adMonsters

playbook:

User Experience

sponsored by: THE MEDIA TRUST

1 Introduction

The prominence of revenue operations (ops) as a critical function within the digital media world has had its ups and downs. While programmatic and other indirect channels have proven ops as a serious revenue center, it's also forced the department into highly unfamiliar territory such as creative development and user experience. And this more prominent role attracts the interest of other groups across the organization such as legal, IT/security and privacy/risk.

AdMonsters has long noted that ops professionals are the gatekeepers at digital publishers when it comes to advertising—nothing gets on the page without their (sometimes forced) approval. However, the the digital advertising industry is at a unique intersection: publishers' revenue teams are eager to try any and every monetization resource as traditional digital revenue streams wane; however, creative has also never had such a high potential to be annoying, intrusive, alienating, downright threatening (e.g., malvertising) or prohibited (e.g., violating government regulations).

The situation is exacerbated by the disconnect between advertiser goals, publisher capabilities and audience acceptance. In response, digital readers are increasingly embracing ad-blocking extensions across platforms and governments are penalizing non-compliant activity.

While it may not seem intuitive, ops must do more than act as site gatekeepers who only follow publication-specific quality assurance guidelines. They must also actively analyze and strategize around how specific revenue efforts affect user experience.

This includes protecting the end user (and the site) from malware and other security concerns; validating all tech partners involved in advertising on the site; ensuring ad creative meets a certain standard; mediating the effect of ads on site speed and page weight; and complying with federal regulations around data privacy and other matters.

This playbook will examine these areas and more in an effort to help ops form an optimal user experience strategy.

What's A Playbook?

A playbook is an extension of what the AdMonsters community has been delivering at our conferences for more than 14 years. A playbook solidifies what has made our events a "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, "crowdsources" a document that outlines best practices on a specific topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy. This document intentionally does not get into specifics around individual solution providers.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too generic. 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 version of this playbook will start to take shape and, with additional contributors, grow in both depth and breadth. Publication of future versions will be scheduled based upon the needs of the community.

User Experience: Ops' New Problem

We know what you operations professionals may be thinking: "Whoa, user experience isn't in my job description." Sorry, it most certainly is—over the years, though, we've given this task names like "quality assurance"; "creative control"; or "ad upkeep." Similar to the print world, the onus has been on publishers to assure the quality of ads running on their properties is consistent with the quality of all other content.

However, we're not just concerned anymore with malfunctioning pieces of rich media that don't meet specs or errant Flash creative delivered via ad networks. Publishers are increasingly leaning on programmatic channels for revenue, which presents some serious QA challenges beyond the scope of ensuring the ads run properly. The annoyance potential of video is palpable with autoplay and sound, while the outstream format can easily be overused. Though they are essentially more secure than their Flash brethren, HTML5 ads are proving heavier and lumbering. Oh, and did we mention the amount of malware out there is higher than ever?

Quality assurance has migrated into user experience, which before typically fell into the realm of designers and developers. Not any more. In addition to verifying ads meet a certain quality standard, ops must also ensure that the ad experience does not detract from the overall site objective nor run afoul of regulations.

You already know what happens when you fail—malware slips in the door, negative media coverage abounds, regulators come after you with fines, and your slighted audience abandons you for other sites and/or turns on ad-blockers. Any dark path you travel down, the final destination is the same: monetization efforts are harshly affected.

Prevention is the best medication for all these symptoms—shield yourself against malware, follow the line of the laws, and don't give users an excuse or even a desire to add a blocker. The drag? While there's a lot of guidance on various aspects concerning user experience, there are very few standards to follow. Therefore, ops must develop a user experience strategy that addresses advertising and monetization angles (e.g., data collection and transacting), and by working with other departments, confirm this strategy complies with publisher policies and various government regulations.

We've broken down these responsibilities into four essential categories:

- **Security and Malware prevention**
- **Partner Verification**
- **Creative Control**
- **Regulatory Compliance**

User Experience:

A person's perceptions and responses resulting from the use and/or anticipated use of a product, system or service.

Source:
International Organization for Standards (ISO), ISO 9241-210:2010A

How Much of a Problem Is Ad Blocking?

The true cost of ad blocking to publishers is unclear. While Adobe and PageFair's 2015 headline-grabbing report suggested that ad blocking would lead to $22 billion in lost revenue that year, their methodology was widely disputed. It's hard to judge an exact revenue effect because if all those blocked ads were served, they likely would have driven down the price of other impressions.

