QuickFrame

The Marketer’s Handbook to Data Privacy Regulations

(and How To Respond)

INTRO

The world of digital marketing and advertising is fundamentally changing

An increased global focus on consumer data privacy has set off cascading effects that are rocking the industry. To remain compliant with a growing number of international regulations, tech giants are restricting how consumer data is collected and used—changing the rules of the marketing game.

While these changes will create some new challenges for marketers, they're long overdue in terms of privacy regulations for consumers. These new mandates will ensure consumers have more access to and control over their data and how it's used.

Now, the way you acquire and retain customers will require serious re-evaluation. Marketers will need to restructure advertising strategies and modernize creative production approaches to continue to meet KPIs in a privacy-friendly way.

While we're not set to feel the full brunt of these changes immediately, it's essential to start revamping your strategies now. To get you started, we're bringing clarity to the muddied data privacy landscape and presenting viable solutions.

In this guide, we'll dive into:

- A timeline of how the privacy landscape has evolved
- Easy-to-digest summaries of major regulatory acts
- How brands and publishers are responding
- The solutions currently being explored to retain some aspects of granular targeting
- Strategies to fuel your creative approach in a privacy-friendly way

Table of Contents

The Data Privacy Landscape Timeline

2016

Apr 2016
General Data Protection Regulation (GDPR) introduced

2017

Jun 2017
Apple releases Intelligent Tracking Prevention (ITP)

2018

May 2018
General Data Protection Regulation (GDPR) implemented

Jun 2018
California Consumer Privacy Act (CCPA) signed into law

2019

2020

Jan 2020
Companies must make sure they meet all CCPA guidelines

Jan 2020
Google announces third-party cookie deprecation

Mar 2020
New York SHIELD Act goes into effect

Mar 2020
Apple blocks third-party cookies on Safari

Sep 2020
Apple releases iOS 14

Nov 2020
California Privacy Rights Act (CPRA) passes, expands on CCPA

2021

Mar 2021
Virginia Consumer Data Protection Act (CDPA) signed

Apr 2021
IDFA limitations with iOS 14.5 update

Jun 2021
Apple Releases iOS 15

Jul 2021
Colorado Privacy Act signed

2022

Mar 2022
Utah Consumer Privacy Act (UCPA) signed

May 2022
The Connecticut Privacy Act is approved

Jun 2022
Firefox rolls out Total Cookie Protection by default to all users worldwide

Sep 2022
Apple releases iOS 16

2023

Jan 2023
California announces an enforcement sweep aimed at mobile apps that do not comply with the CCPA

The Key Regulatory Forces Reshaping Data Privacy

General Data Protection Regulation (GDPR)

Likely the most well-known data privacy regulation, the General Data Protection Regulation (GDPR) is the strongest set of data protection laws in the world. It is credited with kicking off an international wave of changes after it was introduced in 2016 and put into effect in 2018.

The primary goal of the GDPR is to unify data privacy laws across the European Union to provide greater protection for individuals by modernizing the ways organizations collect and handle data from their consumers. Even if your organization isn’t located in the European Union, if you collect personal data from E.U. residents, you are responsible for being GDPR compliant.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

The GDPR limits the ways organizations can harvest and commodify the personal data of European Union residents through seven key data protection principles:

1. Data must be processed lawfully, fairly, and transparently.
2. The data you collect should be limited to the legitimate purposes specified explicitly to the user.
3. You must minimize the data you collect only to what is absolutely necessary for the purposes specified to the user.
4. Personal data must be accurate and kept up to date.
5. Data may not be stored longer than necessary for the specific purpose.
6. Processing data must ensure appropriate security, integrity, and confidentiality, like through the usage of encryption, or other privacy methods.
7. Organizations must remain accountable by demonstrating their compliance with these GDPR principles.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) secured new privacy rights for California residents and took effect in January 2020. This act is incredibly similar to the GDPR. For example, like the GDPR, whether or not your organization is located in California, businesses are required to comply with CCPA regulations if they collect any personal data from California residents.

The CCPA is a boon for individual users as it gives them more autonomy for what information they share, but know that the act is only applicable to certain businesses. Your organization must remain CCPA compliant if it:

- Has a gross annual revenue of over $25 million;
- Buys, receives, or sells data from 500,000 or more consumers, households, or devices;
- Makes 50% of its annual revenue from selling consumer data.

While they are similar, the CCPA and GDPR have separate legal frameworks. If you are compliant with GDPR but are also subject to the CCPA, your organization may have additional obligations that will need to be addressed.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

Another major difference from the GDPR, however, is that the CCPA doesn’t require businesses to ask permission from users first before harvesting data. The CCPA gives consumers rights, which are divided into four principles:

- The right to know what personal data is collected, used, shared, or sold.
- The right to delete any personal data held by businesses and their service providers.
- The right to opt out of the sale of personal data.
- The right to non-discrimination in terms of price or service when a user exercises a privacy right under the CCPA.

California Privacy Rights Act (CPRA)

California expanded on the CCPA in November 2020 with the passage of the California Privacy Rights Act (CPRA). This addendum helps fix loopholes left in the CCPA, like redefining the definition of businesses to exclude small and mid-sized businesses and focusing on larger enterprise entities that collect massive amounts of data.

It also updates the right to opt-out to directly regulate cross-site advertising and offers more transparency to consumers about how personal data is shared across websites, applications, and services. The new act also establishes the California Privacy Protection Agency (CPPA) to supervise and ensure that businesses comply with both CPRA and CCPA regulations.

As of January 1, 2023, the act also allowed consumers the right to correct inaccurate information that a business has about them and the right to limit the use and disclosure of sensitive personal information collected.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

Virginia Consumer Data Protection Act (CDPA)

In March 2021, Virginia became the second state to enact sweeping data privacy regulations with the Virginia Consumer Data Protection Act (CDPA), granting its citizens more control over their personal data.

The CDPA applies to any businesses that:

- Control or process data from at least 100,000 users;
- Or sell and collect personal data from 25,000 users while making 50% of their annual revenue from these personal data sales.

A major difference between Virginia's CDPA and California's CCPA is that there is no monetary threshold for which businesses must remain compliant. That means that even large-scale enterprise organizations will not have to be compliant with the CDPA so long as they do not fall under the act's applicable rules.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD)

New York's SHIELD Act is the East Coast version of California's Consumer Privacy Act. While the act utilizes many of the same frameworks from the CCPA and the GDPR, it is markedly different. Where the CCPA is a data privacy law, the SHIELD Act is a security regulation that amends the state's data breach disclosure law.

This broadens the scope of what a data breach entails to include any unauthorized access to private and/or personal information. The SHIELD act also makes significant changes to the definition of private user information. It expands protections to biometric data, like thumbprint and facial recognition, as well as user email addresses, passwords, and security questions. Like with other privacy regulations, businesses outside of New York State must still remain compliant with the SHIELD Act if they collect data from New York residents.

The SHIELD Act and the CCPA are primed to make a dramatic impact on nationwide privacy laws due to the fact that New York and California consumers make up nearly 18% of the total US population. This means most major businesses are impacted by these regulations.

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

Congressional Momentum for Federal Data Privacy Regulations

Since the implementation of Europe's GDPR in 2018, momentum has continued building for the United States Congress to pass national data privacy regulations.

This has been compounded by a litany of recent high-profile data breaches—from Microsoft to the popular video game Fortnite—that have put the protection of individual personal information under increased scrutiny. Federal regulations would help unify the data privacy laws across the country, setting a nationwide standard.

Federally-recognized data privacy protections are important as they will also end the hoops businesses must currently jump through to be compliant with the various state-sanctioned regulations. As Jon Leibowitz, chairman of the 21st Century Privacy Coalition, told the Senate Committee on Commerce, Science, and Transportation, "A proliferation of different state privacy requirements would create inconsistent privacy protections for consumers...you don't want a cacophony, or crazy quilt patchwork of 50 different state laws."

The Key Regulatory Forces Reshaping Data Privacy (Cont'd)

In addition, as Senator Brian Schatz from Hawaii told The Hill, “The reason to lay down broad principles and let the FTC referee this is that we have no idea what kind of data will be collected 15, 25 years from now and we want a statute that can stand the test of time.”

In June 2022, the American Data Privacy and Protection Act was introduced in the House of Congress. No further movement has been made on the bill as of early 2023. The key elements of this act would create regulations around:

- How companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual.
- How companies collect, process, and transfer personal data.
- Consumer data protections, including the right to access, correct, and delete personal data.

The Impact on Devices, Browsers, & Marketers

In response to the government-imposed regulations impacting the world of data privacy, tech companies have announced a series of changes to remain compliant. The impending changes will establish a new world order for marketers, fundamentally restructuring the role consumer data plays in targeting, measurement, and attribution.

Apple

Apple’s Identifier for Advertisers (IDFA)

You’ve likely read the hyperbolic headlines about Apple’s contentious iOS14 update that “kills” the IDFA—or Identifier for Advertisers—that tracks user activity across different apps on an iOS device. But that’s not exactly what’s happening.

Apple isn’t phasing out the IDFA, rather they are providing iOS users with increased transparency into how their data is collected and used.

Apple’s iOS14 update provided an additional layer of transparency for its users by asking them to opt-in to sharing their data with third-party apps. This feature, called App Tracking Transparency, requires user authorization before any app can collect data that is then shared with other companies for purposes of tracking user behavior across apps and websites. Before the update, users were automatically opted-in and had to manually opt out of data tracking and sharing.

Data Sharing Solutions for Apple Devices

Because Apple has over 1.6 billion users, the updates to the IDFA will have sweeping impacts for virtually every brand targeting iOS devices. Social apps like Facebook have bristled at the transparency that Apple is providing its users. They argue that, with less granular data on target audiences, small businesses will have greater difficulty reaching their core consumers.

Apple (Cont'd)

Because of this, solutions are being devised to help organizations still reach their audiences while remaining sensitive to changing attitudes on data privacy:

SKAdNetwork

In 2018, Apple introduced an alternative, privacy-oriented solution for tracking user data outside of the IDFA. On the SKAdNetwork (StoreKit Ad Network), when a user clicks on an ad that leads to an app download, that data is stripped of any user-level or device-level data before being sent to the ad network, where it can be accessed by the advertiser. The SKAdNetwork will tell app developers when their product is downloaded, but it does not provide information on any other event that results in a conversion.

This solution comes with its own set of limitations. Because the SKAdNetwork lacks any granularity on which users are interacting with your ad, advertisers will need to shift from persona-based targeting to a contextual method. Marketers will need to pinpoint which platforms, rather than users, their content performs best on, and then optimize their campaigns through creative strategies like multivariate testing.

Apple (Cont'd)

Apple Search Ads

Another point of contention for Apple’s changes to the IDFA is the theory that it gives preferential treatment to its own advertisements in the Apple Search Ads network. Where Apple’s updates to the IDFA make users opt-in to sharing their data with third parties, it doesn’t provide the same service for Apple-delivered advertisements. Users will still need to opt out of personalized ads from Apple’s own network.

That being said, a way to combat the loss of granular tracking is simply by reinvesting in the Apple Search Ads network. Look for opportunities to get in on the ground floor of target keywords to heighten your brand’s visibility before the competition increases as App Tracking Transparency and the SKAdNetwork become the norm.

Android

The IDFA and App Tracking Transparency updates above will only impact iOS users. Android, however, has implemented new safety measures to ensure the data privacy of their customers.

They provide users with the ability to control when to share certain sensitive data with apps they download. For example, the updated protections allow users to grant applications access once, never, or always, allowing each individual user to customize their data experience.

Firefox and Safari

Mobile users aren't the only ones who will be directly impacted by the changing sensitivity toward data privacy. Web browsers, like Firefox and Safari, have made decisions to phase out cross-site tracking on their platforms.

In 2018, Firefox revealed plans to block cross-site tracking in an effort to mitigate harmful data collection practices through third-party cookies. One year later, they introduced Enhanced Tracking Protection (ETP) that blocked, by default, third-party cookies on their platform.

Apple rolled out their own set of anti-tracking features for their Safari browser called Intelligent Tracking Prevention (ITP). In its initial iteration, the feature forced trackable domains to purge third-party data after 30 days of inaction. Since then, the ITP has been iterated on multiple times. In its most recent update in March 2020, the ITP fully blocked third-party cookies on Safari, as well as on all iOS devices.

Google Chrome

Google's phase-out of third-party cookies on their Chrome browser parallels the privacy regulations already in place on Firefox and Safari. Chrome's changes, however, are taking place a bit more slowly than their predecessors.

The first announcement was released in 2020, with an anticipated finalization of the process by the end of 2022. The latest update states they will "begin phasing out third-party cookies in Chrome in the second half of 2024."

As Chrome accounts for more than half of all global web traffic, when Google's changes go into full effect, nearly every marketing team will be affected. Advertisers tracking any one of the 2.6 billion Chrome users won't be able to collect, use, or retain any of that user data.

Google Chrome (Cont'd)

Data Sharing Solutions

Google knows the depreciation of the third-party cookie will create significant challenges for marketers. That's why they're also trying to create a solution that meets data privacy guidelines while also providing advertisers with the information they need.

Their proposed solution for limitations on granular tracking is the Google Privacy Sandbox, where non-identifiable data is stored across the web and Android applications.

By implementing the Sandbox, Google aims to:

- Build new technology to keep your information private
- Enable publishers and developers to keep online content free
- Collaborate with the industry to build new internet privacy standards

Google summarized the mission best: "Improving people's privacy, while giving businesses the tools they need to succeed online, is vital to the future of the open web."

Privacy-Friendly Approaches to Data-Driven Video Creative

In addition to the solutions being explored by tech giants, a number of other publisher-led initiatives are underway to preserve some aspects of the targeting, retargeting, and attribution capabilities marketers have come to rely heavily on.

Still, the world modern marketers operate in is fundamentally changing, and the level of granular audience data you've become accustomed to is becoming a thing of the past.

Next Steps

To remain effective, you must reevaluate your creative strategies. There are two clear privacy-friendly approaches that can be integrated into plans immediately:

1. Use your creative to surface data and insights.
2. Diversify your marketing strategy.

Let's dive into these in more detail.

Use Your Creative To Surface Essential Insights

As retargeting opportunities fade into the background, brand creative will likely begin to skew toward more awareness and top-of-the-funnel concepts. Since you'll know less about your audience at the targeting level, it's likely best to start with more general creative.

Even within a broader approach, you can pinpoint the creative variables that resonate most with your audiences. Over time, these data can produce audience insights, which can be invaluable to many aspects of your business. Once you know which broad ideas work best, you can begin iterating and refining your video strategy.

A Step-by-Step Guide

STEP 1: Identify Platforms, Placements, and KPIs

At the start of your campaign, identify all of the platforms and placements you plan to run on, as well as your core KPIs. The audiences you will be able to reach will vary from platform to platform—and even placement to placement on a single platform.

Use Your Creative To Surface Essential Insights (Cont'd)

STEP 2: Create a Custom Testing Strategy

With your KPIs in mind, construct a performance testing plan to methodically test key variables within your creatives through multivariate testing.

With multivariate testing, you can continuously optimize your content and give your audience what they really want. Identify the variables you want to test in the next round and edit your creatives with that winning concept accordingly.

The list of variables to test is nearly endless. To get started, ask yourself what you want to learn about your audience. Maybe you want to see if they respond to a certain type of talent or you want to figure out which of your key value props have the most pull. You can also take a look at the performance of your previous creative.

Plus, here are some examples. You may want to test:

- Customer testimonial vs. lifestyle content
- Live action vs. animation
- Locations
- Messaging styles
- Product focus vs. brand focus
- Talent vs. no talent
- Value propositions

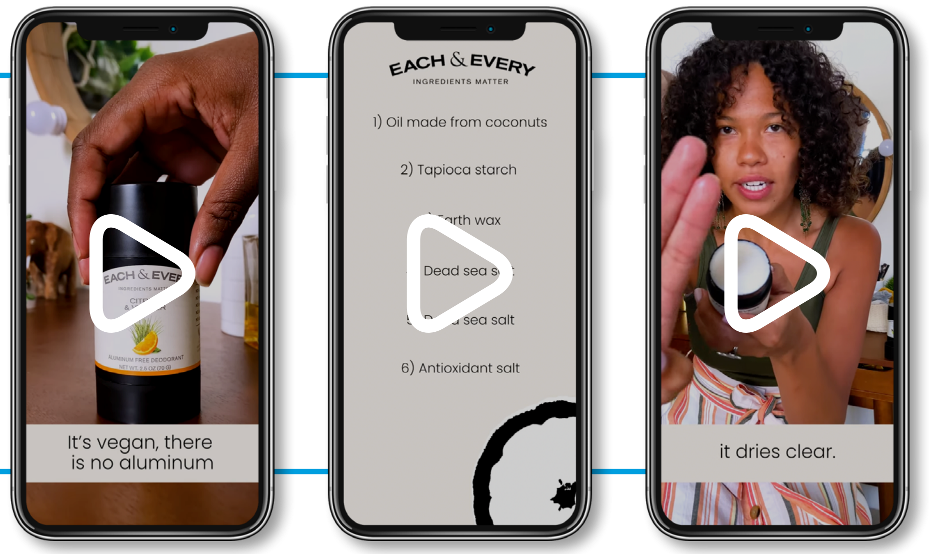
Use Your Creative To Surface Essential Insights (Cont'd)

Don’t have video data? Don’t worry!

You don’t need to have run video before in order to generate learnings—looking at the performance of still image assets will also surface insights.

Once you’ve identified the variables you want to test, build a multi-month testing plan. You’ll want to start broad, testing conceptual approaches first. Then, hone in on effective variables through methodical testing.

See how this beauty brand used QuickFrame to methodically test the effectiveness of different talent.



STEP 3: Get Ready for Production

Once your testing plan is sketched out, you need to identify your creative concepts and variables of interest. This information will be key to the next phase of pre-production, which is generating a shot list.

Use your plan to build an exhaustive shot list to ensure you capture all of the necessary footage for your entire campaign. Since the collection of shots will be the building blocks of the video ads you’ll create and iterate on, this list is essential.

Use Your Creative To Surface Essential Insights (Cont'd)

STEP 4: Capture Your Footage

Once you have your testing plan and shot list ready to go, it’s time to capture the footage!

To maximize your budget, try to get everything you need in a single shoot. Schedule all of your on-screen talent to shoot on the same day. You’ll also want to aim to capture all of the product photography and b-roll you’ll need in as few locations as possible.

STEP 5: Campaign Launch and Data Collection

After your shoot, it’s time to edit together the first set of video content and launch your campaign. In the first round, test broadly and focus on high-level attributes like concepts and styles.

Let your creatives run for 1-2 weeks and track your KPI at the creative level. Which concept was more successful at driving your KPI? Identify the winner and continue optimizing your content through more and more specific testing.

Use Your Creative To Surface Essential Insights (Cont'd)

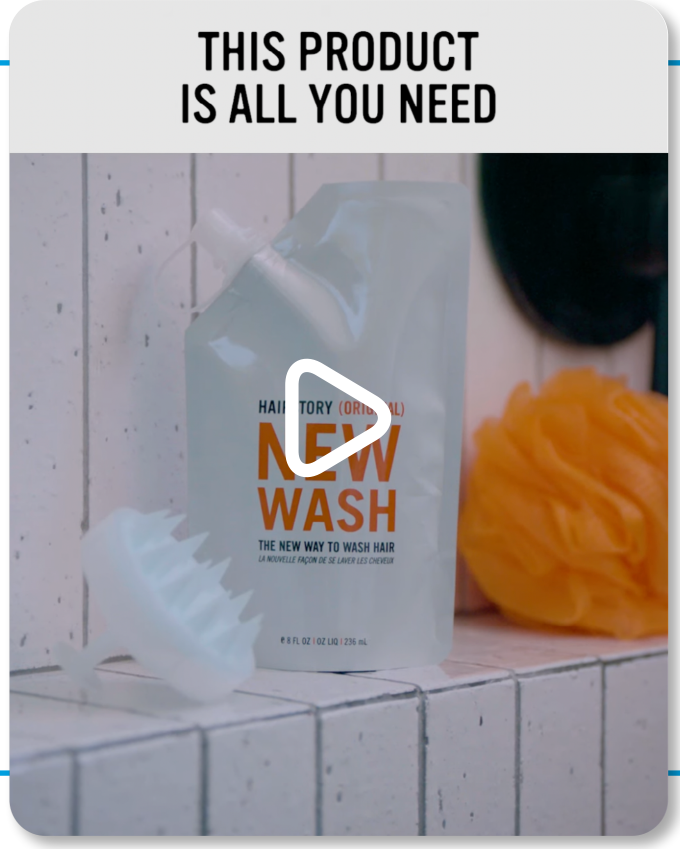
STEP 6: Iterate and Optimize

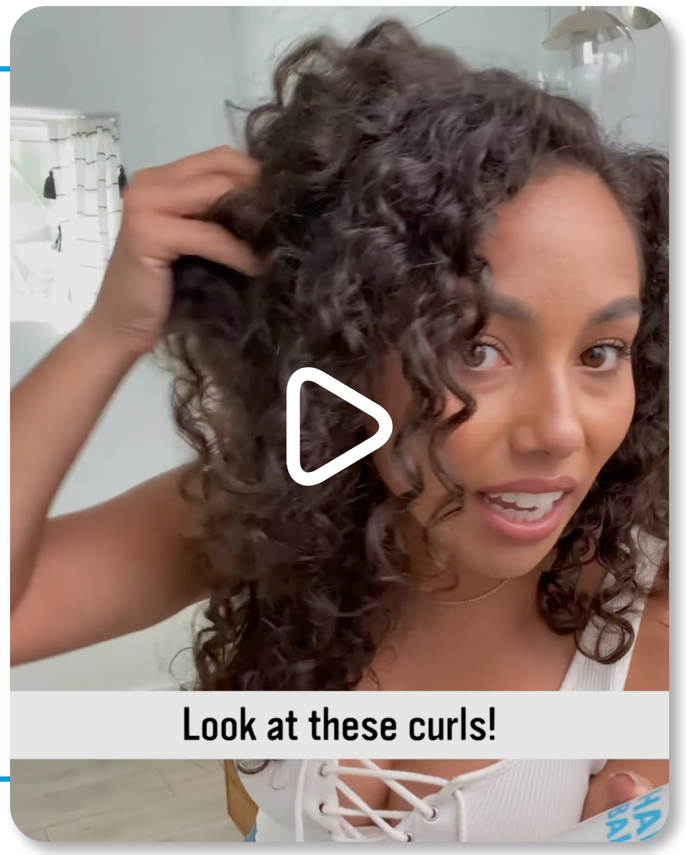
Take the winning concept from the first round and move it on to the next stage of your testing strategy: iterating and optimizing it!

Because you captured a library of footage in your initial shoot, you can swap out shots with ease through post-production techniques. Since no additional shoots are required, new assets can be turned around quickly, sometimes in just 24-48 hours.

Again, once this round of creatives is ready, it’s time to publish. Let these videos run for 1-2 weeks, monitor performance, and collect data to analyze.

See how this hair brand built a performance testing plan with QuickFrame and uncovered that narrative-driven UGC-style client testimonials were more effective with their audiences than product-focused concepts.





Use Your Creative To Surface Essential Insights (Cont'd)

STEP 7: Iterate and Optimize

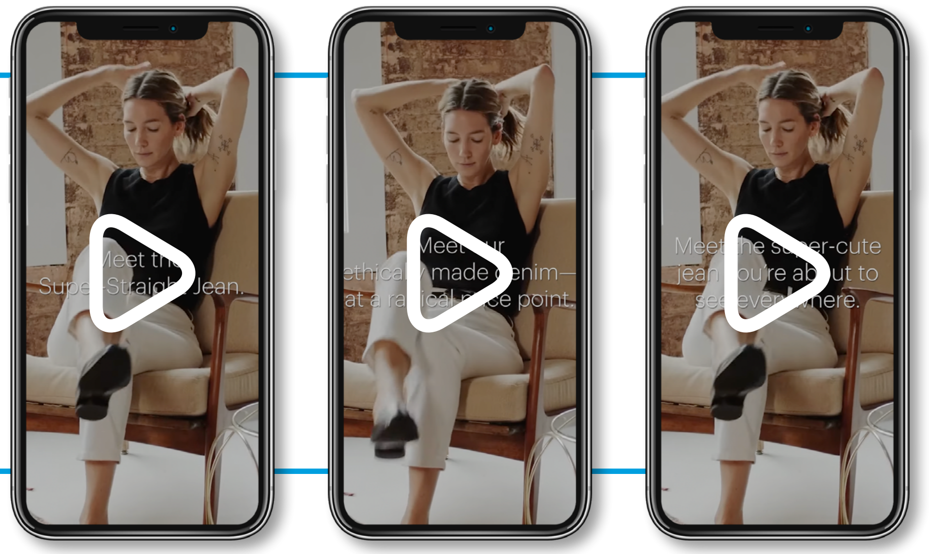
Do it again!

The creative insights you learn from multivariate testing will continue to become more granular, as you understand the concepts, themes, and styles that are most effective for your audience. Each week as you monitor performance, you grow your library of data, learning which creative attributes work best for your brand.

After a campaign wraps, you'll have solid insights generated by your creative data that will inform the pre-production planning of your next campaign. Use these insights to not only finetune your creative strategy but also to extrapolate broader learnings about your audiences that can be applied to other aspects of your business.

Through an ongoing, effective testing strategy, you'll be able to continuously optimize your video creative, driving higher engagement with your audience.

See how this fashion brand used QuickFrame to affordably test various messaging.



Diversify Your Marketing Mix

Since data privacy regulations will limit your ability to confidently target specific consumers across the funnel, you'll need to lean into first-party and additional audience-related data.

All platforms have overviews of their audience demographics and content consumption habits—use these to see where you need to be publishing.

Don't be surprised if you realize your platform distribution needs to grow—drastically. Consumers are increasingly using more platforms (for varying purposes, including watching Connected TV) on a daily basis, making your audience more spread out than ever before.

In order to get granular data and audience insights, brands must adopt the experimentation mindset outlined above on multiple fronts: at the platform level, the placement level, and the creative level. Diversifying platforms and placements will be key to locating where your target audiences are receptive to your content. Then, creative-level multivariate testing will surface the creative variables most effective for each one.

Update Testing Strategies as You Diversify

Your audience is not homogenous, and they're having unique content experiences across each platform. Once you diversify your platform mix, update your testing strategy to account for the new platforms.

Create platform- and placement-specific testing strategies to ensure you're learning as much as possible about the user experience and increasing the granularity of your data.

You may be asking yourself, “How do MNTN and QuickFrame work together?”

MNTN’s Connected TV advertising platform allows brands to drive measurable conversions, revenue, site visits, and more by giving them the power to tie performance directly back to their television campaigns. Learn more at mountain.com.

QuickFrame gives brands access to a network of creators who can build high-performing video for every channel, audience, and objective, at scale and backed with exclusive performance data. Learn more about QuickFrame!

But MNTN and QuickFrame work even better together. QuickFrame powers MNTN’s Creative-as-a-Subscription service, which bundles creative production into the cost of media—providing advertisers with the ability to quickly produce net-new ad creative—as well as refresh existing campaigns, so they are investing their budget solely in video that drives performance. Learn more about the service here.