PLAYBOOK:

ALIGNING REGULATORY COMPLIANCE & USER EXPERIENCE

admonsters | geoedge Add Integrity

INTRODUCTION

If digital media monetization was as easy as hooking up a slew of page placements to programmatic demand sources and just watching the revenue roll in, all of our lives would be far less stressful. We also probably wouldn't have jobs.

No, there is a nuance to digital media monetization—dare we call it an art? Understanding the ins and outs of ad servers, exchanges, and supply-side platforms is only a part of the job. What you might call the softer side of operations is ensuring that digital advertising and the mechanics behind it such as data collection and processing do not significantly detract from user experience.

This year, the softer side gained a harsher edge as the European Commission's General Data Protection Regulation (GDPR) came into effect, codifying the collection and processing of personal data for persons in the EU. The law applies globally, meaning any company with data operations—including publishers—affecting people in the EU must be in compliance. In addition, the state of California passed a similar law that will affect companies that interact with 50,000 citizens of the highly populous state.

However, instead of viewing these regulations as another burden, publishers should look at them as opportunities to dramatically improve user experience. The push towards opt-in consent for data collection and processing has been a long time coming, and should help mend the fractured relationship between media companies and their users.

This playbook will dive into the details of GDPR and why best practices for compliance are also overall user experience and privacy concerns. We'll also examine the ramifications of the California Consumer Privacy Act and movements toward regulation at the federal level. Finally, the playbook will tie privacy regulation compliance back to other revenue team user experience responsibilities, such as ad quality and malware prevention.

WHAT'S A PLAYBOOK?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for more than 19 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.

THE GDPR EFFECT

When the history of digital advertising is written, May 25, 2018—the day the EU's General Data Protection Regulation (GDPR) went into effect—will likely be considered a turning point for the industry. No longer is respecting the data privacy of users simply an ethical practice—rules for the collection and processing of all personal data have been officially (if a bit confusingly) codified with severe consequences for violators: up to €20 million fine or 4% of annual worldwide revenue.

The most interesting part of GDPR may be its global implications. The data protection protocol applies to "natural persons" within the European Union—this means any individual within an EU member country, whether they are a citizen or not. The regulation's purview is not limited to EU entities, but any global company that offers goods or services (including web content) to natural persons in the EU or monitors their behavior.

In effect, GDPR established a virtual minimum level of regulated data privacy protection worldwide, and other countries and regions seem to be following suit. On the day of activation, many American publishers served stripped down sites or simply blocked content to traffic coming from Europe. But this is not a long-term solution, particularly as a more rigid California law is set to go into effect in 2020 and federal data privacy regulation seems inevitable.

Therefore, understanding and complying with GDPR is a baseline as you prepare for potentially harsher regulations. Steps such as establishing the consent process, employing a Data Protection Officer, and ensuring all vendors you work with are known and within the consent framework are not only publisher best practices, but also keys to staying on the sunny side of GDPR. In addition, GDPR compliance offers your users more assurance that you're looking out for their data and not trying to take advantage of them.

Instead of being afraid of a Data Protection Authority bringing the GDPR hammer down, publishers should embrace the methods proffered by the regulation, as they provide great guidance in the face of the unknown data privacy future and offer a model for a better user relationship.

GDPR TOP FINE:

€20 Million or 4% of annual revenue, whichever is greater.

GDPR BASICS

Going into effect May 25, 2018, the General Data Protection Regulation (GDPR), is a data protection protocol appling to “natural persons” within the European Union, which includes any individual residing within an EU member country, whether they are a citizen or not. Any global company that offers goods or services to natural persons in the EU (“data subjects”) or monitors the behavior of data subjects.

- GDPR regulates the processing of personal data; processing is an umbrella term for collection, recording, organization, storage, alteration, and dissemination.

- Acceptable purposes for processing are very vague due to the wide scope of companies falling under GDPR. Article 5(b) 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.” The article further states that this collection should be limited where possible, and stored no longer than necessary. It seems the supervisory authorities will have ultimate judgment here.

- Personal data includes what has been generally considered personally identifying information (PII)—e.g., name, email address, phone numbers—as well as “one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” This concerns most online data collected from users by websites and other Internet technology companies, and definitely behavioral or interest data—discerning or deducting characteristics from personal data is labeled as profiling.

