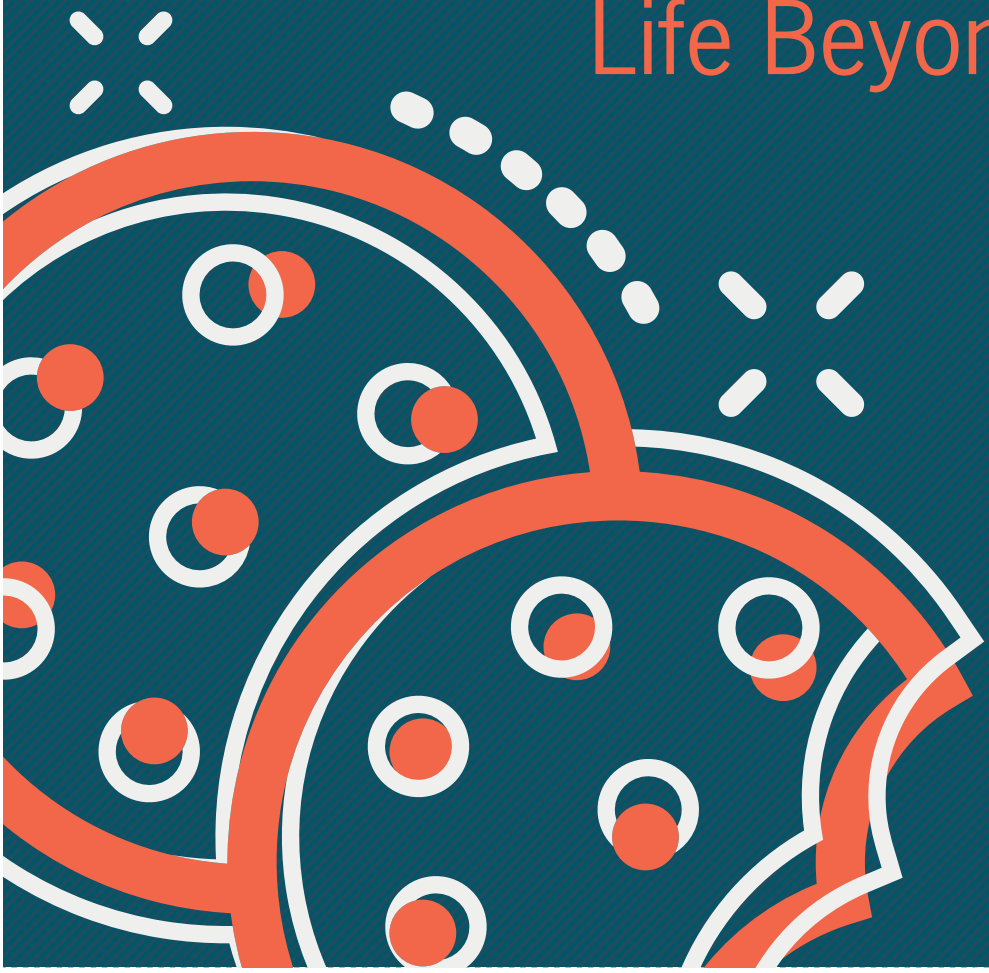
admonsters

PLAYBOOK

Life Beyond Cookies



Sponsored by:

LiveRamp®

WHAT'S A PLAYBOOK?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for 20 years. A playbook solidifies what has made our events "must attend" for many digital strategists. By bringing people together to share learnings and best practices in a focused way, people can create a plan and avoid hours—if not days—of doing research on their own.

The AdMonsters playbook concept takes existing AdMonsters content (from conferences and AdMonsters.com) and, with the help of the AdMonsters community, "crowd sources" a document that outlines best practices on a particular topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy. This document does not get into specifics around individual solution providers intentionally.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too general. In a technology-driven industry like digital advertising, information quickly becomes obsolete. The intention is that, based on the feedback of the AdMonsters community, the next playbook will start to take shape and, with additional contributors, grow in both depth and breadth.

INTRODUCTION

Ubiquitous as the cookie has become today, it's weird to think the little .txt file was originally cooked up by Netscape engineers in 1994 as a simple way to power virtual shopping carts. Based on developer kit "magic cookies," these enabled sites to "remember" items that had been selected by users as they navigated page to page by saving byte-sized files into browser storage space.