While a 2015 IAB survey suggested that 26% of desktop users turn on ad blockers, the majority of AdMonsters' premium publisher base puts their percentage of blocking traffic between 10% and 15% (with notable outliers such as sites focused on video games). These numbers are still cause for concern, and most publishers are at least monitoring the amount of traffic coming through that employs an ad blocker.

Security and Malware Prevention

Malvertising—malware delivered via digital advertising—is pervasive across the Internet and an ever-growing problem. The Media Trust has seen the rate of ad-related malware incidents double every year for the last several. Security is a major reason users and corporate networks embrace ad blockers—if no ads are served, they reason, malware can't slip through. (Actually, it can.)

Malvertising is not just a problem for the long-tail; The Media Trust confirms that a significant percentage of malware attacks occur on "premium publishers," or popular sites with legitimate, high-volume traffic. They are at risk of serving malware from both programmatic channels as well as direct sales. Every few months or so the media reports how a publisher revenue team, blinded by a big check, overlooked a buyer's inventory quality and served a guaranteed campaign riddled with malicious content.

Ops' first and foremost role in user experience is keeping malvertising out. Fortunately, industry awareness of malvertising has grown and the onus is no longer singularly and squarely on publishers to stop the threat. Since we can now better trace outbreak sources, exchanges and other ad tech partners have become more vigilant about scanning lest they gain reputations for spreading malvertising. (Even agencies are jumping on the prevention bandwagon). In fact, the Trustworthy Accountability Group (TAG) recently introduced best practices for malware scanning of creative and launched an anti-malware certification program.

Alas, the publisher is still the last stop before the user, so your level of protection must be formidable. There's no way for a publisher to escape blame for a malware attack, so a blanket block is the only solution.

Tips for tackling ad-based malware:

- **Check third-party code:** Third-party code on a site—of which there is often plenty—is not to blame for malware attacks, but not understanding which third-party code is running on the site can open the doors to malvertisers. Ops must make a point to identify and monitor all third-party code executing on the site and communicate it to IT.

- **Execute continuous scanning:** Ad servers have tools that scan creative for malicious code; the scanning must be ongoing because code can be changed during campaign flight. Sometimes a miscreant will insert after the campaign kickoff because they think your guard is down. In addition to shielding you from malware, a media scanner can provide insight into all third parties operating on your site, including an audit trail for activity. Certain providers also enable blocking of restricted vendors.

- **Leverage malware expertise:** There's nothing wrong with added security—a third-party scanner can be quite advantageous. Your ad server's main job is to help decision and serve ads; employing a company that specializes in malware prevention could be the extra layer of protection that saves your hide. The provider must warn you of malware in real-time or actually block the malicious code from appearing on the site.

- **Quickly remove malware:** Ops must take immediate action when detecting or being notified of malware. This is imperative when it comes to programmatic channels as delays can be costly from monetary, brand and regulatory perspectives.

- **Review tags and landing pages:** If you didn't have enough trouble with advertisers stuffing a boatload of tags onto every creative, you also have to make sure the tags are clean. Yup, malware can be hidden both in creative files as well as tags, so your provider must hit the tags as well. And sometimes both of those can be clean and it's the advertiser landing page that's rotten. Don't skimp in checking these items for direct-sold campaigns, and continuously scan as they can be shifted mid-campaign.

- **Don't forget mobile:** Think you're safe on mobile? WRONG! Mobile is the most personal of all devices, which is exactly what bad actors aim to leverage. Because publishers are leaning heavily on networks and exchanges for mobile monetization, you have to be extra watchful that malvertising doesn't sneak in.

- **Certify your buyers:** Be careful of buyers you don't know and vet every new advertiser that comes sales' way. This means ensuring they boast legitimate domains and email addresses. If the potential advertiser's site is hosted in a country different from the one in which the company is based, or if the domain registrant's contact information is hidden, suspicion is warranted—and you should probably turn down the money. Potential fraudsters will try to impersonate legitimate advertisers, but facades often crash with a bit of due diligence.

- **Create vendor verification guidelines:** More about this in the next part.

Have A Recovery Plan

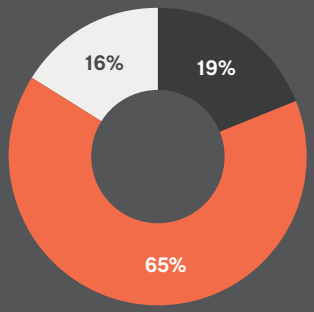
Even with the most powerful shield, malvertising will find cracks and seep through. Malware developers are a clever lot, constantly tinkering with and enhancing their product. So although it may hurt your ops pride, you need to have a blueprint in place to deal with a malware breakout.