- Personal data may only be processed if the data subject offers clearly informed explicit user consent—according to the language of the act, a “freely given, specific, informed and unambiguous indication” via a “clear affirmative action.”

- A data controller is the entity that determines the purposes and means of processing, while a data processor is the entity that performs the processing—you could think of the latter as the tool or service provider. Data controllers can be held liable for the actions of data processors.

- Consumers must have a process for viewing, correcting, and potentially deleting personal data.

- If a processor is found in violation of GDPR, the controller can be held liable.

- Each EU member country has its own Data Protection Authority (DPA) that monitors compliance with GDPR via audits.

- Penalties for violations can go as high as €20 million or 4% of annual worldwide revenue, but will be relative to the DPA’s judgment regarding the severity of the offense. In addition, there is a corrective period for companies to steer themselves back into compliance.

"The Unspoken Handshake" is how AdMonsters has long referred to the silent agreement between publishers and their audiences—the publisher gives a user access to content in exchange for allowing advertisers to vie for their attention; and enabling publisher data collection and monitoring of user activity. This data can be leveraged for a variety of purposes, including targeted advertising.

While site privacy policies usually detail this arrangement, and the EU's EPrivacy Directive of 2011 demanded websites display these practices upfront, industry policy has long been an opt-out mechanism. Gaining opt-in consent from your audience for you and your service provider partners to use "personal" data is one of the key tenets of GDPR (and the California Consumer Privacy Act, detailed later).

There's a high probability opt-in consent will become the standard for privacy policies to come, and it's frankly a good practice for user experience. In this increasingly connected era where consumers are wary about intimate data being casually tossed about, it's a sign of respect to ask visitors for consent before processing their data.

But what if you don't get consent from the user? According to GDPR guidance, you cannot to deny users content if they refuse to consent. In the initial days of GDPR's activation, some US publishers bypassed this rule by blocking content to all users coming from the EU—consent was never asked for.

Instead, you can go old school and serve those users ads that don't rely on targeting based on behavioral or personal data. It's no surprise that publishers and advertisers alike are showing renewed interest in contextual targeting, which has advanced by leaps thanks to machine learning technology.

IAB CONSENT FRAMEWORK

IAB Europe and IAB Tech Lab came up with the GDPR Transparency & Consent Framework where publishers, digital advertisers and ad tech companies can more easily comply with the privacy policy. The Framework helps publishers tell visitors what data is being collected and how they and their vendors plan to use it—and which vendors are using it. It also helps to obtain consent or denial for each item as necessary and then makes sure that the user's consent is communicated throughout the ad ecosystem.

There are already 350 registered vendors on the Global Vendor List (Google was a notable exception at the time of

HIDDEN UPSIDES?

While GDPR initially hit the European programmatic markets hard, several publishers we have talked to reported that they've seen a boost in eCPMs in Europe. They attribute this to thinned out data resources (particularly third parties with sketchy sources) and effectively made publisher first-party data more valuable. In addition, contextual considerations have higher priority for buyers in terms of targeting.

publication) and over 100 registered Consent Management Providers. And now that specifications for the Framework for mobile in-app have been released, providing support for publishers to whitelist vendors, the addition of thousands of publishers is expected.

With the Framework in place, users will receive a popup or some other communication through a publisher's site that reveals what data is being collected, how that data is being used and who is using it—and then ask for consent. Once consent is given, the consent is stored as first-party cookies and a vendor on the list can serve ads to the user.

If all works correctly, a bid request will contain consent flags about the user with targeted ads only using the data that was consented to. Consent can be specific to that one publisher or across the web, so that users don't have to provide consent multiple times.

Most important, the user's consent communicates legit interest in interacting with advertising targeted to their location or demographic or other such variables.

DO YOU NEED A CONSENT MANAGEMENT PLATFORM?

Providers of Consent Management Platforms (CMP) are cropping up rapidly to aid publishers in managing consumer consent in relation to how their data is collected, used, and transmitted across the advertising ecosystem.

GDPR compliance (and soon CCPA) has been the driving force behind the rise of CMPs over the past year, and especially more recently with the launch of IAB's Consent Framework. CMPs can help publishers present opt-in or opt-out information to site visitors regarding how their data is being collected and for what purposes. These consent forms will also offer users a peek into the companies that are processing/have access to their data.