The cookie's potential outside of e-commerce was readily apparent to Internet pioneers, and the device quickly became a prized tool in the web developers' kit for site personalization… As well as a lynchpin for tracking, targeting, and measuring in digital advertising.

Even before the Internet, businesses have struggled with how to remember their customers at each interaction—whether by recording names in ledgers for in-store credit; designing loyalty programs with log-ins; or creating accounts based on email addresses or phone numbers. As commerce and media consumption moved online, media companies and advertisers needed a new way to remember consumers in the new anonymous world wide web—and the cookie proved up to the job.

Times and tech change—as the limits of third-party cookies have become increasingly glaring, regulators and browsers have answered growing consumer privacy concerns by limiting their functionality or outright banning them. In effect, the third-party cookie becomes less useful by the day.

While new regulations and browser cookie crackdowns have inserted some chaos into the advertising ecosystem, publishers should view the fall of the third-party cookie as a good thing. Third-party cookies were arguably diminishing the value of publisher first-party data, which are becoming more prized as the cookie well dries up. Smart publishers will help their advertisers adjust during this time of transition while also driving additional revenue monetizing their valuable data tied to unified identifiers that stretch across devices.

This playbook aims to show publishers how to not only survive without cookies, but come out the other side more powerful than before. Over these pages, we'll

- Detail the many reasons the cookie is fading;
- Examine the benefits of traffic authentication;
- Dive into the role of an identity resolution partner;
- Look at the potential for universal IDs; and
- Identify the most important traits for an identity resolution partner.

WHAT IS AN IDENTIFIER?

Recognizing customers consistently over multiple interactions or website sessions is a constant challenge for businesses and publishers. They may do this by assigning their own customer ID, or using a unique customer username or contact information such as an email address or phone number, in order to tie purchases, logins, account information, and marketing information to an existing customer. In environments where a user does not log in or identify themselves, such as a website or mobile app, companies attempt to consistently identify users through browser cookies or mobile advertising IDs (MAIDs), in order to personalize website content or advertisements, frequency cap, or measure the effectiveness of ads.

WHY THE COOKIE IS CRUMBLING?

The original sin of digital publishing may be the embrace of ad-driven revenue models. This in turn led to the user perception that Internet content is "free." The cookie's virtual invisibility kept many consumers blissfully unaware of the true value exchange with Internet content.

Rumors of the third-party cookie's death have been greatly exaggerated for years, but recent regulatory developments and browser privacy efforts have upset the dominance of this digital identifier. GDPR, CCPA, and browser privacy initiatives are only the beginning of a wider movement around data privacy, but they paint a clear picture of the next generation of consumer expectations.

Much of the contemporary Internet—and certainly digital advertising—has been built upon tools for data transference. While the cookie has been key in the development of digital advertising and programmatic transactions in particular, the architecture is not going to collapse without it. Understanding why the third-party cookie has gone out of favor—or really, outlived its usefulness—illuminates what will replace it.

PRIVACY REGULATIONS AND BROWSER CRACKDOWNS

GDPR: The European Union's General Data Protection Regulation requires parties involved in online data transfer to gain informed and explicit consent from users residing in the EU before collecting and generally handling a wide realm of personal data.

GDPR Article 5(b) further states that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;" collection should be limited where possible, and personal data stored no longer than necessary. GDPR fines are hefty—€50 million for Google was far smaller than penalties faced by Marriott and British Airways.

Since GDPR went into effect May 25, 2018, there has been a notable drop in third-party cookies in EU online traffic. It's in the interest of publishers—regarded as data controllers—to limit the actions of third-party data processors on their European traffic because they can be held liable for any GDPR violations committed down the chain.

In addition, there is still a great deal of confusion about enforcement and just what constitutes a violation. The Dutch Data Protection Authority has ruled that "cookie walls" that facilitate quick opt-ins are not in line with GDPR while the UK DPA has come out with a ruling that real-time bidding technology in general is in violation. The EU's renewed ePrivacy Directive, which threatens even stricter enforcement, is yet to be finalized.

We're only beginning to see the fallout from EU online privacy initiatives. The good news is that people in the EU people are starting to understand the advertising-driven value exchange with digital media. In 2019, there's far more awareness thanks to the consent requirement.

CCPA: The California Consumer Privacy Act, which applies to any publisher or company that deals with the data of 50,000 or more California residents a year, has a wider scope than GDPR when it comes to defining personal data. However, the biggest difference between the two laws is that instead of

requiring consumers to opt in to data sharing, CCPA demands publishers offer a comprehensive opt-out.

