

# Brand Safety

SEPTEMBER 2019



**GroupM**  
3 World Trade Center  
175 Greenwich Street  
New York, NY 10007  
USA

All rights reserved. This publication is protected by copyright. No part of it may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, mechanical, photocopying or otherwise, without written permission from the copyright owners.

Every effort has been made to ensure the accuracy of the contents, but the publishers and copyright owners cannot accept liability in respect of errors or omissions. Readers will appreciate that the data are as up-to-date only to the extent that their availability, compilation and printed schedules will allow and are subject to change.

# CONTENTS

- 04** INTRODUCTION
- 08** SOCIAL RESPONSIBILITY  
& CONTEXTUAL RISK
- 16** PROGRAMMATIC  
BRAND SAFETY
- 19** PRIVACY & DATA  
COMPLIANCE
- 25** AD FRAUD
- 34** CONCLUSION

# Introduction



# Brand Safety: Limiting Risks and Improving Trust and Quality in the Digital Supply Chain

Although GroupM started our Brand Safety practice at the beginning of 2017, we have been tackling risks in the digital supply chain on behalf of our clients for more than a decade.

As digital media has grown and become more sophisticated, enabling precise and behavioral communication with individuals, so has the complexity and the potential risk of harm to advertisers.

This document will give the reader an overview of the GroupM Brand Safety practice, how and where we operate and some of the important trends and changes we have observed.

GroupM defines Brand Safety as any risk that an advertiser may face in the digital supply chain.

There are three main categories of risk: financial, reputational, and legal.

An ad should be seen, by a human, in the assigned demographic and in a safe and suitable environment.

## FINANCIAL RISK

- Viewability
- Fraud
- Demo
- 3rd-party tracking

## REPUTATIONAL RISK

- Content environment
- User experience

## LEGAL RISK

- Consumer privacy
- Anti-piracy
- Terms & conditions

We will delve into some of the key areas that are most topical:

- Social platforms and navigating risk tolerance (reputational risk).
- Brand safety in programmatic (financial and reputational risks).
- Privacy compliance (legal risk).
- Ad fraud, aka invalid traffic (financial risk).

We begin with the premise that an ad should be seen, by a human, in the assigned demographic and in a safe and suitable environment.

Thus, in digital adspeak a quality impression equals one that is viewable, free of invalid traffic, in the required demographic and location and in a contextually safe and suitable environment.

Of course, it is not possible to ensure that every impression meets these exacting specifications, but our planning and implementation teams optimize their spend toward publishers who offer this type of quality (and away from those who do not).

Although much of what we read about brand safety is negative, there have been encouraging advances:

- GroupM has seen some spectacular results in viewability — 150% increase in viewability in the first 18 months after inception, as measured by Moat against the GroupM video viewability standard.
- The DoubleVerify Fraud Lab shows GroupM clients are twice as well protected as the industry at large, with a 2% reported invalid traffic (IVT) incidence rate vs. the 4% global benchmark. (DV Fraud Lab, April 2018)

## Changes in Brand Safety

Contextual brand safety awareness really accelerated in February 2017 when The London Times published a five-page exposé headlined “Big Brands Fund Terror.” Journalists discovered brand advertising appearing in extremist videos on YouTube; thus, marketers were inadvertently funding terror organizations through the advertising revenue they received. The fact that mere pennies would have found their way to the organizations who posted the videos did not seem to matter — the potential for reputational damage to the brands created an instant reaction in the marketing community. Advertising on YouTube was suspended by many advertisers, and the London Times event caused marketers to critically look at their overall brand safety strategy.

Since then, actions taken by the platforms to identify and limit high-risk content, as well as the application of more sophisticated technology and practices in agencies, have made the digital environment measurably safer. However, clients in 2019 still regard brand safety as an escalating issue. Why, then, in the face of these improvements are marketers not feeling any better? Perhaps part of the reason is that the brand safety space is becoming more complex and nuanced. In 2017 and 2018, the task was clear. The foundations of brand safety were measure, benchmark and optimize.

**Measure**, because if we do not understand the scope of the problem, it cannot be effectively addressed.

**Benchmark**, because once we understand the level of, say, invalid traffic, we can set an objective to decrease IVT by a certain percentage and measure our success against this benchmark.

**Optimize**, because once we have a benchmark, we can formalize agreements with our publisher partners to deliver low or no IVT.

We have added **compliance** as a fourth step so that we can measure progress against the brand safety goals.

These remain the bedrock of brand safety implementation—the hygiene factors, if you will—but as digital advertising grows and becomes more complex, so does brand safety. In 2019 the conversation with clients has stepped up from brand safety to public safety and related trust issues like supply chain integrity.

Now our conversations with clients center around supply chain transparency (which intermediaries are reducing the pure media spend and what value are they adding?), consumer protection (the protection of users' privacy and data), brand suitability (while an impression is served in a safe environment, is the context suitable for the brand?), risk tolerance (how to manage risk vs. performance in the social and programmatic space—more about this later in the document) and social responsibility (will my brand be perceived as irresponsible if I support a publisher or platform that carries harmful content?).

These issues have mainly come to the fore because of the dominance of the social platforms and the endemic risk of user-generated content that they have to manage. This translates into potential reputational damage for brands using these platforms.

As a way of addressing this, the World Federation of Advertisers (WFA) formed the Global Alliance for Responsible Media, which has called for cross-industry collaboration to address safety and sustainability issues across media, with an early focus on brand and public safety on social platforms. GroupM is a founding member of this alliance.

GroupM is  
a founding  
member of the  
WFA's Global  
Alliance for  
Responsible  
Media.

# Social Responsibility and Contextual Risk





# Navigating Brand-Safe Environments

It used to be easy. Ten years ago, DoubleVerify and Integral Ad Science, then known as AdSafe, began reading URL strings and matching page content descriptions to client-specific keyword lists. This helped soft drink manufacturers avoid articles linking childhood obesity to sugary drinks, helped beer marketers avoid running opposite articles about drunk drivers causing injury or death, and helped airlines avoid advertising on pages featuring planes exploding into fireballs during emergency landings.

The practice of contextual brand safety was born during the last days of the FCC Fairness Doctrine, a U.S. regulation that required news outlets to present opposing opinions, and in the formative days of social media platforms that gave a voice to all, for better or worse. Since then, the exodus of consumer news media consumption from direct, credible, real-world news and entertainment publishers to algorithmically driven social platforms has marginalized mainstream media and extended the grasp of a myriad of nefarious players, including streaming pirates, pharmaceutical counterfeiters, conspiracy theorists and propagandists, extreme political pundits and disinformation and hate speech purveyors. Publishers of harmful content rely on the brilliant ignorance of advanced artificial intelligence to find readers who will like and share their vitriolic and/or illegal content, and then continue to feed the reader with more and more extreme versions of the content as the reader continues to engage.

Technology that can be used to spread hate can also be used to hunt it and kill it at the source. Legitimate news media are organizing to provide “trust indicators” to enable social platforms to more easily identify credible, quality content to promote in their feeds while demoting the haters and hucksters. Clients and their buying agents are holding the social platforms responsible for not only avoiding harmful brand adjacencies, but for enabling the behavior at all.

Publishers  
of harmful  
content rely  
on the brilliant  
ignorance  
of advanced  
artificial  
intelligence to  
find readers  
who will like  
and share their  
vitriolic or  
illegal content.

# Advancements in Third-Party Verification

The technology arms race between the verification vendors and the vandals has resulted in continuous improvements in third-party detection and interdiction. Companies like DoubleVerify now employ a filter, monitor and block approach to evaluate content before an auction bid, block egregious content in reserve buys, and provide detailed reporting on up to 100 distinct categories of non-safe or misaligned content. Their toolsets have evolved to encompass exclusion and inclusion lists, avoidance categories and complex semantic analysis. In 2019 we have seen the introduction of so-called sentiment analysis tools that use artificial intelligence (AI) to categorize content based on negative, neutral or positive sentiment related to an article’s primary topic. This promises to enable an advertiser to appear in impactful content environments like news while avoiding headline-grabbing partisan op-ed pieces that have become prevalent in today’s newsfeed-driven media consumption environment.

Social platforms are at once the biggest risk environment and the least open to independent, third-party measurement.

One surprising fact is that nearly all video content analysis and classification is done via metadata and audio track/closed captioning analysis. Improvements in image recognition and computer vision promise to enable analysis of the actual video content. Right now, this technology exists paradoxically only at the biggest social platforms and very early stage start-ups. We are watching this develop to see how mainstream verification vendors will evolve in this space. If the best technology remains closeted within walled gardens that deny unfettered verification access, we will never have the chance to evaluate these platforms with a truly independent perspective.

## YouTube & Facebook

As bellwethers of the social walled-garden phenomenon, Facebook and YouTube face the harshest outside criticism over their content policies, targeting strategies and inability to police their own platforms. Social platforms are at once the biggest risk environment and the least open to independent third-party measurement. Our clients continue to be deeply concerned about brand safety measurement and reporting on the platforms. If the seller of the medium is the same entity that measures and reports on the medium, it presents a real governance issue.

That said, responding to media exposure and advertiser pressure, both YouTube and Facebook have improved their internal oversight and advertiser-configurable brand suitability controls. They have employed improved AI; reprogrammed discoverability algorithms; hired armies of human reviewers; launched limited/restricted inventory mode; built partnerships with NGOs to educate their teams on child endangerment, gang violence, drug trafficking, terrorism and political science; and more. Yet there is no end to the litany of new incidents and embarrassments that seem to say these platforms would rather put out the fires than protect the forest.

Since 2016, our continuous pushing for improved internal controls and independent third-party verification has achieved some success. YouTube, Facebook, Twitter and others now maintain viewability APIs that allow human-viewable optimization. DoubleVerify and Integral Ad Science offer brand safety monitoring; this is useful, but it is a little like helping clients see they had an accident without being able to prevent the crash. Perhaps the strongest third-party integration is the proprietary GroupM Guard Channel Inclusion list developed with OpenSlate, which enables clients to run on a limited, curated list of pre-screened and quality scored channels, vs. the YouTube universe of approximately one million monetized channels.

## Risk Tolerance

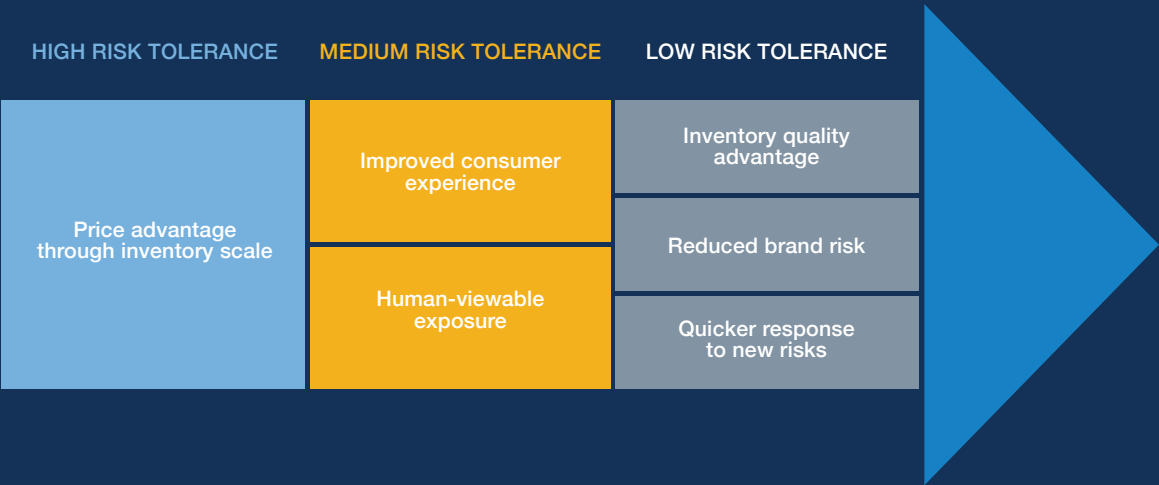
Our approach to contextual brand safety is one of zero tolerance for advertising placed adjacent to harmful content. But, particularly in environments where much of the content is user generated, we recognize that zero tolerance does not always equal zero risk. Therefore, GroupM applies a consultative approach to brand safety. We believe clients should be fully aware of the strategic, implementation and tactical implications of an aggressive, performance-driven approach to brand safety vs. a conservative, low-risk approach. To help us communicate this balance between tolerance and tactics, we created the GroupM Risk Assessment Exercise.

A risk assessment exercise should leave a client and its agency team with a clear idea of the answers to five key questions:

- 1. What is our risk profile for brand safety?
- 2. What are we prepared to do with publishers who will not comply?
- 3. How could we align our internal KPIs with higher quality inventory?
- 4. What do we need to do to implement these changes?
- 5. What communications should we develop around brand safety and possible missteps?

Our approach to contextual brand safety is one of zero tolerance for advertising placed adjacent to harmful content – but that does not always equate to zero risk.

## BRAND SAFETY RISK ASSESSMENT



What is your risk profile for brand safety?

A risk assessment exercise could be a philosophical discussion or a detailed evaluation of each tactic’s contribution to ROI vs. the risk it engenders, but by the end of the engagement these questions should have clear and consistent answers.

The starting point is to ask the marketer to consider three philosophical statements (in reality this is a continuum, but for ease of use we have three segments). Where do they think they fit on the risk continuum in relation to the corporate sensibility or from a brand perspective? We then introduce the idea that the philosophical stance they take has strategic and tactical implications. The most extremely risk-averse marketer will necessarily omit certain tactics or partners that may be considered core or endemic relationships, but that do not support brand safety best practice. It is likely that as you move through the exercise, a marketer’s sense of where they sit on the continuum will change as they consider the implications of their self-assigned risk tolerance level, especially those that consider themselves high risk tolerant or extremely low risk tolerant. It is important that each decision be made jointly, with transparent awareness of the potential risks.

BRAND SAFETY ASSESSMENT: TOLERANCE VS. TACTICS

Brand safety evaluation consists of matching digital tactics to a client’s self-assessed risk tolerance.

HIGH RISK TOLERANCE	MEDIUM RISK TOLERANCE	LOW RISK TOLERANCE
<p>PHILOSOPHY</p> <p>“Performance is the most important factor in our digital media selection decision process. Within reason, we direct our agency to use all available data, technology and media options to deliver KPI. We are willing to accept a certain amount of risk regarding fraud, viewability and questionable content environments.”</p>	<p>PHILOSOPHY</p> <p>“We believe in a balance between performance and brand safety. We expect our agency to use existing brand safety technology to inform and/or protect us from situations where we are incurring financial or brand risk, especially around the growing preponderance of user-generated social media environments.”</p>	<p>PHILOSOPHY</p> <p>“Brand safety is our paramount concern. We believe in a zero-tolerance approach to all brand safety risks. Furthermore, we will only run with inventory sources that offer full human-viewable audience guarantees.”</p>

Once the base philosophy has been established, we move on to aligning the strategy and implementation implications of each risk level. Even clients with the highest tolerance for risk benefit from the basic GroupM campaign governance setup, including our base master service agreements which cover editorial adjacency language and payment terms, data protection, and more; our global mandatory exclusion list; our third-party verification relationships; and the industry-leading custom GroupM viewability metrics. As we move across the risk continuum, we add strategic elements like brand-safe partner criteria, viewable reconciliation, and a more curated approach to social media as well as brand safety as primary partner criteria.

The next step is to evaluate differences in campaign setup. Medium- and low-risk approaches add optional exclusion lists, which prohibit extreme political opinion, propaganda, conspiracy theories, clickbait and more.

They also require assessment of verification-friendly technology like blocking tags, Digital Video Ad Serving Template (VAST 4.1) and buying on a strict site inclusion list, which can be a central [m]PLATFORM or Xaxis list or curated at the client level.

SETUP & TACTICS ALIGNED WITH RISK TOLERANCE

Brand safety evaluation consists of matching digital tactics to a client’s self-assessed risk tolerance.

	HIGH RISK TOLERANCE	MEDIUM RISK TOLERANCE	LOW RISK TOLERANCE
CAMPAIGN SETUP PROGRAMMATIC & RESERVE BUYS	<div>STANDARD GROUPM CAMPAIGN GOVERNANCE:</div> <ul style="list-style-type: none"><li>• GroupM MSAs, including adjacency guidelines, fraud reimbursement and data protection terms</li><li>• Brand safety monitoring on all buys</li><li>• GroupM mandatory exclusion list</li><li>• 3rd-party tracking and reconciliation as available</li><li>• GroupM human-viewable measurement used as optimization diagnostic</li></ul>	<div>STANDARD GROUPM CAMPAIGN GOVERNANCE PLUS:</div> <ul style="list-style-type: none"><li>• Viewable tracking, optimization &amp; reconciliation when available</li><li>• Brand safety blocking where available with limited keyword lists</li><li>• Augmenting mandatory exclusion list with high-risk optional exclusion list</li><li>• VPAID/VAST 4.1 sources preferred</li><li>• Applying risk assessment to social media placements</li></ul>	<div>STANDARD GROUPM CAMPAIGN GOVERNANCE PLUS:</div> <ul style="list-style-type: none"><li>• Brand safety as the primary partner/tactic decision criterion</li><li>• Layered brand safety partner setup</li><li>• 100% human-viewable reconciliation</li><li>• Augmenting mandatory exclusion list with high- &amp; medium-risk optional exclusion lists</li><li>• Requiring brand safety blocking with extended keyword lists</li><li>• Buying only on GroupM-approved - inclusion listed domains</li><li>• VPAID/VAST 4.1 video sources only</li><li>• Proprietary IO - level terms and remedies</li><li>• Extreme caution/avoidance of social user-generated environments</li></ul>

Once we’ve established strategic and campaign setup parameters, we begin to evaluate specific tactical differences by risk level. These are GroupM-recommended alignments by tactic. Remember, though, that the assessment is meant to be a custom consulting engagement, which may include rejecting certain tactics shown within a given tier and embracing others.

Social platforms have become the central focus of the evolution of brand safety to include consumer protection and social responsibility. Given the big budgets, video reach, deep consumer engagement and distributed content model, there is inherent conflict in the need to use these platforms and the need to pressure them to better police their content and comments. GroupM and our largest clients are engaged in an ongoing dialogue to pressure these platforms to improve their risk profile for consumers and brands.

GroupM is also working with industry leaders around influencer verification to build out better solutions for clients with respect to influencer activation.

Brand Suitability

The concept of risk tolerance can be applied across all forms of brand safety, including management of financial, reputational and legal risks. The most subjective area is content association. There are widely different views on what constitutes an appropriate environment for a message, depending on the brand in question.

The risk assessment is meant to be a custom consulting engagement, which may include rejecting certain tactics and embracing others.

Graphic depictions of violence or gratuitous drug use may be palatable to some advertisers.

Moreover, the current political climate around the world has increased the danger of brand association with fake news, hate speech, and extreme political opinion, which has led to many clients avoiding news placements entirely. So, while association with some content may still be safe per se, it could be considered unsuitable for the brand.

The 4A's Advertiser Protection Bureau has created a Brand Safety Floor and a Brand Suitability Framework to define for the industry the types of content that are never appropriate under any circumstances (now a baker's dozen), and to define editorial treatment of hard news topics that can be considered appropriate for high, medium, and low risk tolerant advertisers.

These resources can be used to determine the types of content that an advertiser might find acceptable and to guide buying decisions and page-level inclusion list development. Brand suitability also extends to matching brand messaging to appropriate editorial environments.

The Brand Suitability Framework can be used to help gauge a client's risk tolerance level for appearing in sensitive content when it is presented in a brand-safe manner. The promotion and advocacy of terrorism, hate speech or violence meets the definition of non-brand safe all the time, but graphic depictions of violence or gratuitous drug use may be palatable to some advertisers, while others might draw the line between dramatic depiction of violence vs. a documentary discussion of changes in a country's violent crime rate. The model here is quite specific and detailed, designed to spark a discussion and lead to the development of specific brand implementation guidelines that can drive planning, buying, targeting, optimization and verification investment decisions and vendor selection.

CONTENT RELEVANCE CONTINUUM

Content environments have been mapped based on editorial approach to sensitive topics and contextual relevance.

BRAND SAFETY FLOOR (NEVER SUITABLE)	HIGH RISK SUITABLE	MEDIUM RISK SUITABLE	LOW RISK SUITABLE	CONTEXTUAL RELEVANCE
Graphic, excessive use or promotion and advocacy of dirty dozen content	Glamorization/gratuitous depiction of dirty dozen content	Dramatic depiction and topical news coverage of dirty dozen content	Educational, informative, scientific or documentary treatment of dirty dozen content	<ul style="list-style-type: none"><li>• Endemic</li><li>• Target relevant</li><li>• Related interests</li><li>• Local interest</li><li>• Professional interest</li></ul>

\*Obscenity & profanity, illegal drugs, spam/harmful content, terrorism, tobacco/e-cigarettes/vaping, sensitive social issues/violations of human rights, adult & explicit sexual content, arms & ammunition, crime & harmful acts to individuals and society, death or injury, IP piracy, hate speech and acts of aggression, military conflict

<https://www.aaaa.org/wp-content/uploads/2018/09/APB-Brand-Safety-Floor-Framework.pdf>  
<https://www.aaaa.org/wp-content/uploads/2018/09/APB-Brand-Suitability-Framework.pdf>

## On the Horizon

Impending privacy legislation around the world, the establishment of GDPR case precedent, improved verification technology and the slow but steady impact of marketplace pressure on walled gardens depicts a near future in which advertisers will have greater transparency, control, and the awareness to consciously decide how much risk they are willing to engender in the pursuit of business performance.

New and emerging areas of focus include brand safety in connected TV, potential and proven bias in AI and extreme brand safety settings, and the imperative initiative to rescue revenue-starved credible news media outlets crushed between the forces of consumer flight to non-ad-supported environments, platform distribution hegemony, and eye-catching and click-generating fake news.

GroupM will continue to work to protect our clients' brand equity while supporting legitimate, credible, quality content sources across the evolving landscape of global digital media.

# Programmatic Brand Safety





Contextual brand safety in programmatic has not taken as much heat as brand safety on social platforms. Nevertheless, the issues are the same: online piracy, hate speech, online disinformation, terrorism and obscene content. Unlike the social platforms, programmatic offers more mitigation tactics, primarily through third-party verification. Despite this fact, the use of third-party verification and pre-bid blocking remains optional for many advertisers, which may result in inappropriate adjacencies on long-tail websites typically bought through ad exchanges and ad networks.

## Content Is King

Brand safety drives greater demand for quality and premium content or buying media in controlled environments. Trusted marketplaces (TMPs) are already trending in Europe, and we will see this trend peaking in the next 6 to 12 months across the globe. Inventory offered via TMPs will, by default, be third-party verified and vetted, and contextually safe as well as contractually compliant. Apart from quality inventory available via TMPs, the market is already seeing publishers forming conglomerates and selling quality inventory tied up with first-party data. These joint-publisher ventures are likely to attract more ad spend as they offer high-quality journalistic content mixed with appropriate audiences.

Brand safety  
drives greater  
demand for  
quality and  
premium content  
or buying media  
in controlled  
environments.

## Emerging Technology

New channels such as connected TV or programmatic out-of-home are likely to have their own adolescent brand safety problems. Developing and independently certifying technologies able to conduct the proper measurement needed to trust these media will be of great importance. In turn, traditional measurement companies operating in the web/app brand safety measurement realm will have to step up their game with regard to deploying more efficient machine learning that will be able to digest and effectively block linguistically nuanced content, begin analyzing visual and audio in video content, and venture further beyond metadata and ad-positioning analysis.

## Best Practices

Every advertiser gets to define what kind of content is suitable for their brand. According to their preferences and assessment, different tactics are recommended.

Here are GroupM's best practice tactics to avoid inappropriate brand safety adjacency in programmatic:

### TRADE DIRECTLY

When trading media, we prefer to buy programmatic media directly from high-quality and trusted media owners, and to avoid non-transparent ad networks and ad exchanges. If it is impossible to buy media directly, we require the use of inclusion lists, exclusion lists and independent technology verifying whether the content of pages and apps is safe.

PROTECT CONTRACTUALLY

GroupM aims to agree on contractual brand safety terms that protect the interests of our clients. These terms may stipulate take-down procedures and the kind of content that is appropriate for brands' adjacency.

DEPLOY AVAILABLE 3<sup>RD</sup>-PARTY VERIFICATION TECHNOLOGY

GroupM uses technology in two ways: to inform the GroupM global exclusion list (over 300,000 apps and websites) and client-bespoke inclusion or exclusion lists, and to limit or block where ads appear at the point of the delivery.

ESTABLISH CLEAR OPERATIONAL PROCESSES

We have defined operational processes to monitor or vet media-owner inventory to ensure it meets our own or client brand safety standards.

WORK TOGETHER (WITH THE INDUSTRY)

Industry cooperation is of incredible importance. Industry bodies across the world are establishing programs and often accrediting (following an independent audit) companies for their compliance with industry-established best practice guidelines. We work with several trade initiatives — including the Joint Industry Committee for Web Standards (JICWEBS) in the UK and Ireland, Trustworthy Accountability Group (TAG), Media Rating Council (MRC) and China Media Assessment Council (CMAC) — to help develop industry standards and best practices. The GroupM brand safety team is on the board of these institutions and is certified by both JICWEBS and TAG. Other noteworthy initiatives are Digital Ad Trust in France, the IAB Quality Index in Italy and the Digital Trust Initiative in Germany.

PROVIDE EDUCATION

Educate staff, clients and the public about the risks and how to mitigate them.

# Privacy and Data Compliance



The GDPR made data protection famous. The acronym was searched for more often than Beyoncé.

## A Force for Good — If We Can Navigate the Legal Minefield

Privacy as a risk area spans financial, legal and reputational risks. Any company in breach of the relevant privacy law is subject to losing user trust (reputational), getting fined (financial) and undergoing long proceedings (legal). This is not only a matter of legal compliance; it is equally about addressing user concerns about privacy in a holistic manner through transparency, accountability and fairness.

Around 57% of the global population uses the internet. Some [reports](#) indicate that every day, one million people go online for the first time. More than 80% of Europeans and North Americans are already online. Therefore, it is no surprise that the safety of online consumers and the need to transpose analogue notions of privacy and data protection to the digital sphere is high on consumers' and legislators' agendas. Privacy legislation has become not only desirable, but inevitable.

While data protection legislation has been around for a while now, the best known example is the European Union's General Data Protection Regulation (GDPR). The GDPR is best known for several reasons: it came at a crucial moment (beginning of the fourth industrial revolution), it set a global precedent, and it set the bar very high for compliance.

The GDPR made data protection famous. The acronym was searched for more often than Beyoncé.

Preparing for the GDPR made marketers, data companies and agencies rethink their data protection practices not only from the compliance perspective, but also from the standpoint of transparency and information provided to consumers. As an industry, we have taken a big step toward providing more and better information to consumers about what exactly is happening with their data — what it is used for, with whom it is shared and more. The GDPR has also brought the industry together under the auspices of trade bodies to design sensible solutions.

The preparation work done for the GDPR will come in handy, as the law has inspired many governments across the world to propose virtually identical or very similar laws. The WFA map (featured on pages 22 and 23) shows at least a dozen laws around privacy and data that have been adopted or proposed. The trend is obvious, but the challenge is that the proliferation of privacy legislation can lead to regulatory fragmentation. Consistent regulation is of great importance for smooth implementation of media execution, as well as consumer transparency. A perfect example of a potential challenge is the United States legislation. What if 50 U.S. states adopted their own privacy legislation, similar to the impending bill in California (CCPA)? We would have a clumsy patchwork of legal requirements to comply with and consumers would have a confusing array of different rights and information to deal with, depending on the state. An industry body called Privacy for America is working to normalize U.S. legislation under one federal bill before CCPA comes into effect in 2020.

As important as it is for the United States to have one federal law, it is equally important that privacy legislation be aligned globally.

## Data Protection Best Practices

Here is a checklist of useful privacy and data hygiene questions to address before each campaign:

### INTERROGATION OF THIRD-PARTY AUDIENCES & DATA VENDORS:

- What are your business objectives tied to the acquisition of third-party audiences or data? Can you lawfully use the data you intend to acquire as you plan?
- Does the vendor have a data privacy policy, and where is it made publicly available?
- Do you have a vendor privacy assessment checklist to enable consistent review of third parties?
- Have you identified the consequences and remedies should a vendor fail in their answers to questions on your checklist?
- Have you delineated employee responsibilities and authority as related to vendor review, including when they are onboarded using digital tools?
- Does the vendor employ the same care for personal data and handling as prescribed in your own business?

Preparation for GDPR will come in handy. At least a dozen new privacy laws have been proposed or adopted.

### TRANSPARENCY TO CONSUMERS:

- Comprehensive understanding of why the planned personal data use is necessary for identified business objectives.
- Detailed understanding of how the data will be technically processed and by whom.
- An easily accessible display of information on why personal data is collected and how it will be used.
- Language describing processing activities that may be understood by the average person (not educated about processing of personal data in the relevant sector).
- A means for consumers to easily opt out of personal data processing.

### GOOD TAG MANAGEMENT:

- Identification of data categories for capture via tags that are consistent with the privacy notice.
- A policy that only necessary data will be captured.
- Clear delineation of the responsibilities held by those setting and managing tags.
- A process for reviewing data proposed for capture via usability fields to ensure alignment with the established privacy notice, or amending the notice as needed to support business objectives.
- A process for notifying recipients of tag data feeds about exactly what data they should expect.

# Global Privacy Map



Source: World Federation of Advertisers (WFA), August 2019. This map is not an exhaustive list of all legislative developments in the world. It does not constitute legal advice. The map is indicative and may change over time.



The defining issue around data privacy and protection: the balance between strict compliance, detailed user information and user experience.

## Looking Ahead

The GDPR has not been fully enforced yet. As time passes, we expect to see data protection authorities issuing notices and decisions that will further shape the data protection landscape in Europe. Equally, the courts have yet to set important compliance precedents. These developments will be carefully observed by the rest of the world.

Important future considerations are the adoption of new technologies such as the Internet of Things, which will require a fresh approach to user transparency given the ubiquity of data collection particular to IoT. This will accentuate the need to solve perhaps the defining issue around data privacy and protection: the balance between strict compliance, detailed user information, and user experience. Furthermore, data is the sine qua non of AI development. The ethics of AI will continue to be a focal point of discussions as we will have to ensure AI is non-biased, like the humans who created it, while being able to secure the privacy rights of consumers whose data AI is using.

2019 EU [research](#) shows that consumers are less likely to read privacy statements than they were in 2015 (-7 percentage points). User experience design will come to the forefront of data protection as we will have to learn to communicate more with less, while being fully transparent and compliant.



# Ad Fraud



## How Much Internet Traffic Is Fake?

One of the areas of brand safety that raises alarm bells within the C-suite of large corporate organizations (beyond the marketing department) is the report of their marketing dollars being spent on fraudulent advertising. Not only is this a concern about wasting their shareholders' money, but also about the moral and ethical issues of funding harmful and illegal practices such as digital piracy and crime syndicates.

Overall estimates of fraud vary widely, but even the most conservative put the money involved worldwide well into the billions annually. Recent estimates vary from \$6.5 billion to as high as \$23 billion. This has forced some marketers to take action: The most recent high-profile incident involves Uber suing five ad networks for squandering tens of millions of dollars on low-quality or fraudulent inventory.

This section will examine whether ad fraud is as big an issue as the headlines suggest, or if organizations with a vested interest are creating hyperbole to scare marketers into deploying their “special sauce” technology to make this all go away. We will also provide advice on how to avoid fraud.

## What Is Ad Fraud?

According to the 2012 IAB Guidelines for the Conduct of Ad Verification, ad fraud is constituted as “impressions that result from an intentionally deceptive practice designed to manipulate legitimate ad serving or measurement processes or to create fictitious activity that leads to inflated counts.”

Ad fraud is a practice that is conducted by criminal organizations and not by reputable, legitimate publishers (at least not intentionally).

## What Ad Fraud Is Not

Ad fraud is not an ad appearing on a legal site bought legitimately through an exchange that an advertiser feels may negatively impact their brand image and/or reputation. For example, an advertiser may not want their ads on Breitbart, but Breitbart is entitled to sell advertising space. If an advertiser has accidentally been placed there, it is not fraud.

Ad fraud is not legitimate ads bought that are not being viewed. Viewability is an issue around trading standards with publishers (the same way receiving a certain percentage of position in break on TV is a trading standard between advertiser and broadcaster). GroupM holds direct online publishers to a higher viewability standard than the market does. However, when digital ads are bought through open exchanges, the CPM billing event includes non-viewable impressions. While this impacts advertising effectiveness (i.e., how can an ad be impactful when not seen?), it is not illegal activity.

## GIVT vs. SIVT

General Invalid Traffic (GIVT): GIVT is traffic generated by known industry crawlers (such as search engine crawlers) and traffic generated by bots doing the kinds of things that real humans would probably never do (like switching between websites every 10 seconds for hours on end), making it easier to spot. GIVT can be identified using routine methods of filtration using lists or standardized parameter checks.

Sophisticated invalid traffic (SIVT): Sophisticated invalid traffic is more difficult to detect because fraudsters are actively trying to avoid simple patterns that would raise a red flag. These fraudsters are making an extra effort to mask their behavior as legitimate, so it requires advanced analytics, multipoint corroboration/coordination, and significant human intervention to detect, identify and analyze.

Invalid Traffic (IVT): IVT is the sum of GIVT and SIVT, representing reported ad traffic that should be scrubbed from payable impression counts.

Note that while some GIVT is not fraud, it still is invalid traffic for purposes of calculating payable impressions.

Note that while some GIVT is not fraud, it still is invalid traffic for purposes of calculating payable impressions.

## What Are Typical Ad Fraud Tactics?

- Selling inventory automatically generated by bots or background mobile-app services.
- Serving ads on a site other than the one provided in an a real-time bidding (RTB) request – this is known as domain spoofing.
- Delivering pre-roll video placements in display slots.
- Falsifying user characteristics like location and browser type.
- Hiding ads behind or inside other page elements so that they cannot be viewed; this is known as:
  - Ad stacking - multiple ads on top of each other like a stack of pancakes.
  - Pixel stuffing - when ads are crammed into a tiny pixel box on a web page, which cannot actually be seen.
- Hindering a user’s opportunity to engage by frequently refreshing the ad unit on the page.

## Where Does Ad Fraud Typically Occur?

There are two general areas where the majority of ad fraud occurs:

1. Fraudsters follow the money! It is a pretty simple rule of thumb, but if there is a scalable opportunity to be exploited by ad fraud

companies, they will find a way. Programmatic digital display represents a huge chunk of digital ad budgets, both in the U.S. and around the world, and it is highly vulnerable to fraud thanks in large part to long, complex and opaque supply chains. The result is a significant risk of invalid traffic finding its way to programmatic display campaigns.

- 2. Nascent formats are often more vulnerable, as quite often the traditional fraud detection companies (IAS, DV, White Ops, etc.) have not been building their tracking capabilities as fast as the fraudsters’ ability to game the system. While not big in terms of volume, new, niche inventory types like native audio or connected TV offer an opportunity to slip under the radar.

GroupM estimates the risk of total fraud to be \$22.4B globally, with an average fraud rate at 10.8%.

### How Big Is the Ad Fraud Problem?

GroupM estimates the risk of total fraud to be \$22.4B globally, with the average fraud to be at 10.8%.

REGION	AVERAGE IVT	DIGITAL AD SPEND (M)	FRAUD (M)	SHARE OF FRAUD
North America	3.30%	\$79,036	\$2,608	11.6%
China	30.7%	\$60,931	\$18,675	83.4%
EMEA	1.60%	\$50,220	\$804	3.6%
APAC (excl. China & Japan)	1.60%	\$14,429	\$231	1.0%
Latin America	2.70%	\$2,922	\$79	0.4%
TOTAL	10.8%	\$223,950	\$22,397	

### Ad Fraud by Market

REGION	MARKET	AVERAGE IVT	DIGITAL AD SPEND (M)	FRAUD (M)	SHARE OF FRAUD
NA	USA	3.4%	\$73,400	\$2,496	11.1%
APAC	China	30.7%	\$60,931	\$18,675	83.4%
APAC	Japan	n/a	\$16,411	n/a	n/a
EMEA	UK	2.4%	\$15,550	\$373	1.7%
EMEA	Germany	1.6%	\$6,338	\$101	0.5%
APAC	Australia	1.4%	\$6,216	\$87	0.4%
NA	Canada	2.0%	\$5,636	\$113	0.5%

Sources: Digital Ad Spend: GroupM This Year, Next Year; Average Ad Fraud: DoubleVerify, Integral Ad Science (non-China), RTB Asia, AdMaster, AdBug (China)

It is important to note that these are “nominal” fraud statistics. Because there is an estimated \$22.4B of ad-fraudulent inventory in the market, it does not mean that this is bought by marketers. Most ad fraud can be avoided using selective buying and verification technology (see “What can marketers do about fraud?” later in this section). GroupM’s clients are particularly well protected as we employ all ad-fraud avoidance measures and we seek contractual assurance from our partners that any fraud that is detected will be made good.\*

## China

According to this data there is \$18.7B of ad fraud in China, making it over 80% of the total ad fraud market globally. However, it is important to note that measurement standards are not yet widespread in China, which presents challenges in benchmarking any areas of risk and determining with certainty if brands appeared in a fraudulent environment. Additional market-specific challenges we address include the following:

- Clients are unfamiliar with the practice of brand safety and need to be educated on the technology involved and the business ROI for measurement accuracy in the digital supply chain.
- Chinese tech vendors have yet to mature on the verification front, as demonstrated by a lack of accreditation by the Chinese trade bodies (this auditing process is being addressed by the China Media Assessment Council). More so, global vendors that may be MRC-accredited are not fully realized/operational in the Chinese market.
- Support for JavaScript tagging is lacking among Chinese publishers, which in turn limits analysis and measurement capabilities of sophisticated invalid traffic (SIVT).
- Chinese associations like the China Advertising Association (CAA) and their endorsed parties, such as the China Media Assessment Council (CMAC) and Mobile Marketing Association, are still working on better solutions for digital media regulation and accreditation.

In addition, the walled internet environment in China results in a notably different app ecosystem compared to those in Western countries. If the Chinese industry adopts one open-source SDK for mobile, especially given that mobile accounts for 80% of the digital spending, viewability and IVT measurement will be significantly increased and improved.

\*In some developing markets where measurement challenges exist (like China), fraud is benchmarked at a level above zero, but much lower than the industry average, and publishers are contracted to deliver on the agreed benchmark.

Non-Chinese Markets

Excluding China, GroupM estimates fraud to be \$3.7B at 1.8%, which is considerably lower than some of the global estimates. The more major Western markets (UK, USA and Canada) have higher levels of ad fraud than the global benchmark, with the USA contributing 65% of the total estimated fraud.

Why is ad fraud more prevalent in Western markets?

- High-value ad spend tends to be concentrated in the most developed digital markets.
- There is a greater legacy of desktop display advertising, which has a level of fraud generated through bots. APAC has a higher level of mobile video advertising.
- There is a higher volume of inventory traded programmatically in more developed markets.

In Which Channels Is Ad Fraud More Prevalent?

DEVICE	BOT FRAUD	APP/SITE FRAUD	OTHER DEVICE FRAUD
Desktop	45%	7%	48%
Mobile App	11%	54%	35%
CTV/OTT	86%	6%	8%

Source: DoubleVerify Global Norms

The majority (54%) of fraud seen in mobile apps is classified as app fraud. App fraud consists of ad impression fraud or invalid traffic practices such as misrepresentation, laundering and hidden ads.

In general, bot fraud is more difficult to perpetrate in closed app environments, so this type of fraud is more prevalent on desktop and connected TV/over-the-top (CTV/OTT).

## Seven Things Marketers Can Do About Fraud

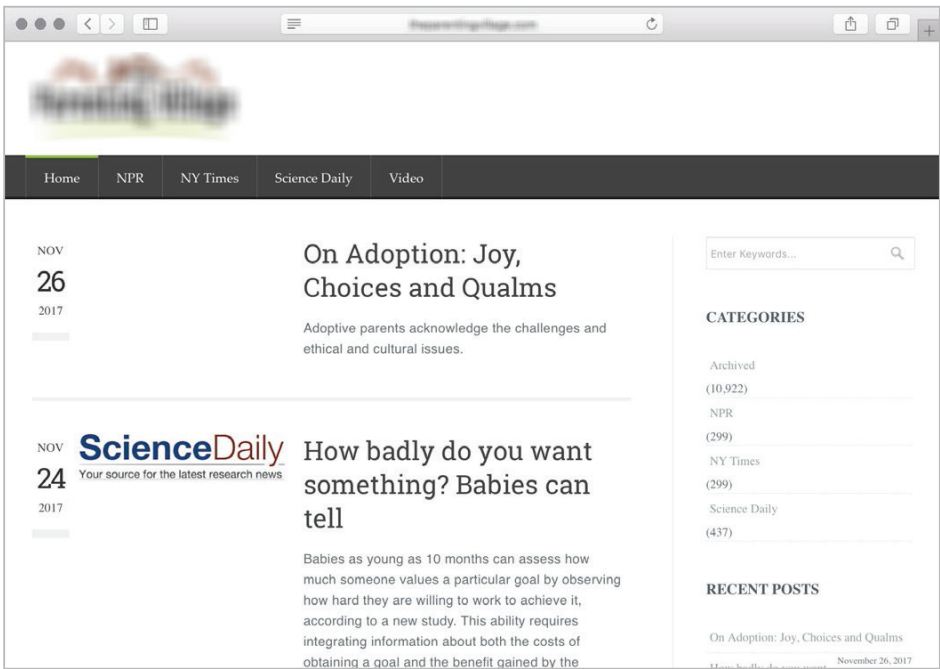
1. “Walking in the best-lit neighborhoods is the best way of keeping safe...” said Rob Norman, former global Chief Digital Office of GroupM. Work with publishers directly, as they have a higher percentage of fraud-free inventory compared to open exchanges.
2. Insist on make-goods for any fraudulent impressions delivered by publishers. Nothing will ensure that a publisher delivers ad-fraud-free inventory like knowing that clients will not pay for IVT. (GroupM contracts protect clients by stipulating that clients will not pay for IVT.)
3. Partner with best-in-breed technology to block all unsafe inventory. Moat, IAS and DoubleVerify are the market-leading specialists in their approach to fraud detection, and their verification technology is applied in both programmatic pre-bid and post-bid environments. “Pre-bid” means the fraud detection company will evaluate if an impression is free of IVT before inventory is bought in a programmatic environment, and “post-bid” means the technology will evaluate if an impression is free of IVT (and brand safe) across all inventory so that any issues can be discussed with non-compliant publishers.
4. Remove untrustworthy sources of inventory. For example, in Australia there are 264 open exchanges serving 19 billion impressions per month. However, not all of these exchanges have 100% fraud-free environments. GroupM removed the vast majority of these sellers and decided that the key criterion for inclusion was that the operator have an office in Australia.
5. Ensure campaign-level optimizations are applied in different cases where, through human and machine monitoring, unusual occurrences such as “click clusters” can be identified to determine if they are fraudulent or instances of classrooms, businesses or other Internet Protocol (IP) groupings. Conduct ongoing evaluations of known proxies, including the ability to set cookies and IP addresses, and deploy advanced fraud detection processes to evaluate the legitimacy of the impressions.
6. Use inclusion/exclusion lists to further ensure that buying programmatically is safe and non-fraudulent, so all sites are reviewed for suspicious activity and suspiciously high clicks, known bot traffic is removed, and previously detected bad IPs, sites and user IDs are blocked.
7. Employ human vetting, a manual process performed weekly on inventory using technology. It involves reporting to review URL masking, manually checking domains and excluding any suspicious domains, monitoring dramatic spikes in web traffic as well as traffic referrals, and visiting domains with low performance and navigating to determine if the site needs to be excluded due to ad placement quality.

“Walking in the best-lit neighborhoods is the best way of keeping safe.”

# How to Spot if a Website Is Delivering Fraudulent Inventory

## “Borrowed” Content

Overt plagiarism is a glaring sign that a publisher might have questionable ethics. For instance, on the site depicted below, every article is lifted from a mainstream publisher and filed under tabs for NPR, The New York Times or Science Daily.

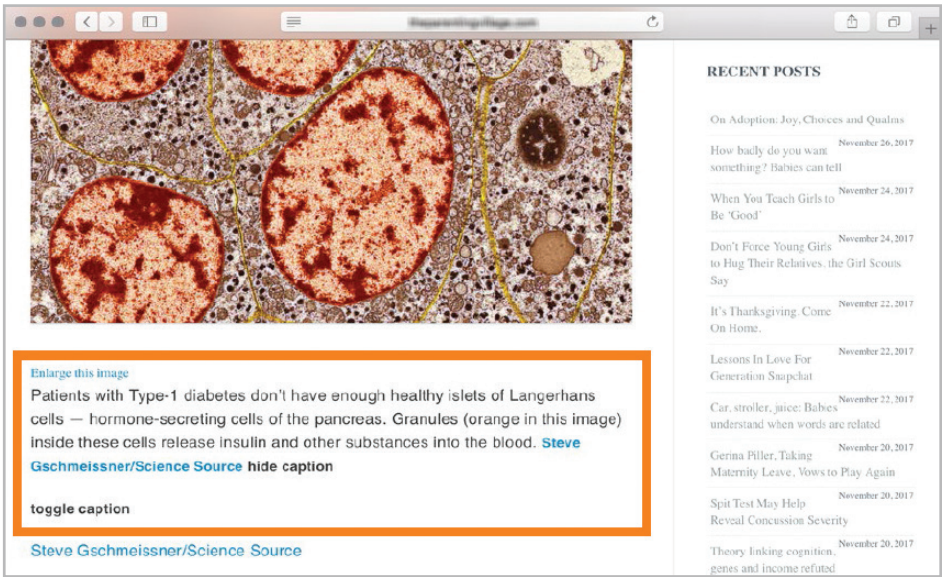


Source: Viral Content: The First Warning Sign of Fraud, Michael Misiewicz, Manager, Data Science, AppNexus



Awkward Formatting

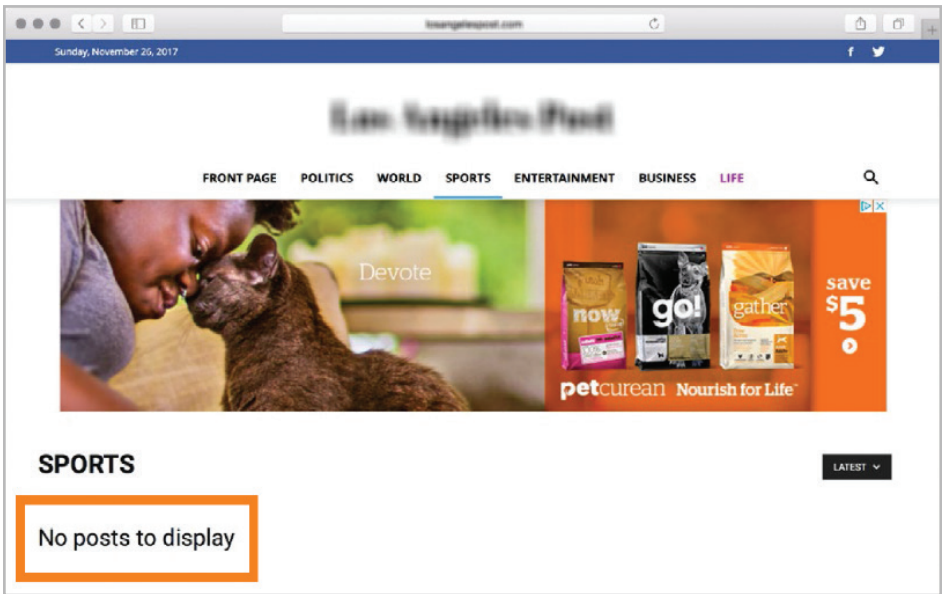
A telltale sign of lifted content is that parts of the story look out of place on the offending publisher’s website. This happens when fraudulent viral publishers scrape a story off another site without reformatting it to fit their own design. For instance, the story below was lifted from NPR. It also has photo captions shoehorned into the regular article text.



Source: Viral Content: The First Warning Sign of Fraud, Michael Misiewicz, Manager, Data Science, AppNexus

Missing Sections

Low-quality viral sites frequently appear as if they are still in the process of being built. For example, take a look at the site below. It is built to look like a conventional online newspaper, but contains only posts, lifted stories and low-quality viral content. When you click a link to its sports section, nothing comes up.



Source: Viral Content: The First Warning Sign of Fraud, Michael Misiewicz, Manager, Data Science, AppNexus

# Conclusion



As noted earlier, brand safety is increasingly observed in the context of social safety and responsibility. The internet hosts some awful content that is not only damaging to adjacent brands, but potentially to our society. Online disinformation is a direct attack against our societies; hate speech ignites social division; and child molesters lurk behind false identities and exploit social platforms to distribute their harmful content. Advertisers and agencies cannot fix this on their own, but they do have a role to play. Trade associations across the world call for greater accountability and for the industry to step up. This is not just because it is the right thing to do, but because of another pervasive trend — regulation. We are witnessing regulators across the world launching investigations at scale and tabling laws that address social and public safety on the internet, and advertising is rarely excluded from such considerations.

## Brand Safety as a Moral Imperative

The work that the 4A's and MRC have done to identify the Brand Safety Floor of “dirty dozen” content categories that should always be avoided is valuable in that context, as these categories are not just dangerous for brands, but potentially illegal. This, however, remains just the “floor” beneath which no brand is likely to want to dive. Most companies will be pushed by their own imperatives, by the public and by regulation to communicate at a level well above this.

Increasingly, marketers are choosing not to wait for regulation but are adopting Immanuel Kant's moral imperative: Do what is morally good because anything else is contrary to reason.

There is a call for media sustainability from marketers (in the same way that they view sustainability in their operational supply chain) and this, together with regulatory pressure, will force a reevaluation of digital media's suitability and effectiveness.

Marketers are  
choosing to  
adopt Immanuel  
Kant's moral  
imperative: “Do  
what is morally  
good because  
everything else  
is contrary to  
reason.”

### AUTHORS:

JOE BARONE – [JOE.BARONE@GROUPM.COM](mailto:JOE.BARONE@GROUPM.COM)

BETHAN CROCKETT – [BETHAN.CROCKETT@GROUPM.COM](mailto:BETHAN.CROCKETT@GROUPM.COM)

JOHN MISKELLY – [JOHN.MISKELLY@GROUPM.COM](mailto:JOHN.MISKELLY@GROUPM.COM)

JOHN MONTGOMERY – [JOHN.MONTGOMERY@GROUPM.COM](mailto:JOHN.MONTGOMERY@GROUPM.COM)

STEVAN RANDJELOVIC – [STEVAN.RANDJELOVIC@GROUPM.COM](mailto:STEVAN.RANDJELOVIC@GROUPM.COM)

GroupM is the world's leading media investment company responsible for more than \$48B (COMvergence) in annual media investment through agencies including Mindshare, MediaCom, Wavemaker, Essence and m/SIX, as well as the outcomes-driven programmatic audience company, Xaxis. GroupM creates competitive advantage for advertisers via its worldwide organization of media experts who deliver powerful insights on consumers and media platforms, trading expertise, market-leading brand-safe media, technology solutions, addressable TV, content, sports and more. Discover more about GroupM at [www.groupm.com](http://www.groupm.com).

3 World Trade Center  
175 Greenwich Street  
New York, NY 10007  
USA

A WPP Company