- Your scanning must quickly help you identify where the malware came from so you can shut down the source.

- Your customer support division should have a response plan for audience questions, which includes a list of questions to get user assistance in finding the culprit.

- All departments within the publisher should be notified of the outbreak as it may affect other site operations. Be sure to update them regularly on your response efforts.

How knowledgeable are ops professionals when it comes to malware?



- **Very well informed - 19%**
- **Somewhat informed - 65%**
- **Not well informed - 16%**

Source: "The Perceptions and Realities of Malvertisingin the Digital Publishing and Advertising Industry," ExchangeWire Research and The Media Trust

Short for *"malicious software,"* malware comes in many styles.

Worm:
A code that replicates itself and spreads to other computers.

Trojan Horse:
A downloaded file that misrepresents its purpose, usually allowing a perpetrator or perpetrators back-door access to private information.

Spyware:
Software that sends information on a user and his/her actions to another party without the user's knowledge.

Adware:
Creates ad placements on web pages and serves campaigns that generate revenue for the malware owner.

Ransomware:
"kidnaps" a computer by freezing it or locking out a user; the only way the user can regain control of his/her data is through paying the culprit. The FBI and FTC are quite concerned about the rise in ransomware, and the FTC is considering enforcement actions on companies that fail to adequately protect users.

Bots:
A significant percentage of ad fraud occurs through non-human generated impressions executed by bots. These bots are surreptitiously appended to campaigns, both legitimate and illegitimate, to drop on consumer devices.

5 Partner Verification and Sourcing

You don't need to look at an updated ad-tech LUMAscape to know there's a lot of intermediaries clogging up the path between advertiser and publisher, and it may seem like your agency clients want to use every one of them.

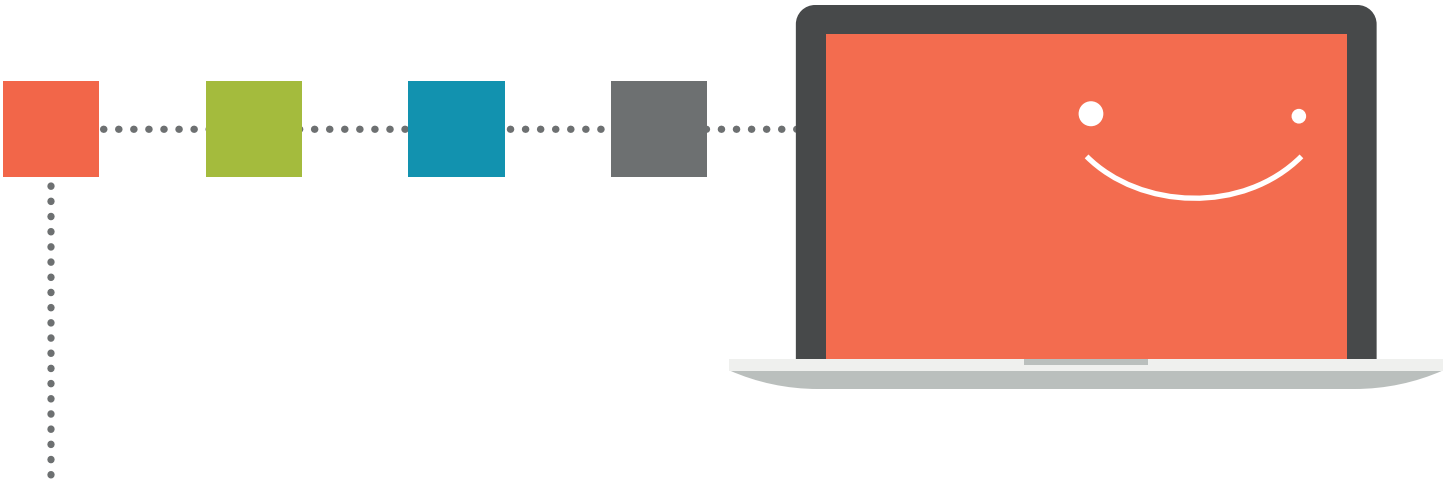
Campaigns often feature tags and/or pixels from data management platforms, verification providers, viewability measurement sources, attribution modelers and a host of other services. On the flip side, publishers are regularly adding header bidding providers, reporting consolidators and various other point solutions such as ad-block detectors.