Most important, CMPs should be able to add new IAB authorized vendors to the consent form and share consent information with other technologies in the ad tech stack. For global consent, a CMP should be able to pass consent throughout the ad ecosystem. Google has its own consent system, so a CMP that also makes those consent options available might be a good choice.

Of course a publisher could decide to in-house their CMP since they already collect personal data for ad targeting—but consent gathering would have to be fully transparent and pass data throughout the already complex ad ecosystem. Getting consent is vital to thriving as a publisher in today's current data privacy climate, so working with a vendor who can guarantee compliance should be high on the list.

VENDOR CERTIFICATION

In the new privacy age where publishers can be held liable for the actions of their downstream partners, knowing and documenting every vendor running on your site is no longer a best practice or a luxury—it's a necessity.

Every publisher should implement a vendor certification program, or strengthen their current one. At the very least, this should include company address, up-to-date information on the chief point of contact, and written description of the function provided by the vendor. A rigid program should also test tags and code to ensure they act in the way documented by the company (and don't do anything unexpected) as well as get signoff by your legal team.

It's simple enough to create a standardized form for acquiring necessary information. Some publishers have actually created online portals allowing vendors to seamlessly pass information.

Advertisers are notorious for abruptly adding vendor code to campaigns, and publishers have sometimes let un-vetted vendors slide in order to seal a deal. Now more than ever, you need to present a solid front on vendor certification—inform your advertisers it's a necessary legal protection for both of you.

4 GDPR ENFORCEMENT & COMPLIANCE

What enforcement will look like for GDPR—as well as CCPA and other state laws—is still a mystery. Fines have yet to be doled out, but the test cases as of this report's publish date show what many industry commentators have speculated: the DPAs are most concerned about the intent to comply with GDPR. Good faith attempts to stay on the right side of the regulation go a long way, and the DPAs appear to be accommodating in terms of corrective periods.

The violations so far have mainly been reported by the French DPA, and suggest that different countries are likely to interpret the regulation in their own manner. However, infringements surprised some because the companies called out were relatively small. This demonstrates that DPAs will go after fish both small and large, and no one is too tiny to escape scrutiny. Doing nothing towards compliance and praying you stay off the DPAs' radars will come back to bite you if (when?) you get caught.

But in general, viewing GDPR compliance as a burden is the wrong attitude. Establishing a process for managing user consent and installing a Data Protection Officer to ensure the company is in compliance both with regulations and internal data privacy policies are solid practices, and fundamental preparation for future privacy regulation we all know is coming.

EPRIVACY REGULATION

Did you think GDPR was the end of EU data privacy laws? Maybe, maybe not!

As a supplement to GDPR, the EPrivacy Regulation is supposed to replace the EPrivacy Directive of 2011. The ramifications of this regulation have many in the digital advertising community nervous, as it focuses on the privacy of personal communications and online consumer tracking as well as the collection and processing of behavioral data. It could potentially have a greater impact on the digital advertising space than GDPR.

If it ever passes, or even finished. The original reform proposal was drafted in 2017, but since then member states have not come to a consensus on the final regulation. Reportedly, they are quite divided as ad tech lobbyists and consumer data advocates have sparred relentlessly.

When GDPR went live in 2018, the EPrivacy Directive was planned to go into effect in 2019. As of the publish date of this report, 2020 is the new aspiration for activation.

U.S. DATA PRIVACY REGULATION

CALIFORNIA CONSUMER PRIVACY ACT

With the passage of the California Consumer Privacy Act of 2018, consumers will get a lot more visibility into the information collected about them when they visit online properties, as well as what is done with that data.

Set to go into effect January 1, 2020 with enforcement coming six months later, CCPA will apply to any company with CA-based assets or customers, including Californians who visit a website and whose data you touch. To sum it up, the law will apply if you have 50,000 unique CA visitors annually. For digital media companies, this will mean rewriting privacy policies, tinkering with data management systems, and providing more transparency to consumers.

Overall, the Personal Identifiable Information (PII) defined in CCPA is much broader than what's been outlined in GDPR—"information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This includes IP addresses, cookies, beacons, pixel tags, mobile ad identifiers, browsing history, search history, and geolocation data.

