bluecava

The Next Generation of Advertising Platforms

Privacy Safe Technologies that Leverage Statistically Generated Identifiers for Digital Advertising have arrived

Device recognition technologies have moved front and center as a result of significant shifts in the AdTech marketplace including: browser deletion of third-party cookies, the introduction of mobile platform identifiers such as IDFA, and Android's Ad ID. As a result, the traditional (albeit imperfect) balance between the interests of digital marketers and the interests of privacy advocates has been strained. Marketers look to serve up the right ad to the right consumer on the right device at the right time while privacy advocates seek to guard against the creation of persistent databases and other – sometimes ephemeral – privacy concerns.

The tension between these competing interests places the advertising technology marketplace into a difficult balancing act. The question for all parties today is 'how much is just right'. Moreover, the use of technological innovations such as 'fingerprinting' – when utilized outside the scope of their original purpose of enabling security and fraud prevention – may cut at privacy interests when used in a digital advertising context.

This white paper outlines a new approach based on statistical identifiers that improve quality and accuracy for digital marketers while ensuring a layer of anonymity for consumers. It's an approach pioneered by BlueCava, a leader in cross-screen audience association solutions that is gaining support across the AdTech and standards community as being privacy safe. This approach builds upon the foundation provided by the Fair Information Practice Principles as well as the more recent privacy Bill of Rights published by the White House.

This white paper was created to help interested parties understand how BlueCava addresses key consumer privacy concerns. Those with additional questions should contact privacy@bluecava.com.

©2014BlueCava, Inc. All Rights Reserved

INTRODUCTION:
More than just the cookie crumbling

The privacy issue for digital advertisers began back in 1999 with DoubleClick's purchase of the Abacus offline direct marketing database. Concerns over the potential merger of offline PII data with an online profiling database resulted in the first of many privacy firestorms that have plagued digital advertising for over a decade. While the Network Advertising Initiative[1] (NAI) and Digital Advertising Alliance[2] (DAA) Codes are helpful in terms of addressing some of the more significant privacy concerns that have been raised, they don't address every privacy concern.

Over time, the digital privacy debate has grown and multiple issues are routinely confused and conflated to include:

• Conflating digital advertising and privacy concerns with unrelated privacy concerns such as identity theft and alleged Government wiretapping.

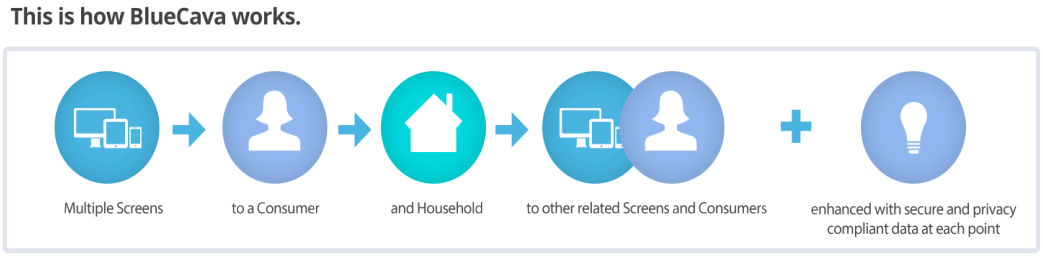
• Proprietary Publisher networks vs. Open Network debates over identification standards that create competitive disadvantages.

> While generally more elastic than law, industry standards that have emerged over time are often stretched as such standards struggle to keep up with the rapid pace of marketplace innovation. Digital advertisers want to move beyond 'first generation' approaches such as cookies, but are loathe to utilize technologies such as device fingerprinting and listening techniques that lack transparency or consumer privacy controls. Although advertisers recognize audiences through identifiers within closed networks, they can't engage consumers outside of that environment.

Recently, BlueCava has stepped forward with a more reasoned approach, one that leverages what it calls 'digital threads' that are generated anonymously based on statistical identifiers. These digital threads are privacy-safe and provide advertisers with a highly accurate platform for ad delivery, reporting, targeting and attribution. This white paper details the approach starting with what BlueCava does (and does not) do in its process, the reasons why statistical identification is required in today's digital advertising marketplace and how BlueCava applies its ID's in a privacy-compliant way by embracing well known

[1] www.networkadvertising.org
[2] www.aboutads.info

©2014BlueCava, Inc. All Rights Reserved



BlueCava moves across screens and channels as fast as your audience, mapping all of the screens, consumers, and households, and adding valuable segment data and industry-used ids.

privacy frameworks such as the Fair Information Practice Principles. The white paper also places device recognition into historical context as part of a larger evolution and growth of digital ad spend.

What BlueCava Does

BlueCava offers an audience association platform that enables advertisers to recognize devices (i.e., computers, mobile phones & tablets) for the purpose of sequential targeting, cross-screen attribution, and optimization of digital advertising. Our platform is designed to seamlessly integrate into advertising networks, exchanges and platforms in order to:

1. Establish and map relationships cross-screen.
2. Measure true audience reach and frequency across all channels and screens, 2nd screen conversions, and cross-screen paths.
3. Make targeting data actionable by deploying across all environments, optimizing based upon digital consumption across those environments, and leverage existing data to new associated devices.

What Blue Cava Does NOT Do

BlueCava does not engage in digital fingerprinting. Somewhat ironically, BlueCava actually coined the term "fingerprinting" when BlueCava was spun out of security firm Uniloc. Given our parent company's success in the security and copyright protection sphere, the initial approach was to leverage many of those same techniques in a digital ad serving context. Over time, BlueCava realized that the fingerprinting process created significant privacy concerns when utilized for advertising purposes. As a result of feedback received, we have built a next generation platform that addresses the key concerns raised by fingerprinting by building on the Fair Information Practice Principles.

What Is Digital Fingerprinting?

Fingerprinting is a term initially used to characterize firms operating in the security, fraud prevention and copyright protection space. Fingerprinting is generally characterized as a process where an exhaustive list of data are collected from a device and/or browser, including personally identifiable information and data such as a MAC address. Fingerprinting often utilized techniques such as DNS caching and HTTP Authentication caching. Moreover, fingerprinting often utilizes Flash/Silverlight cookies and ETags for more persistent storage. BlueCava does not use any of these techniques or collect this type of data.

Here's what BlueCava does.

BlueCava offers an enabling technology platform – we do not collect data for online behavioral advertising purposes or remarketing purposes. While we facilitate the cross-screen management of our client's data (including client Online Behavioral Advertising (OBA) data), BlueCava does not directly engage in OBA. Moreover, we do not collect data that is proprietary to website publishers or that

©2014BlueCava, Inc. All Rights Reserved

otherwise identifies a particular publisher or advertiser in violation of the IAB terms and conditions 3.0. Additionally, BlueCava does not track users as they move from one publisher to another, only recognizing a user at a specific moment in time when they interact with a site or ad that includes our technology.

BlueCava does not compete with our network, exchange or platform clients, remaining an open and neutral partner. We only collect the minimum amount of data necessary for our clients to be able to utilize our platform.

Why Statistical IDs & Device Recognition Now?

For a number of years, the use of Device Recognition in an online context was mostly limited to fraud protection. That said, most third party AdTech companies have been collecting IP address and user agent string for years in an attempt to bolster their attribution and reporting capabilities. In other words, device recognition has been taking place for years – albeit with a more limited scope.

Similarly, a myriad of different identifiers have been utilized in the mobile space for years – having become a necessity due to the fragmented nature of mobile advertising. As we aim to improve the digital advertising marketplace, we recognize that extending the use of device recognition technology into the broader online marketplace is not only natural – it's necessary for the growth and development of the online ecosystem. A few observations that lead us in this direction:

The Cookie and Internet Browsers – Even though the debate between Mozilla and the IAB has subsided in recent months, the larger trends still demonstrate that cookies are under attack. When mainstream news starts discussing it, and it becomes a consumer-facing issue, it's no longer mere speculation. As some advertisers have lamented for years, Safari blocks third-party cookies by default and Internet Explorer is one memo away from doing the same. And of course, there's Mozilla.

Cookie Deletion – Industry conflict and disagreement aside, cookie deletion rates continue to increase year over year.

Mobile – As it's commonly known, cookies don't generally work on many mobile devices. As a result, mobile ad delivery and attribution has historically relied upon non-cookie based technologies. In fact, Google and Apple have offered unique user identification tools that incorporate privacy controls that have been well received by privacy advocates and regulators.

Platform Providers – Google and Microsoft have recently made announcements about their respective IDs. And carriers such as Verizon and AT&T have long had Subscriber IDs used for advertising across their customer base. We believe that it is likely that additional IDs will be offered by Adobe, Facebook, Twitter and other social networking platforms in the near term.

DigiTrust – Born out of the IAB Beyond Cookies working group, the Cookie Trust is a co-op of Adtech companies that are building a non-cookie based platform for delivery and attribution.

What Advertisers Want – As digital budgets continue to increase, so do advertiser expectations and requirements. In short, advertisers are demanding to better engage with their customers. And statistical identifiers and device recognition techniques are well suited to meet those expectations.

Business Need – The points above confirm that there is a business necessity to have a more stable and reliable delivery and attribution mechanism for digital advertising. One that reaches the right consumer on the right device, while protecting privacy interests.

©2014BlueCava, Inc. All Rights Reserved

Utilizing Device Recognition
in a Privacy Compliant Way

BlueCava's privacy framework builds upon existing privacy standards such as the Fair Information Practice Principles and the more recent White House Privacy Bill of Rights.

Learn More About This Ad

For Consumers

The Web sites you visit work with online advertising companies to provide you with advertising that is as relevant and useful as possible. Some of the online ads you are served may be based on the content of the Web page you're visiting or mobile device you are using; some others may be based on registration information you provide; some may be based expressly on your search history and other ads may be customized based on predictions about your interests generated from your visits to other Web sites. These companies may use techniques other than cookies to recognize your computer or device and/or to collect and record information on or off the [website you are visiting] or [mobile application you are currently using]. Please note that your web browser may not permit you to block the use of these techniques, and those browser settings that block HTTP cookies may have no effect on such techniques.

Who placed this ad?

• This ad was served by XYZ.

Where can I learn more about how XYZ selects ads?

• Please read about XYZ's privacy and advertising practices.

©2014BlueCava, Inc. All Rights Reserved

• XYZ may use your searches, demographics data, and location information to select the ads you see. To manage your location, please visit XYZ's Management page.

What choices do I have about interest-based advertising from XYZ?

• Manage interest-based advertising categories, or opt-out of all categories, from XYZ.
• Visit the Network Advertising Initiative and the Digital Advertising Alliance to see your opt-out choices from other participating companies.
Learn More!
• Find out about how online advertising supports the free content, products and services you use online.
• Understand your choices for online advertising from the Digital Advertising Alliance.
• Learn more about online advertising from the Network Advertising Initiative.
• Explore browser controls and plug-in tools to help set and maintain your privacy choices.

ENHANCED NOTICE & TRANSPARENCY

BlueCava is a member of the Digital Advertising Alliance, and we support the DAA's privacy principles. More importantly, we integrate seamlessly with Evidon in order to enable our partners to support Enhanced Notice (i.e., the DAA Ad Choices icon) as appropriate.

©2014BlueCava, Inc. All Rights Reserved

CHOICE

BlueCava respects consumer choice, and is supportive of privacy innovation around consumer controls. We provide multiple paths for consumers to opt-out: via BlueCava.com, via the Enhanced Notice mechanisms offered by DAA compliant technology partners, and via the DAA opt-out page. Moreover, BlueCava offers three primary implementations with respect to consumer choice mechanisms:

DAA Opt-Out Choice –BlueCava supports opt-out choice as prescribed by our industry trade associations, and is listed on the AboutAds.info opt-out page. Our technology is designed to be flexible: honoring the BlueCava opt-out, our partner's opt-outs, or both.

ID Rotation / Reset – This choice mechanism was popularized by Apple's IDFA, and is also supported by Google's Android ID. The premise behind enabling ID rotation is that many consumers recognize that advertising supports a free Internet, but have concerns regarding the use of persistent IDs for ad targeting. When the BlueCava ID is resent, we disassociate any information that is tied to that Device ID. By enabling consumers to exercise choice by rotating their BlueCava ID, BlueCava preserves our client's ad targeting capabilities on a going forward basis. To view and rotate the ID that is associated with your device, please visit http://bluecava.com/opt-out/.

Do Not Track – While DNT has been criticized by many for upsetting the competitive balance of the digital advertising ecosystem, BlueCava recognizes that DNT may ultimately become a de facto privacy standard. As a platform partner, BlueCava is agnostic regarding DNT, but is poised to support DNT if/when it emerges as a standard.

©2014BlueCava, Inc. All Rights Reserved

The Effectiveness of **BlueCava's Current Opt-Out Methods**

When BlueCava receives an opt-out request, that request syncs with the BlueCava opt-out database, where that device (and any devices our platform has associated with that device) is then opted-out. An opt-out cookie is set primarily for partner identification purposes, as BlueCava does not rely solely on cookies to identify a device. When BlueCava's platform encounters that opted-out device again, we will not share access to that device with partners or clients to use for targeting.

Persistency of the Opt-Out Mechanism

We recognize that device recognition is probabilistic in nature. As such, there is a risk that we won't recognize a consumer's opt-out choice the next time we encounter their device. In order to mitigate against that, BlueCava drops a 1st party opt-out cookie when users opt-out, as 1st party cookies are less prone to being blocked or deleted by browsers, or in certain mobile environments. Moreover, when cookies are deleted on a particular device, our systems will protect the opt-out choice by dropping another opt-out cookie so that this choice can be recognized by our partners.

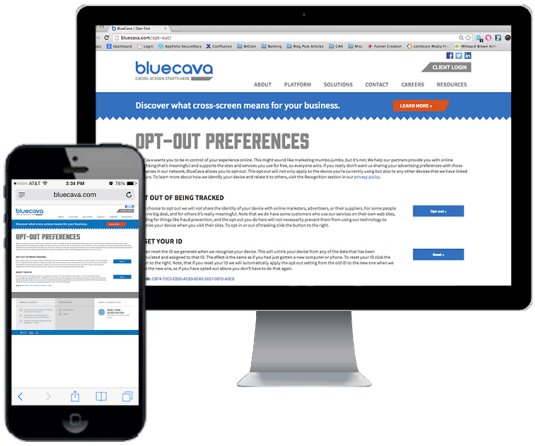
Similarly, BlueCava supports the opt-out protector tools offered by the Digital Advertising Alliance.

Please visit www.bluecava.com/opt-out to see BlueCava's opt-out mechanism.

©2014BlueCava, Inc. All Rights Reserved

TRANSPARENCY

Transparency is a privacy concept that has taken on greater importance in the digital age. BlueCava supports transparency by enabling Users to see the ID that is associated with their device by visiting http://bluecava.com/opt-out/.



As shown by the graphic above, consumers have access to their BlueCava device digital ID and the ability to reset the ID. We believe that utilizing device ID rotation is in line with the approach championed by Apple's mobile IDFA identifier that has been well received by privacy advocates and regulators. The tangible privacy benefit of creating an ID rotation mechanism is that it cuts at the persistence of digital ID's, which is one of the primary objections raised by advocates when it comes to device identification technologies.

CONCLUSION

BlueCava takes privacy concerns seriously, and strives to aid the industry in establishing innovative, and consumer-centric policies. This document was designed to help interested parties better understand how BlueCava addresses key privacy concepts and provide some perspective on why device recognition is a necessary element to the continued growth of digital advertising.

Device identifiers and other non-cookie based attribution technologies are being created, and will be created in the future. The only question is: who gets to create them? The importance of having independent (i.e., not created solely by large companies within the marketplace) device identification is essential to a vibrant ad supported marketplace. BlueCava will be a trusted partner to help DSPs and other third-party Adtech partners as the industry moves into a post-cookie world.

BlueCava has adopted a privacy by design approach that incorporates key concepts espoused in the Fair Information Practice Principles. We will continue to innovate on privacy in order to be a safe and trusted partner.

Please reach out to privacy@bluecava.com with additional questions.

©2014BlueCava, Inc. All Rights Reserved