Any of these third parties has the potential to ruin a user's day, whether it's through malware delivery, illicit data collection, data drainage on mobile devices or our old friend latency.

If your site is like an exclusive club (and we hope you treat it that way), you're not going to let just anyone through your door. Yes, we're talking about a vendor certification program. Any third party that wants to run code on your site must seek your approval first. Advertisers—or any other upstream player—cannot use a vendor's services on your site without letting you dole out some due diligence.

Knowing exactly who is executing on your site is key to sourcing creative and tag troubles—when a situation goes belly-up, it will be much easier to track down where and what went wrong.

A certification application can simply be a PDF or, if you're old-fashioned, a paper form sent over by the fax machine (just blow the dust off or it gets finicky). Some publishers that work with a plethora of providers actually host the registration form on an online portal.



A partner certification form should collect:

- **Complete company contact information including websites (domains).**
- **References/partners so you can ensure this is a legit service and not some fly-by-night operation. In addition, you should do some checking on CrunchBase and with fellow publishers to see if said vendor has a bad reputation.**
- **Support or operational contacts so you can immediately address any problems that appear with the correct parties.**
- **Documentation on what the vendor is doing and a brief explanation of how this information should be shared with other departments such as IT, development and site security so they can judge whether the vendor's code will have unwanted side effects.**
- **Partner's intention to uphold the site's data and privacy policies; if they violate them, you have a paper trail that proves they knowingly ran astray.**

Upon receipt of the completed form, verify and share the information with your legal department so they can confirm you're not skating any regulatory issues or tripping into a privacy sinkhole.

Certifying partner relationships is not a simple task. With programmatic channels, it can be difficult to tell just where an ad actually comes from let alone the vendors at play. In addition, sometimes a great but time-sensitive direct deal will come through the pipeline, leaving you without enough time to evaluate and certify the vendors. What's important is to thoroughly vet as many upstream partners as possible, starting with the most strategic.

You must assert as much control over what hits the site as possible—preventive medicine is all about stopping issues before they become problems.

Creative Control

Everyone plays a role in bad creative, from the advertiser to the agency to the (often too many) ad tech providers to the publisher. Getting everyone to accept their fair share of responsibility may seem like a Sisyphean task. However, there's a lot you can do from the publisher side to moderate the situation, including being rigid with ad specifications, controlling the type of ad units allowed, carefully choosing the number of ads on a page, and more.

How Many Ads Are Too Many?

The rise of viewability-based transactions has been good for user experience as it's made publishers cut down on the often-overwhelming number of impressions per page. This inundation of advertising has been another driver of ad blocker adoption.

Sure, most users agree to the "unspoken handshake" that they don't have to pay money for digital content in exchange for letting advertisers vie for their attention. But the rise of ad-blocking can be seen as an argument that publishers have broken their side of the compact with a tsunami of gratuitous distractions.

Keep the user experience in mind when evaluating page designs and ad placements. As recent studies have shown, the "NO ADS EVER!" brigade is not that large, and many users who have added ad blockers are willing to whitelist sites when asked. At what number do the ads become burdensome or even detrimental to user experience?

It's tough to gauge, and honestly any decision will likely be a judgment call based on your site's experience and audience response. In addition, **a little analysis** may show that adding another placement on a page may actually decrease revenue.

Case in point: USA Today made a bold decision a few years back to minimize the number of display units per story and the result is a much cleaner interface. Of course, any publisher that cuts down on the number of placements per page may take a short-term revenue hit or even feel the wrath of advertisers due to an ensuing rate hike associated with less inventory.

For ops, user experience doesn't necessarily need to take a backseat to driving revenue, but it can certainly become a higher priority.

What Units Cut the Mustard?

Another place where publishers can mediate creative's effect on user experience is in determining which ad units are allowed on site. This is a tricky area because the zeitgeist on ad formats is often shifting. For example, user complaints about Facebook's autoplay in-feed video were loud and rowdy at first, but today it's mainly accepted. On the other hand, auto-play in-banner video has universally become a unit-non-grata, even more so if the sound is up—this stems from user irritation as well as false labeling of these units as pre-roll inventory.

Unfortunately, more disruptive units such as interstitials or takeovers often garner higher CPMs. Once again, your revenue goals and user experience prerogatives might be in direct conflict. Balancing the two is quite the high-wire act, made all the more complicated by the IAB's decision in Fall 2016 to sunset support for "Rising Stars" and other units. (See sidebar on LEAN units.)

There is no right or wrong—every publisher will have its own answer based on organizational priorities as well as the audience. A certain site may prefer to gamble on

outstream video, in-image ads or some other type of arguably intrusive unit, while another may avoid these as it knows the sensitivities of its user base.

In deciding what ad units to use, here are some things to consider:

- **Your take:** Ask yourself what you would put up with if you wanted to view your content. A 30-second pre-roll to watch a 20-second video sounds ridiculous, but is a quick interstitial or takeover more infuriating?

- **Latency:** Is the unit particularly heavy? Is there a chance it will cause latency or otherwise disrupt user experience (e.g., block content) in unexpected ways? Those are all good reasons for a ban.

- **Check with the rest:** Are publishers in your vertical using this unit? What's the experience like on their site? Reach out to your peers and see what their experience has been.

- **Test the unknown:** There's nothing wrong with experimentation. If you have misgivings about a new type of ad unit, run a campaign employing it and analyze user reaction through your analytics team (e.g., bounces) as well as directly from users.

- **Get your freq(uency) on:** If you choose to deploy disruptive units, the key is frequency control. Make sure users aren't barraged with a certain ad or format. Again, judging this can be based on traffic and feedback analysis, but it's kind of a gut call.

- **Skip-ability:** There's something to said for offering the ability to skip ads such as interstitials and pre-roll—not only will users appreciate being given a choice, it also encourages engagement.

Units The Media Trust Discourages:

- **Auto-play audio**
- **Out-of-browser redirect**
- **Pop-up/under**
- **OS/interface lookalike**
- **Shaking/flashing**
- **Provocative/adult**

Where Are the Specs?

Surprisingly, something that has made the creative situation even more tenuous is the "Death of Flash." Although the former creative standby isn't supported on mobile and is being relegated pretty much useless on desktop browsers, Flash isn't technically dead: you will still see some creative floating around made of Flash and many videos will contain a backup Flash file. But browser decisions to freeze non-essential Flash on pages—and Chrome's announcement that it will stop the software from loading automatically by the end of 2016—have encouraged publishers and (most) agencies to abandon the tech for HTML5.

The issue: Flash file sizes are tiny—its chief benefit was file compression—while HTML5 creative tends to be big. One of our publisher sources suggested that the average creative received is now three times as large. You can bet this puts a lot more pressure on page load, and can prove disastrous when lumbering creative hits data-sensitive platforms such as mobile.

With the increase in cross-platform campaigns, tight ad specifications are more important than ever. (And they're definitely in flux—see sidebar on LEAN Ads). The IAB updated its standard ad specs in 2015 to accommodate the mass switchover to HTML5:

- **Max Initial File Load: 200K**
- **Subsequent Max Polite File Load: 300K - 1MB**
- **Subsequent Max User-Initiated File Load: 1.1MB - 2.2MB**
- **HTTP Request Max: 15**
- **Fallback Image Size: 50K (varies by ad size)**

Many of the maximum file sizes offer allowances on the type and functionality of the unit (e.g., the Rising Stars series). Still, some publishers may consider these too heavy and put out their own specs: e.g., 100K for an initial file, 10 HTTP requests max, etc. This is especially true for publishers that have heavy pages to begin with, due to a lot of active code (e.g., weather or local news sites).

While HTML5 ultimately makes for a better web and ad experience, it's essential that publishers become vigilant when it comes to checking creative file aspects.

Consider Native Placements

Native placements are in-feed display ads with flexible creative that matches or complements a site's visual aesthetics. Basically, they're "better banners," but SSPs and networks get upset if you bring in that maligned term. While they are prominently labeled as sponsored (lest they run awry of the Federal Trade Commission—see section 7), they seamlessly fit into a site's visual flow when done correctly. Plus, the creative files themselves should not be very large, cutting down on loading time. Open RTB 2.3 provides programmatic support for the unit, so it can be traded on exchanges. However, don't forget that native is still an ad format and therefore must be monitored from a malware, data leakage and performance perspective.

Advertisers and agencies will try to drop heavy files on you, regardless of the IAB's guidelines. Rejecting them is all the more difficult thanks to our old friend "late creative," but the potential latency, data drain and overall negative user experience is not worth any revenue bump. If users don't abandon your site, they'll probably consider an ad blocker.

And for your clients still stuck in the aughts, Flash converters are readily available, with some even baked into ad servers.

What's Up With Site Speed?

Heavy creative! Header bidding integrations! Third-party tags! Page latency causes consistent headaches for ad ops, and those three are among latency's most consistent drivers. To manage the causes of latency and improve site

speed, ops has to coordinate with vendors, monitor what's coming through the pipes, and keep an eye on editorial content.

HTML5 involves numerous components—potentially a handful of pieces of code that can load separately in a manner that adjusts to how the user interacts with them. It's not unheard of for publishers to ask agencies for the individual HTML5 components and then re-integrate them into the page, so publishers can have more control over the way the page loads and the effect that has on the user.

Publishers are inundated with third-party tags, which is troublesome because it's often not entirely clear how many tags, or what kind, are in the creative when it comes through the pipes. Tech vendors have been vocal in insisting buyers drop all kinds of pixels in their creative for measurement. These pixels can slow down page load by requiring an extra skip back toward the server before rendering.

Reducing tag clutter is possible, but it requires transparency. Ops needs to communicate to agencies what they can accommodate without adding latency. Agencies in turn need to have conversations with their advertiser clients to prioritize creative objectives and whittle down to the tags actually needed to run and analyze a campaign, not the tags clients *think* they need.

Header integrations are collectively a double-edged sword—publishers love how header bidding grows revenue, but header integrations are notorious for adding to page latency. It's something header vendors are working on improving, but still something publishers need to monitor. Publishers can step in here and experiment with time-outs—if one or more header partners doesn't respond by x milliseconds, render an ad from another partner.

For each publisher business, there's the right balance of the amount of time you're willing to wait to get all your bids in versus the amount of money you're willing to potentially leave on the table by timing out at a particular point. But monitoring performance this way can also help a publisher understand who brings them the most value by being in the header and who to kick out of the header.

What About Programmatic?

It's a lot easier to remediate the creative that comes through the door through direct sales. Even if it's late, creative that fails to meet specs can be smacked down before the campaign gets rolling.

Programmatic—particularly through RTB channels—is more difficult to handle. Most creative doesn't go through a quality check ahead of time, though with private marketplace deals, a publisher can ask for creative in advance, or evaluate it once the campaign gets rolling. (Still, publishers should evaluate the creative during the campaign as creative is often changed.) Even in programmatic direct, the publisher should be able to perform a QA check before approving the campaign.

The open marketplace is a bit more Wild West. Advertisers will mislead DSPs, exchanges and SSPs about the nature of their ads—what's labeled as a standard display unit might actually contain an expanding video unbeknownst to any party in the chain. Or your demand partners might simply slip and disobey your format and creative requirements.

A creative or media scanner will report to you when a banned ad unit comes through programmatic channels—some offer the ability to block creative from being delivered. When discovering banned units or unfriendly creative, you should share this information with the source. It's your choice to take the next step and lower the source's priority within your tech stack, or even make the drastic move of cutting the source off.

Some publishers will be lenient and issue stern warnings the first few times the seedy stuff slips through as frequently the demand source itself was tricked. That's also a reason why exchanges, DSPs and SSPs are themselves investing in media scanners; with such a plethora of demand sources about, it's no good to get a rep for letting through illicit formats and lousy creative. Chat with your programmatic demand sources about their scanning efforts or lack thereof.

LEAN Ads and the New Ad Portfolio

As a response to the rise in ad blocking as well as latency and data drain caused by big, clunky creative, the IAB launched the LEAN ad program in October 2015.

Light: Smaller file sizes with rigid rules on data calls

Encrypted: Compliant with secure sites (HTTPS/SSL)

Ad-Choice Supported: Complies with Digital Advertising Alliance's privacy labeling
(Note: this is a paid service)

Non-Invasive Ads: Do not block, obscure or disrupt content

To further push the LEAN initiative, in the fall of 2016, the IAB released a new standard ad unit portfolio of LEAN ads that would replace many current units come 2017. The Rising Stars series and other rich media units are to be phased out. The portfolio draft also includes "Flexible Size Ad Specifications" for maintaining aspect ratio and adjusting to screen sizes and responsive design sites. Finally, the released document contains guidance for native placements as well as 360° image, augmented reality, and virtual reality ads.

- Ad expansion must be user initiated in a "discrete" fashion (e.g., a click or swipe), not a hover or a rollover. It is recommended that the expansion take over the full screen (with ad in the center), but a highly visible close button is required.
- Auto-expansion through scrolling is only allowed if the ad does not move or obscure the content on the page.
- Interstitials are ads that appear "before, in between, or after the primary content experience," and are required to have a close button. Pop-up ads are "delisted," and ads that overlay or cover the page after a user has started viewing content are not considered interstitials.
- Any ad that interrupts an experience must include a close button—at the least, an X measuring 50 x 50 dp—in the top right-hand corner.
- Autoplay video is only allowed on wi-fi or broadband Internet connections and must start on mute.

Our publisher sources agree with the LEAN initiative and think that it's a good step forward for the industry. Following these specs will greatly relieve the ad burden on page load and weight. However, publishers are still waiting for the buy side to embrace LEAN units. There may be a long transition time in moving to the IAB's proposed units.

You know who else cares a great deal about user experience and security online? Government entities in the US and EU, which have enacted numerous regulations to protect the citizenry from the ugly elements of the Internet. Every business with a website is under increasing legal and regulatory oversight, and dealing with this requires the involvement of site operations, CISO/security and legal.

While some may consider these good-intentioned rules to be onerous, no one will deny that running afoul of them can be a costly and embarrassing affair. Here are a few big regulations that can affect digital publishers.

COPPA

The U.S. Government is quite apprehensive about the handling of children's data, and the Federal Trade Commission has brought numerous actions against publishers and major brands since enactment of the Children's Online Privacy Protection Act (COPPA). COPPA specifically regulates data collection from users younger than 13 years old. The act applies to "commercial websites and online services (including mobile apps)" directed at this age group as well as general audience sites and services that are knowingly collecting data from users under 13 years of age.

First enacted by Congress in 1998, the FTC made substantial revisions in 2013 including increased parental notice and consent requirements. Most notably, COPPA now applies to plug-ins, advertising partners and others collecting data on other sites, apps, etc. from users they know are under the age of 13.

COPPA demands services and sites 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 in "persistent identifiers"; details what practices should be included in a site/service's online privacy policy; and commands reasonable confidentiality and data security, as well as data expiration dates.

To satisfy regulatory requirements, some social networks strictly state that users under the age of 13 are not allowed to sign up for their services. Other publishers simply avoid collecting any data from users they are sure are under 13, or even if there's a high probability the user is under 13. Sites that cater to younger audiences or have substantial youth followings can get into tight spots when trying to leverage programmatic channels or if advertisers are demanding certain segmentation.

Ops' primary objective is to make sure your site's privacy policy is explicit about the handling of data for those 13 and younger. Ideally, the site will have a highly visible spot where parents can learn about data usage. Besides that, there are several FTC-approved safe-harbor programs for auditing sites and offering guidance: Entertainment Software Rating Board, Aristotle International, Privo, TrustE, and Children's Advertising Review Unit.

While it's good to read through and understand COPPA the best you can, chances are you don't have a law degree. Therefore, you'll want to work with your legal department in assuring your privacy policy is compliant and up to date. But legal should also be approached any time an advertiser wants to target, track, or collect data of users under 13. Finally, your creative QA supplier should be scanning creative and ad tags for COPPA compliance, including dangerous or suspicious data practices from third-party vendors.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) actually covers a lot of ground, setting the rules around group healthcare plans, enabling workers and their families to keep their health insurance when leaving a job or switching jobs (COBRA), as well as maintaining privacy for individual medical records.

While all publishers should make sure every health-related campaign is HIPAA compliant, health-care related sites cannot offer targeting that could potentially identify a patient. This is known as protected health information (PHI) and 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.

GDPR

The EU's pending General Data Protection Regulation, expected to go into force May 2018, ushers in a world of uncertainty for ops. Without going into the ins and outs of the regulation, GDPR will have far-reaching impacts on publishers and their ad tech partners. Among other things, GDPR strengthens existing data protection regulation by:

- Classifying unique identifiers of online behavior (IP address, cookies, advertising ID, etc.) as personal data
- Extending protection responsibilities to those with access to data (data processors), not just the data collectors (data controllers)
- Requiring explicit consumer consent to collect their data
- Providing consumers immediate access to their data and the ability for it to be expunged
- Implementing a penalty structure for those found in violation; fines can be 4% of gross, global turnover

Everyone is awaiting formal guidance on exactly what publishers and ad tech partners need to (and can) do with their data.

Native Labeling

At this moment, there's no industry standard for native disclosure terms. A 2016 study from the Online Trust Alliance found 43 different phrases across 100 leading publishers, ostensibly to denote that a native ad is not content.

The FTC's guidelines about native ad disclosures recommend using the word "Advertisement" for a unit that's purely ad content. The term "Sponsored" can indicate an advertiser underwrote the content, but didn't create it. The FTC discourages using disclosures such as "Promoted" or "Presented," which are common but misleading because they suggest the publisher itself endorses the content.

Currently, these recommendations fall under "best practices," not standards. If publishers continue to feel pressure from the FTC and users to be more transparent and consistent in native ad disclosures, we can expect more of an industry-wide call for standardization.

- Some publishers may have the resources (a.k.a., human-power) to stock a full UX team with a portion dedicated to the ad and monetization elements. Other publishers have a single person on the revenue team (sometimes cycling) constantly monitoring the site for bad ads and other potential UX detriments. Many strapped for resources will make a dedicated time (e.g., "Thursday surfing") when yield teams will pore over the site to make sure the ad experience isn't sullying the overall one. The idea here is make sure you're monitoring from the front end as well as the back end.

- Once you've determined what is acceptable UX for your site, codify it—this means ad specs, data policies, vendor certification programs, etc. Make sure everything is in writing and that it's easily accessible to not just your whole team, but everyone in the organization lest any questions come up.

- The key ingredient to ensuring your ads continuously comply with company policies and regulatory requirements is 24/7 vigilance. The most useful tool here may be a third-party oversight provider that will alert you to violations.

- Never stop scanning—tags and creative can change mid-campaign, potentially affecting ad and site appearance. Even worse, malware could show up. Be vigilant about scanning—there's no such thing as too much.

- The programmatic environment is probably most difficult for identifying the source of problems such as flagrant creative or malware. Again, leaning on a media scanner can remove a fair deal of the burden.

- In testing site speed and overall performance, quantify the impacts of various partners and third-party code. Measure and benchmark vendor compliance, and communicate to your upstream partners what can be improved (as well as what's not acceptable!).

- Strong relationships with the product and content teams are important. The latter party will likely be the first one to tell you when the ads are affecting user experience.

- Have a simple way for users to offer feedback about your ads. In addition to general insight about your site's ad experience, this could help you detect minor issues (e.g., a non-auto-play video ad is errantly playing) or serious problems (e.g., a malware outbreak).

Parting Thoughts

The rise in ad-blocking has set off alarms throughout the digital media world, especially within the ad tech community. While some are seeking ways to reinsert ads in blocked placement or block the blockers, there seems to have been an industry realization that the digital advertising experience itself needs to change.

The IAB's proposed batch of new standard units—all of which are simpler, lighter, and non-invasive compared to their predecessors—is possibly the loudest and clearest signifier of this user-focused movement.

It may seem strange for a publisher's revenue team to play a role in improving user experience, but it's really just an expansion of one of ad ops' central roles: quality assurance. And because ops has its fingers in so many publisher exploits, it makes sense for the group to be central in ensuring the ad experience does not negatively affect the overall user experience.

In fact, it's not too much of a fantasy to think that advertising and monetization can actually enhance user experience—think about how many people tune into the Super Bowl just for the commercials.

There are limited standards to follow in the world of user experience, but many helpful guidelines. Each publisher will make its own approach to UX following four central categories: malware prevention and security; vendor registration and management; creative control; and regulatory compliance.

When developing an ad-related UX strategy, make sure it is flexible and amendable; opinions on "intrusive" formats and acceptable practices will change over time. Still, this playbook should help you build a framework that can be adjusted as the industry grows and preferences change.

About 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 The Media Trust

THE MEDIA TRUST

The Media Trust works with the world's largest, most-heavily trafficked digital properties to provide real-time security, first-party data protection and privacy, performance management and quality assurance solutions that help protect, monetize and optimize the user experience across desktop, smartphone, tablet and gaming devices.

As the global leader in monitoring the online and mobile ecosystems, The Media Trust leverages a physical presence in more than 65 countries and 500 cities around the world to continuously scan websites, ad tags and mobile apps and alert on anomalies affecting websites and visitors alike. Our solutions help clients govern their website or ad tag assets by providing a repeatable process and complete audit trail for digital ecosystem activity.

More than 500 enterprises, publishers, ad networks, exchanges, and agencies—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to protect their website, their employee internet use, their revenue and, most importantly, their brand.

The Media Trust is a privately-owned, profitable firm experiencing YOY growth for more than 12 years—that's not something you see often.

sponsored by:

THE MEDIA TRUST