A button reading something along the lines of "Do Not Sell My Personal Information" must appear on the homepage. While the law is most concerned with the selling of data, the term "sell" itself is vague and includes "renting, disclosing, disseminating, making available, transferring" and more in its definition.

CCPA goes into effect on Jan. 1, 2020, but will not be enforced until July 2020. At the same time, violations could go back to a year prior. The IAB and other trade groups have called for federal regulation that will supercede state laws like CCPA, but no legislation appears to be gaining traction.

Browser Privacy Initiatives: When it comes to third-party cookie hurt, Apple's Safari browser has blocked third-party cookies as a default option since version 6, forcing users to turn on the functionality within preferences. Other browsers like Mozilla's Firefox have followed Apple's lead here and blocked third-party cookies by default.

Apple raised the stakes in 2017 by introducing Intelligent Tracking Protection (ITP) measures meant specifically to crack down on cross-site tracking related to advertising. ITP shortened the lifespans of all third-party trackers to 24 hours (the average cookie has a 30-day lifespan) with some exceptions.

In 2019, update 2.1 shrank the lifespan of first-party cookies to seven days to cut down on ITP work-arounds, and 2.2 then cut that down to a single day as a way to fight cross-site tracking via "link decoration." The latest version also puts an automatic 24-hour block on third-party cookie-reading.

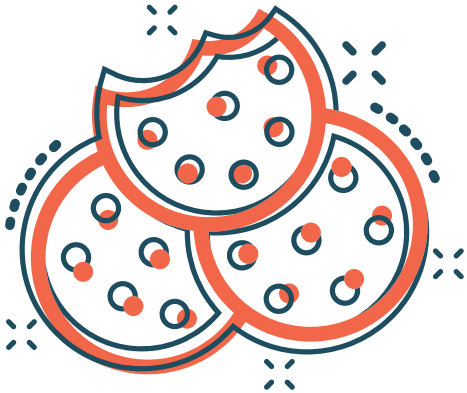
For many publishers, Safari users are now something akin to blank slates, lacking value in programmatic markets where the cookie is a cherished targeting commodity. In addition, third-party metrics for performance and attribution are unavailable. This has been challenging for publisher monetization efforts in mobile, where typically a third of traffic is from Safari.

In 2019, Google's Chrome introduced enhanced privacy controls for users offering greater visibility into cookie use while curbing fingerprinting and aggressive tracking. Many in the industry expect further cookie limitations, while others believe a browser-based advertising identifier along the lines of ID for Advertising (IDFA) in Apple's iOS app ecosystem.

THE COOKIE'S FLAWS EXPOSED

Taken altogether, it's hard not to see these exposing the many faults of the cookie. But beyond that, digital media had really reached the limits of the cookie's usefulness as a stand-alone identifier.

- The cookie is a browser tool, and digital traffic is increasingly being monetized in cookieless environments like mobile and connected-TV apps. The latter is an enormous opportunity as it is siphoning dollars from linear TV advertising.
- Increased traffic to cookieless environments means that the supply of cookies is on the decline.
- The cookie has a short lifespan. It's a general rule that a cookie should expire no more than 30 days after it is placed.
- Cookies can be deleted at any time by a user, and their deployment is halted via ad blockers.
- Cookie-syncing causes great latency within the programmatic pipes, slowing down auctions and potentially causing publishers to miss out on quality bids.
- Cookies degrade quickly in a waterfall effect: every time data is sent through a DMP, then to a DSP, and then to an SSP, the cookie pool shrinks, reducing the reach of advertisers.
- A cookie represents only a device or browser; two browsers on the same device will have completely different identifiers although they represent the same person.
- Users have little visibility into what data is being collected through cookies and how they are being used. Opting out of data collection via cookies can often be a (purposefully) byzantine process.



CAN ADVERTISERS GIVE UP COOKIES?

Study after study shows that advertisers pay a premium for data-driven impressions—the most recent is a Google study that shows traffic with no third-party cookies yielded publishers 52% less revenue than cookie-based traffic.

Part of the reason third-party cookies became an essential part of the RTB ecosystem is that they vastly improved advertisers' online reach and could be used to cherry-pick audiences at scale for super cheap CPMs.

Advertisers will need to trade off quantity for quality going forward, which is a total shift in mindset. They need to transform how advertising campaigns are measured, what their goals are, and how to better use their first-party data to create relevant audiences.

It will be a difficult transition, but with the right tools and partners, publishers can show advertisers the way.

RULE OF THE WALLED GARDENS?

A **Walled Garden** is an ecosystem in which one party has complete control over all operations in said ecosystem. By requiring logins from users, they authenticate all traffic to their owned and operated sites. In digital media advertising, that means a company that controls both the buying and selling mechanisms, and thus the identifiers used for targeting and tracking. That company has no obligation to share those identifiers or the targeting data with any other parties, including the end buyers and sellers.

The cookie has been central to creating an open advertising ecosystem to challenge the dominance of walled gardens like Google and Facebook. Through cookie-syncing and data-sharing among ad tech partners, the open ecosystem offers greater competition and (arguably) better transactional transparency, two key benefits for advertisers and publishers. But as the cookie's relevance has waned, the walled gardens have grown stronger and other companies have consolidated media offerings and ad tech to seemingly construct their own burgeoning walled gardens.

For the open advertising ecosystem to continue, there has to be flow of data between buyers, sellers, and intermediaries. Thus, a variety of companies serving as data conduits have emerged to keep the open advertising ecosystem alive—in a privacy-friendly fashion. And every publisher has the opportunity to monetize their content just like a walled garden by collecting user logins.

LOGGING IN

Though it's long been said that publisher first-party data is the most valuable asset in digital media, it hasn't felt that way on the programmatic markets. Since audience targeting has become priority no. 1 in digital advertising, advertisers have chased their own cookies and third-party ones across both open and private exchanges.

But a diminishing cookie pool amid the privacy crunch and a big push toward identity marketing has advertisers re-adjusting their authentication and targeting strategies. Like the audiences in the walled gardens, that first-party publisher data is looking awfully sweet, especially if it's authenticated. Getting your users to log in enables direct authentication, creating an identifier around a piece of deterministic or personally identifying information. Often this takes the form of an email, which is then hashed to provide security and anonymity.

As you might imagine, users don't want to log in to any and every site they visit, especially when "sideways entry" a la social media and search engines accounts for a great deal of traffic. Asking for a log-in requires some kind of transparent value exchange, and many publishers are finding the answer is old-fashioned—quality content that encourages deep engagement.

Revenue professionals now find themselves very interested in audience development as engaged users are increasingly willing to log into sites for personalized content and other benefits. Often logins are used across devices (e.g., laptop, mobile phone, even connected TV), making it an identifier at the individual level.

While a log-in can be a great asset, it's not a necessity to leverage an identity resolution partner—a step a publisher will want to take to scale their identity-based selling efforts.

IDENTITY RESOLUTION

Identity Resolution is the process of stitching together a wide variety of identifiers based on first-, second-, and third-party data as well as personally identifiable data. Behavioral and contextual data are joined with deterministic identifiers to form a persistent, unified identifier that represents a user on an individual level across channels and devices. An **Identity Graph** is the database where user profiles and their related identifiers are stored.

EMAIL AS AN IDENTIFIER

Another form of content with a direct authentication angle is the email newsletter, which has seen a surprising resurgence in popularity. For publishers, the newsletter is a triple revenue threat: they can use it to garner email addresses, which can be the basis for identifiers; they can gather data submitted by users to better understand audience; and they can actually monetize newsletter content with ads, branded content, or subscription models.

However, a hashed email alone is not a secure identifier. First, an email address is widely considered PII (definitely by GDPR and CCPA), and hashing algorithms can be cracked to reveal the hidden emails. In addition, emails may not extend across connected devices like connected TVs and can often be out-of-date, duplicates, or spam. In leveraging hashed emails, you'll find more value in validating the identifier against other data sets (online and offline).

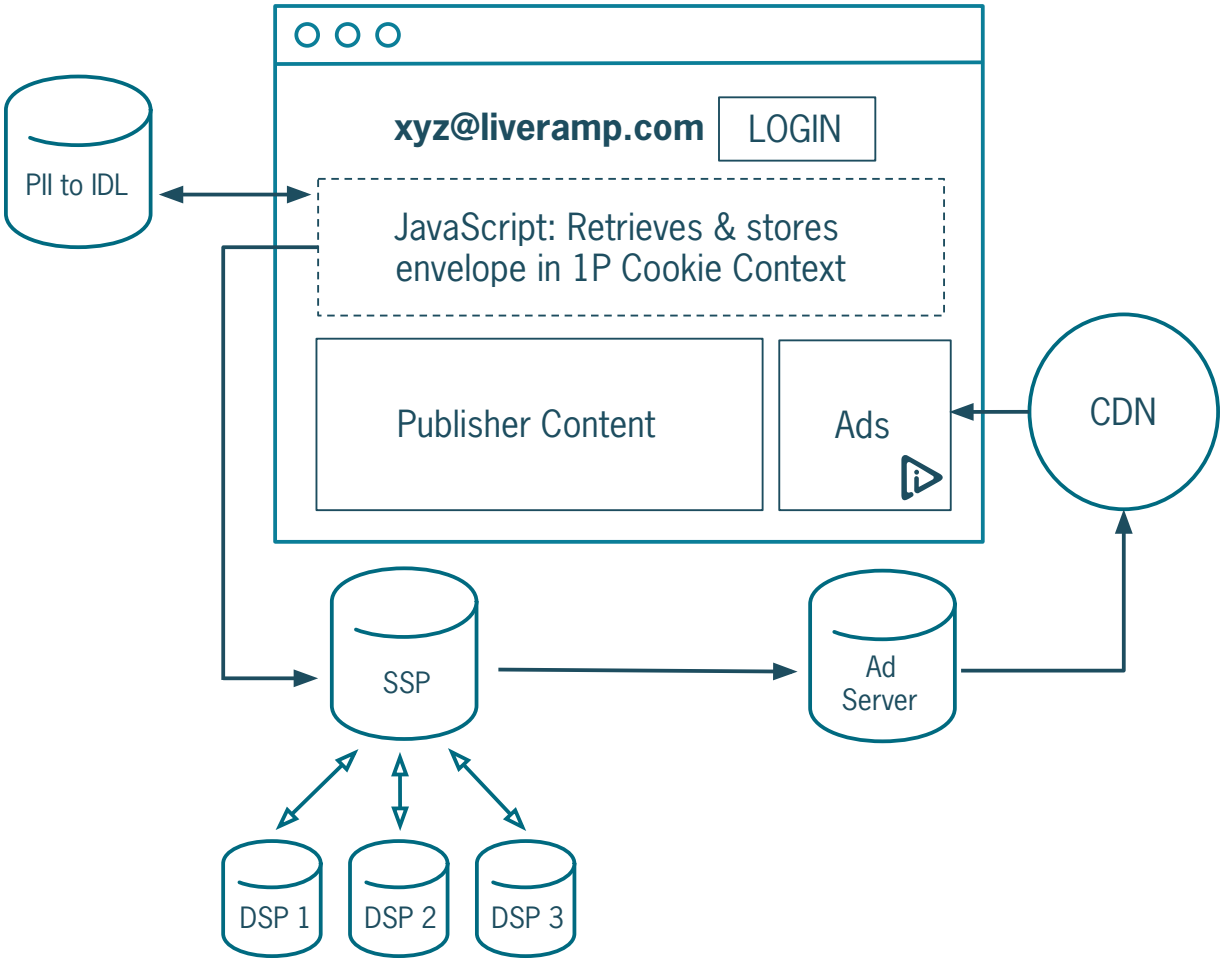
WHY AN IDENTITY RESOLUTION PARTNER?

So great—you got all that log-in data; now what? You can't easily send it off to the programmatic exchanges and expect to be overwhelmed in bids. That data is unique to you as a publisher, and finding matches with buyers will take time you probably don't want to spend. To scale your audience, you want to partner up with an identity resolution partner.

An identity resolution partner will match your identifiers with its identity graph made up of online and/or offline identifiers. By leveraging a conduit or sidecar to SSPs, exchanges, and DSPs, it can provide real-time ID-matching with programmatic partners. It's a far more efficient process than cookie syncing, not to mention quicker and less labor-intensive. On top of that, this dramatically increases addressability for publishers in cookieless (connected TV or mobile app) or cookie-limited (e.g., Safari) environments.

Furthermore, consent management is easier and safer as the publisher is sharing data with just one company, who is then sending out its own identifier for matching, rather than sending a barrage of cookies to countless companies—many of them likely unknown—on the open programmatic market.

AN EXAMPLE OF AN IDENTITY RESOLUTION SYSTEM WORKFLOW FROM LIVERAMP



KEY FACTORS IN SELECTING AN IDENTITY RESOLUTION PARTNER

- **Match Rates.** Match rates are a key indicator in determining how many users can be reached across the omni-channel ecosystem, as well as central to ensuring the accuracy of an identity resolution partner. A thorough provider will match against both online and offline PII data. In evaluating match rates, consider household-level and individual processes, as well as the vendor's ability to match a specific or set of destinations.

- **Partnerships.** Your IDs are going nowhere if your provider isn't integrated with major SSPs, DSPs, exchanges, and other demand sources.

- **Neutrality.** An identity resolution partner that also buys and sells media may have some hairy conflicts of interest. Not a great starting place for establishing a trust-centric relationship.

- **Global Presence.** It's a wide, wide world, and you should be thinking global in your monetization. How are you going to do that if your identity resolution provider doesn't have a global footprint?

- **An Ethical Stance.** Data privacy entering the 2020s is no joke, and your identity resolution partner will be dealing with awfully sensitive information. Brush up on your partners' views on consent and data-sharing, but also seek out providers that aim to be thought leaders when it comes to online privacy

UNIVERSAL IDS

Universal IDs are based on shared identity graphs of multiple SSPs, DSPs, exchanges, identity resolution partners, and others. Typically these are managed by a neutral company and open for use by all parties buying and selling media. The goal is to provide a baseline identity layer to aid in the buying and selling of media within open advertising ecosystems. Two prime examples are Digitrust (run by the IAB Tech Lab) and the Ad ID Consortium, a partnership between LiveRamp, Index Exchange, and others.

CONCLUSION

We salute the cookie for all the service that it has provided to digital advertising, powering data transference throughout the open programmatic ecosystem—for better or worse. However, online-privacy-focused regulations and browser initiatives highlight that the cookie is past its prime, and is a non-entity within the blooming mobile app and connected TV landscapes.

Looking beyond the cookie, publishers and advertisers alike should embrace identity resolution providers that can provide efficient and privacy-friendly solutions for data transference.

There's no better time for publishers to regain ownership of consumer relationships, allowing visitors to safely engage with their content. All while improving monetization, enabling compliance, and driving transparency to help solve the greatest challenges of the modern advertising ecosystem: fragmented data, stringent regulatory guidance, and dependencies on browser cookies.

Think of identity less as the cookie's replacement and more as its rightful heir—finally addressing a problem over 20 years in the making.

LiveRamp provides the identity platform leveraged by enterprise marketers and their partners to deliver innovative products and exceptional experiences. The LiveRamp platform connects people, data, and devices across the digital and physical world, powering the people-based marketing revolution and allowing consumers to safely connect with the brands and products they love.

Headquartered in the technology hub of San Francisco, LiveRamp delivers privacy-conscious solutions that honor the best practices of leading associations, including the Digital Advertising Alliance's (DAA's) ICON and AppChoices programs, the Interactive Advertising Bureau (IAB), the Data & Marketing Association (DMA), and the Advertising Research Foundation (ARF).

AdMonsters is the global leader in strategic insight on the future of digital media and advertising technology. Through our conferences, website, and original research, we offer unparalleled in-person experiences and unique, high-quality content focused on media operations, monetization, technology, strategy, platforms and trends. Founded in 1999, AdMonsters began serving the advertising operations professional through live media and its online community. We provided a forum to share best practices, explore new technology platforms and build relationships. Today's expanding ecosystem now includes publishers and content creators, agencies, SSPs, DMPs, DSPs, RTB and service providers, technology and platform developers, advertising networks, brands, and investors.

This vibrant community is forward-looking and results-oriented. Their success depends on strategic insights about technology and monetization, and the exchange of actionable peer-to-peer best practices. AdMonsters has built its reputation on providing objective editorial leadership based on deep, real-world expertise. We have continued to evolve our editorial strategy to address the changing needs of the market and, as a result, AdMonsters has attracted a highly focused audience who are at the forefront of the industry, and leading marketing partners have found AdMonsters to be a powerful channel to reach these decision makers. Today, our portfolio of integrated media solutions includes industry leading live events, our innovative Connect content solutions, email marketing programs, and more.

As of March 2015, AdMonsters is part of the Access Intelligence family of companies.

For more info:
See admonsters.com
Follow us on Twitter: @AdMonsters
Facebook: facebook.com/admonsters

Media contact:
marketing@admonsters.com
Sponsorship contact:
sales@admonsters.com

sponsored by: