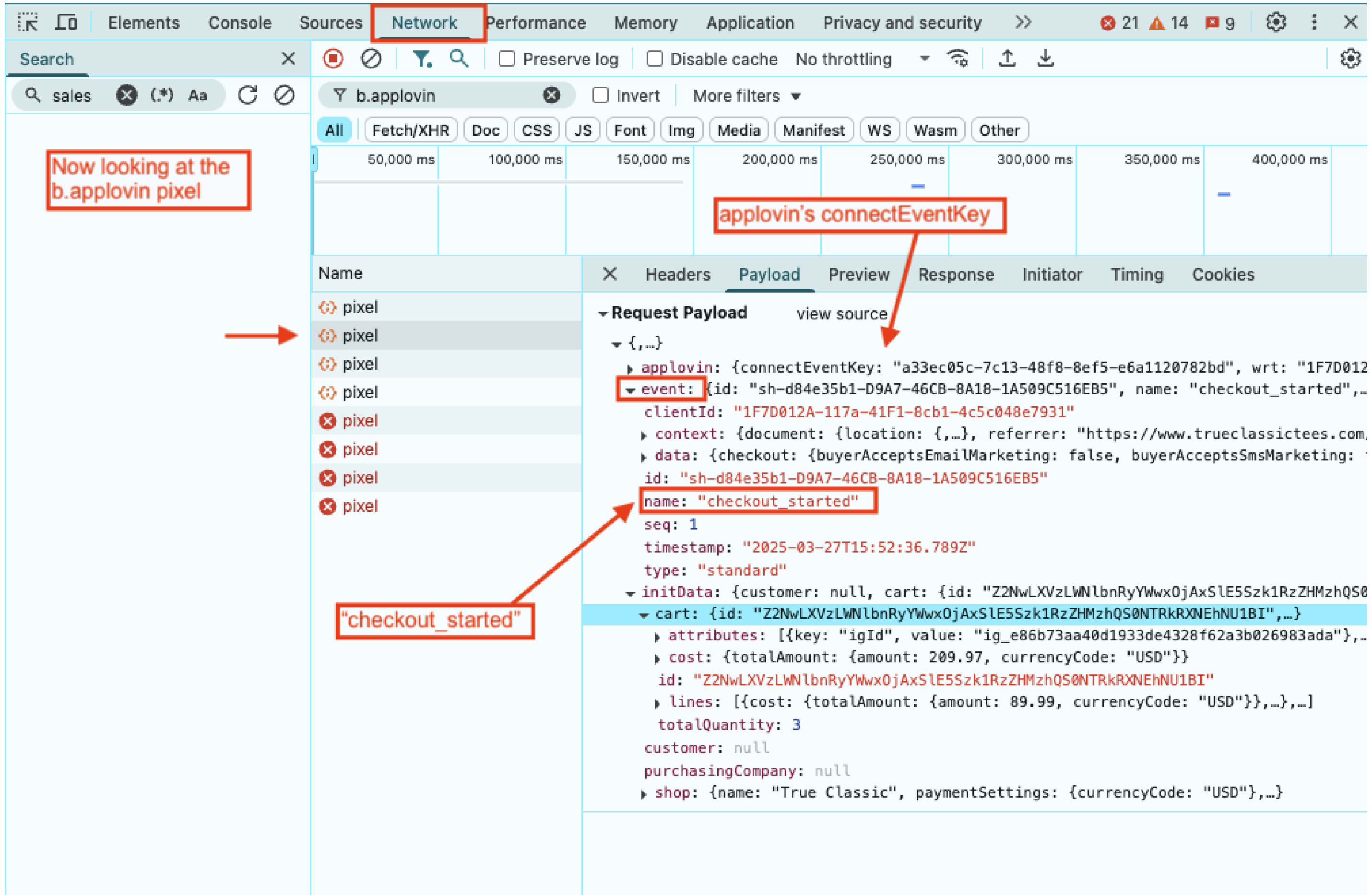
2) Under “event” find one that has “checkout_started”

Guide to Desktop Checking on Fingerprinting

7. Go to the “Payload” tab, then
→ Expand initData (open the arrow)
→ select “cart”
→ select “attributes”

Look for the indicator “checkout_started”

You are now looking in the b.applovin pixel on True Classic’s check out page



Now looking at the b.applovin pixel

applovin’s connectEventKey

“checkout_started”

```
▾ {,…}
  ▸ applovin: {connectEventKey: "a33ec05c-7c13-48f8-8ef5-e6a1120782bd", wrt: "1F7D012
  ▾ event: {id: "sh-d84e35b1-D9A7-46CB-8A18-1A509C516EB5", name: "checkout_started",…
     clientId: "1F7D012A-117a-41F1-8cb1-4c5c048e7931"
    ▸ context: {document: {location: {,…}, referrer: "https://www.trueclassictees.com,
    ▸ data: {checkout: {buyerAcceptsEmailMarketing: false, buyerAcceptsSmsMarketing:
     id: "sh-d84e35b1-D9A7-46CB-8A18-1A509C516EB5"
     name: "checkout_started"
     seq: 1
     timestamp: "2025-03-27T15:52:36.789Z"
     type: "standard"
  ▾ initData: {customer: null, cart: {id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0
    ▾ cart: {id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI",…}
      ▸ attributes: [{key: "igId", value: "ig_e86b73aa40d1933de4328f62a3b026983ada"},…
      ▸ cost: {totalAmount: {amount: 209.97, currencyCode: "USD"}}
       id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI"
      ▸ lines: [{cost: {totalAmount: {amount: 89.99, currencyCode: "USD"}},…},…]
       totalQuantity: 3
     customer: null
     purchasingCompany: null
    ▸ shop: {name: "True Classic", paymentSettings: {currencyCode: "USD"},…}
```

Guide to Desktop Checking on Fingerprinting

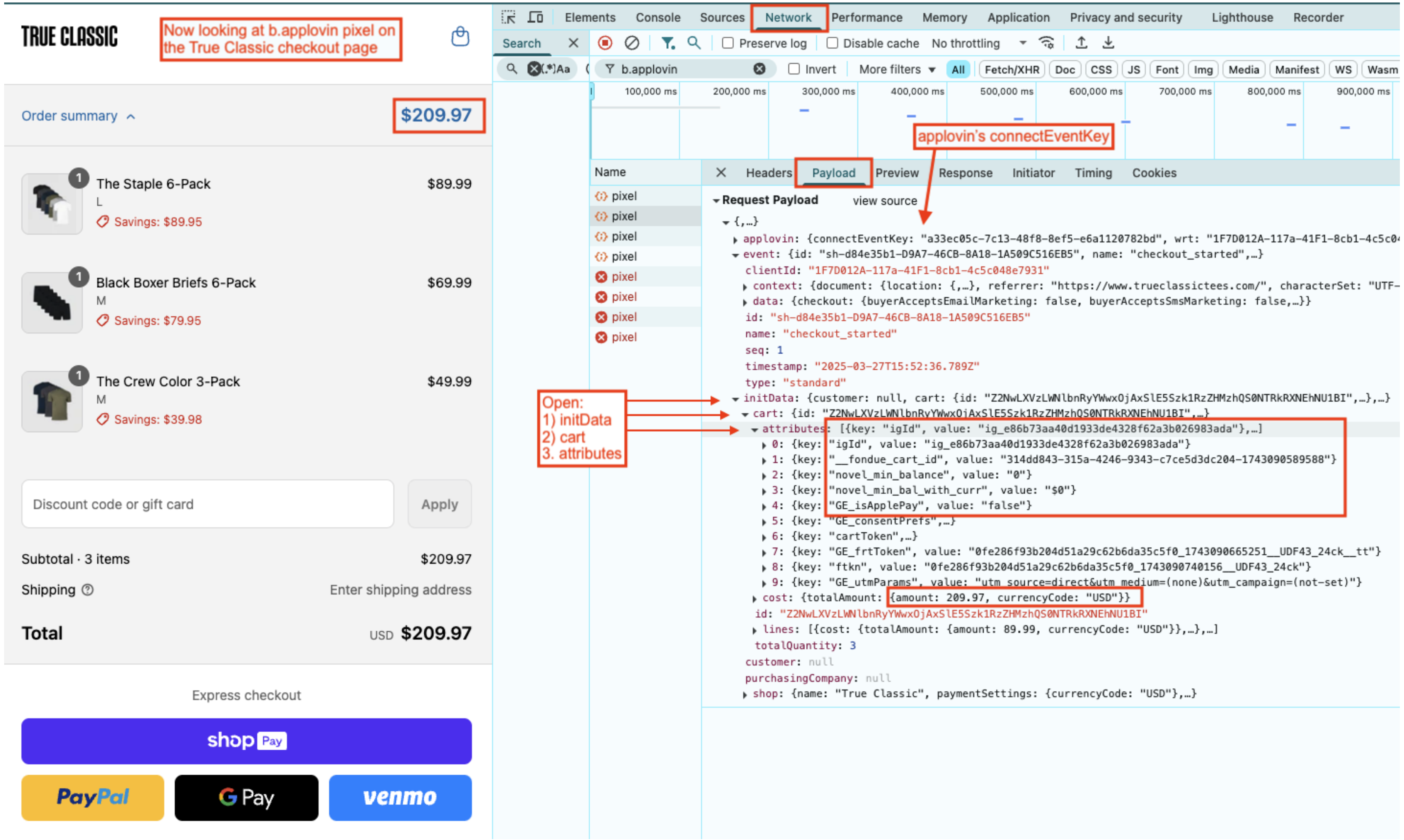
8. Look for entries with a "key" and "value" structure*

You are now looking in the b.applovin pixel on True Classic's check out page

You can see the following key data is picked up:

- igID, Instagram ID
- fondue cart ID
- novel ID

Note "fondue cart" and "novel" are shopify plug ins as tracking an ApplePay signal.



Now looking at b.applovin pixel on the True Classic checkout page

applovin's connectEventKey

Open:
1) initData
2) cart
3. attributes

TRUE CLASSIC

Order summary $209.97

The Staple 6-Pack L Savings: $89.95	$89.99
Black Boxer Briefs 6-Pack M Savings: $79.95	$69.99
The Crew Color 3-Pack M Savings: $39.98	$49.99

Discount code or gift card — Apply

Subtotal · 3 items	$209.97
Shipping	Enter shipping address
Total	USD **$209.97**

Express checkout

Filter: b.applovin

```
▾ Request Payload      view source
 ▾ {,…}
   ▸ applovin: {connectEventKey: "a33ec05c-7c13-48f8-8ef5-e6a1120782bd", wrt: "1F7D012A-117a-41F1-8cb1-4c5c0
   ▾ event: {id: "sh-d84e35b1-D9A7-46CB-8A18-1A509C516EB5", name: "checkout_started",…}
      clientId: "1F7D012A-117a-41F1-8cb1-4c5c048e7931"
     ▸ context: {document: {location: {,…}, referrer: "https://www.trueclassictees.com/", characterSet: "UTF-
     ▸ data: {checkout: {buyerAcceptsEmailMarketing: false, buyerAcceptsSmsMarketing: false,…}}
      id: "sh-d84e35b1-D9A7-46CB-8A18-1A509C516EB5"
      name: "checkout_started"
      seq: 1
      timestamp: "2025-03-27T15:52:36.789Z"
      type: "standard"
   ▾ initData: {customer: null, cart: {id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI",…},…}
     ▾ cart: {id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI",…}
       ▾ attributes: [{key: "igId", value: "ig_e86b73aa40d1933de4328f62a3b026983ada"},…]
         ▸ 0: {key: "igId", value: "ig_e86b73aa40d1933de4328f62a3b026983ada"}
         ▸ 1: {key: "__fondue_cart_id", value: "314dd843-315a-4246-9343-c7ce5d3dc204-1743090589588"}
         ▸ 2: {key: "novel_min_balance", value: "0"}
         ▸ 3: {key: "novel_min_bal_with_curr", value: "$0"}
         ▸ 4: {key: "GE_isApplePay", value: "false"}
         ▸ 5: {key: "GE_consentPrefs",…}
         ▸ 6: {key: "cartToken",…}
         ▸ 7: {key: "GE_frtToken", value: "0fe286f93b204d51a29c62b6da35c5f0_1743090665251__UDF43_24ck__tt"}
         ▸ 8: {key: "ftkn", value: "0fe286f93b204d51a29c62b6da35c5f0_1743090740156__UDF43_24ck"}
         ▸ 9: {key: "GE_utmParams", value: "utm_source=direct&utm_medium=(none)&utm_campaign=(not-set)"}
       ▸ cost: {totalAmount: {amount: 209.97, currencyCode: "USD"}}
        id: "Z2NwLXVzLWNlbnRyYWwxOjAxSlE5Szk1RzZHMzhQS0NTRkRXNEhNU1BI"
       ▸ lines: [{cost: {totalAmount: {amount: 89.99, currencyCode: "USD"}},…},…]
        totalQuantity: 3
      customer: null
      purchasingCompany: null
     ▸ shop: {name: "True Classic", paymentSettings: {currencyCode: "USD"},…}
```