Companies will need to ask for consumer opt-in and divulge which categories and specific pieces of personal data are collected, as well as sources about how those categories were built, the purpose for which their data was collected, where the information comes from, how the information is used, and whether the information is being disclosed or sold. Chief here is the last point—publishers must have a homepage link to a page called, "Do Not Sell My Personal Information."

You must also provide access to the data collected as well as enable portability and the ability to delete personal information (and instruct service providers using the data to delete it as well). You must also honor opt-out requests and cannot attempt to re-authorize until 12 months have passed.

Noncompliance with the law—and failing to secure the data you collect—could be met with some serious costs—$2,500 fine for each violation after a 30-day "cure period"; $7,500 for each intentional violation of the act.

The law is clearly aimed at third-party data brokers, and the people that buy their wares—and many publishers buy third-party data to help with targeting and meeting demographic guarantees. Companies with direct relationships with consumers—such as digital publishers—will likely see less of an enforcement impact, but publishers could probably easily find themselves on the wrong side of this privacy regulation. In addition, the California Attorney General's prerogatives are not entirely knowable.

The fines wouldn't be the only loss for companies not in compliance. Under some circumstance, consumers will be allowed to sue companies when their non-encrypted or non-redacted personal data has been accessed without authorization, theft, exfiltration, or disclosure of a security breach. The threat of class-action lawsuits may actually be more perilous to publishers.

The CCPA was already amended with technical fixes in the fall of 2018. Many in the digital advertising industry expect further revisions as questions linger around enforceability, but this makes it difficult to prepare for compliance and the clock ticks down.

WHAT ABOUT THE FEDS?

In the wake of GDPR and CCPA—as well as a data broker law passed in Vermont and proposed legislation in New Jersey—major tech companies like Apple, Google, and Amazon took to Capitol Hill to lobby for federal consumer privacy safeguards. In particular, the companies feared a "patchwork" of widely varying state laws could seriously hamper business and innovation. Notably, they also argued against mandatory consent opt-ins along the lines of GDPR.

Even the IAB, long an advocate for industry self-regulation, sent a letter to congress advising that "A uniform Federal privacy standard could provide clarity, market certainty, and add fuel to future innovation, while preserving the value and benefit that online advertising brings to the internet ecosystem."

In November, the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce released comments it had received on a proposed digital privacy framework that would balance user privacy and innovation goals. Notably... build off the blueprints of successful "risk-based" data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA). To some extent, the effort sounds like a codification of the Digital Advertising Alliances Self-Regulatory Program.

While some kind of federal data privacy regulation that will supersede state privacy regulations now seems inevitable, the real question is timing—will (or even can) it come into force before CCPA is active on Jan. 1, 2020?

COPPA & HIPAA

The running joke is that there is no data privacy regulation—not even self-regulation—in the Wild West of the U.S. But that's not close to true—the U.S. has long had very strict regulations regarding handling data for children and the management of health-related data that overseen by the Federal Trade Comission

The Children's Online Privacy Protection Act (COPPA) regulates data collection from users younger than 13 years old, and applies to all websites, mobile apps, and online commercial services. Services and sites collecting data provide parental/guardian notice and obtain consent (as well as the right to prevent collected data from being shared with third parties) for data sharing, particularly when used with "persistent identifiers" (e.g., cookies, logins).

The Health Insurance Portability and Accountability Act (HIPAA) restricts health-care and other related sites from offering targeting that could potentially identify a patient— protected health information (PHI). The University of California at Berkeley lists 18 potential identifiers, including common PII such as names, phone numbers and addresses to full zipcodes, IP addresses, and device identifiers.

DATA RECOGNIZED AS PERSONAL IDENTIFIABLE INFORMATION BY CCPA INCLUDES

IP addresses, cookies, beacons, pixel tags, mobile ad identifiers, browsing history, search history, and geolocation data.

UX BEYOND PRIVACY

Of course revenue specialists have user experience responsibilities beyond securing users' data privacy—chiefly seeing that ads do not negatively affect user experience. That covers a wide spectrum, from ensuring ad formats and creative don't irritate users to making sure their devices aren't infected with malware.

THE COALITION FOR BETTER ADS AND THE INITIAL BETTER ADS STANDARDS

Thanks to the Coalition for Better Ads, publishers have a good baseline for determining what ad formats are generally deemed acceptable in digital media. The Coalition does have a powerful enforcement system: the widely used Chrome browser of prime member Google actually blocks creative that doesn't meet the standards from loading.

Ad blocking has grown significantly over the past few years, costing publishers billions of dollars. While desktops and laptops remain the prime devices where people install ad blockers, mobile ad blocking has become increasingly common. Publishers have tackled the challenges of ad blocking by asking or requiring visitors to disable ad blockers in order to see content, and overall ad quality has gotten a lot better and a lot less interruptive. But still, people are choosing to block them.

That's where the Coalition for Better Ads comes in—comprised of 16 companies and trade groups, including the Interactive Advertising Bureau (IAB), the American Association of Advertising Agencies (4As), Association of National Advertisers (ANA), Google, Facebook, Microsoft, P&G, Unilever, App Nexus, Criteo, and others—with a load of research on why users block ads, as well as a set of standards to make a more user friendly ad experience for users on both desktop and mobile.

CRYPTOJACKING: THE NEXT BIG MALWARE THREAT?

In-ad cryptojacking is becoming a real big problem for consumers, publishers and advertisers. The malware threat secretly inserts itself onto a users device through a website or embedded advertising, images or videos that are infected with JavaScript code that automatically runs once loaded.

The code hides itself on the user's device so it can take over their browser and use the device's computing power to mine cryptocurrencies like Bitcoin, potentially harming the device and network servers as well. All the while, the code runs in the background, virtually undetected by the user.

Cryptojacking code has been found on a number of reputable websites, including cable network operator Showtime and YouTube.

The Initial Better Ads Standards (IBAS) goes into detail about which ad experiences should be avoided, such as popup ads without user initiation, auto-playing video ads with the sound on, pre-stitial ads with countdowns, large sticky ads on desktop, ad density higher than 30%, flashing animated ads, and full-screen scroll over ads.

To that end, the Coalition has created a Better Ads Experience Program for the European and North American digital media ecosystem with the hopes of gaining industry-wide adoption of the Better Ads Standards. The organization plans to accredit ad tech companies and browsers that filter ads based on the standards and who assess publisher compliance. Publishers who agree not to use aggressive and disruptive ad practices will be certified.

Google's Chrome Browser is already blocking ads that aren't falling in line with the standards and violations of the Standards are being reported to sites. Publishers can submit their sites for review once the violations have been fixed. This will be standard practice for any organization that is a Program participant.

BATTLING MALWARE

The big malvertising story for much of 2018 was redirects, particularly on mobile. Typically launched around weekends to try to catch ops teams off guard, redirects have become the bane of both publishers and their users.

Real-time creative blocking has helped publishers in this battle enough that it's increasingly being seen as a table-stakes offering for your ad quality partner. Here, malicious, offensive, and low-quality ads are blocked in real time on the pre-impression level, long before any damage can occur. However, real-time creative blocking is only as good as the detection behind it. The actual blocking itself is the easy part of the technology; the most important aspect is to know what should – and what should not – be blocked. The ideal real-time creative blocking should not only be based on malicious IP blacklist, but needs, in addition, to focus on behavioral patterns so it can catch the so-called zero-day attacks.

What is also critical here on the programmatic front is "partner hygiene." As many publishers are consolidating their demand partners following the header bidding boom, the onus is increasingly on the SSPs and exchanges to ensure no malware comes through pipes. In effect, those players are becoming more stringent about which DSPs and buying platforms they work with to minimize potential liability.

Publishers should use their leverage here—demand only clean (and quality!) creative comes through the pipes. Certain real-time blocking solutions, like GeoEdge, help you benchmark the ad quality supplied by each of your partners. After all, there's enough demand for your premium inventory out there that you can be choosy—you have standards, after all!

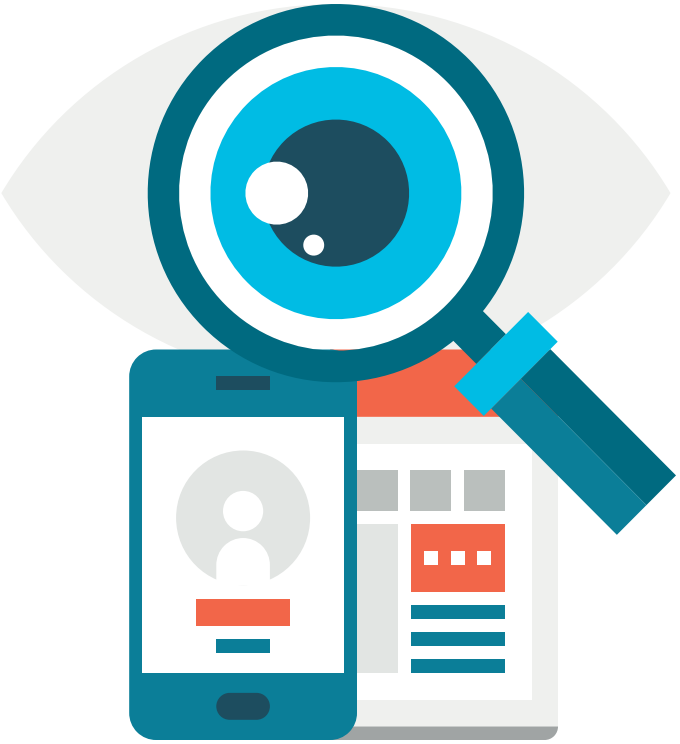
BEST PRACTICES

- Team up with product to examine ad experiences, including how slow load times and various formats affect user behavior.
- Strongly suggest your advertisers follow the IAB's LEAN principles, but demand that they abide by your specific specifications. Show them examples of how heavy creative or too many calls actually dampen viewability rates.
- Particularly on mobile, consider lightweight native formats that match a publisher's aesthetic. Not only do these load fast, they tend to have better favorability and engagement from users. But don't forget to make sure your users are not ending up on malicious sites after clicking on your native banners.
- Employ a real-time creative blocker against malvertising and low ad quality, but don't stop with just blocking. Make sure you can use the same monitoring technology for BI purposes, so you can make strategic decision on which partner to work with.
- In programmatic, higher floors tend to scare away malvetisers looking to scrape the bottom of the barrel.

WRAP-UP: THE BRIGHT SIDE OF DATA PRIVACY

The buildup toward GDPR's launch was filled with dread due to a lack of guidance from the European Commission (it did not arrive until December 2017) and general confusion over proper compliance. Even at the end of 2018 there is much uneasiness over the regulation simply because we have yet to see major enforcement—the violations so far have been minor and quickly corrected.

This distress has obscured the many benefits of the law for publishers. First off, GDPR is a giant plug for data leakage as unsavory data scrapers will have a harder time plying their ill-begotten wares. In effect, this increases the value of first-party publisher data that was collected with consent. With less third-party data to lean on, advertisers will be willing to cough up more cash to leverage quality publisher data.



But perhaps the most important and overlooked benefit is that it's a big step toward re-establishing trust between publishers and consumers. Consumers understand that online content is not "free," but how publishers and their partners use data gleaned from visits is not wholly transparent... It's arguably pretty obtuse.

Industry self-regulation only goes so far in relieving consumer anxiety, and opting out of targeted advertising and tracking tended to drop them in web-based labyrinths. Savvy browsers simply adopted ad blockers. Data privacy regulations that demand opt-in consent will win back consumer confidence because they replace the unspoken handshake with an actual informed conversation.

Safeguarding data privacy is a responsibility toward users, alongside ensuring ads don't overly detract from content and preventing malware attacks. So don't think of user data privacy efforts as mere regulatory compliance; think of them as a service to your audience.

ABOUT ADMONSTERS

admonsters

AdMonsters is the global leader in strategic insight on the future of digital media and advertising technology. Through our conferences, website, original research and consulting services, 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

ABOUT GEOEDGE

GeoEdge is the premier provider of ad security and verification solutions for the online and mobile advertising ecosystem. The company ensures high ad quality and verifies that sites and apps offer a clean, safe, and engaging user experience.

With GeoEdge's detection and real-time blocking of malicious and low quality ads, you can be confident knowing your users are continuously being protected against non-compliance, malware (malvertising), inappropriate content, data leakage, operational, and performance issues.

Leading publishers, ad platforms, exchanges, and networks rely on GeoEdge's automated ad verification solutions to monitor and protect their ad inventory. To find out how GeoEdge can enhance your quality assurance and verify your online and mobile campaigns, head to www.geoedge.com.

sponsored by: