The Marketer's Handbook to Data Privacy Regulations (and How to Respond)

QuickFrame

The world of digital marketing and advertising is fundamentally changing.

An increased governmental 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.

Marketers haven't seen an impact this large since the invention of the cookie more than two decades ago. Cookies opened the door to tracking users across the web, unlocking the capability for granular targeting with personalized creative. The mechanisms behind targeting and retargeting have grown in number over the years, but now, data privacy regulations are set to make these core marketing tactics a thing of the past.

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

It's easy to postpone any major shifts in your strategy since we're not due to feel the full brunt for another year or two. But a passive mindset here is a dangerous one—before you know it, the tools you've come to rely on to hit your goals and grow your business will no longer be there.

Now's the time to reevaluate your marketing and creative operations, and to start integrating novel approaches. To get you started, we're bringing clarity to the muddied data privacy landscape, and presenting viable solutions.

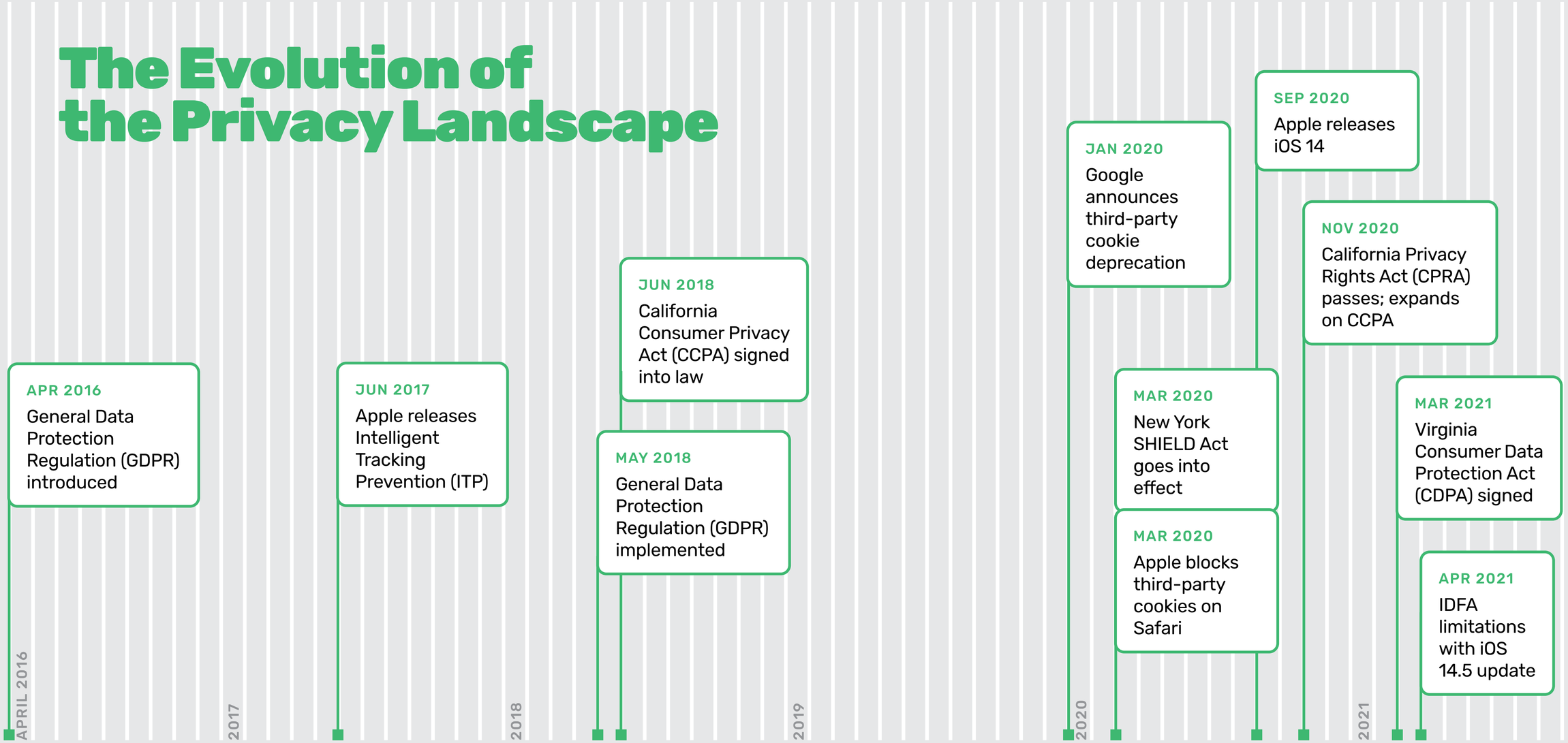
IN THIS GUIDE, WE'LL DIVE INTO:

- A **timeline** of how the privacy landscape has evolved over the past 5 years, so you can get a sense of the forces behind the changes
- Easy-to-digest summaries of major **regulatory acts** and how tech companies plan to respond
- The **solutions** currently being explored to retain some aspects of granular targeting
- How you can **revamp your creative production approach** to get data and insights to fuel your advertising strategy in a privacy-friendly way

Let's roll.

Table of Contents

The Evolution of the Privacy Landscape



The Regulatory Forces Reshaping the World of Data Privacy

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the strongest set of data protection laws in the world—and is credited with kicking off an international wave of changes after it was introduced in 2016.

The GDPR limits the ways organizations can harvest and commodify personal data of European Union residents. The primary goal of the GDPR was to "harmonise" 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 now responsible for being GDPR compliant.

When the GDPR was implemented in 2018, it revised laws that had been in place for almost 30 years. The amount of data we freely share has changed dramatically since the 1990s. Those old regulations couldn't predict the myriad of ways in which our data has been monetized today. The GDPR simply brings historical privacy regulations into the 21st century.

There are seven key data protection principles in the GDPR:

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.

California Consumer Privacy Act (CCPA)

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

One major difference from the GDPR, however, is that the CCPA doesn't require businesses to ask permission from its users first before harvesting data. The rights the CCPA gives to consumers 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.

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 **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.

For example, the GDPR requires businesses to create processes to respond to individual requests for access to personal information. This is also a requirement of the CCPA, but organizations will need to review the different definitions of personal information, and the rules on verification of consumer requests, to remain compliant for both.

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 offer 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.

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 that 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.

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. The act clones many of the same frameworks that make up the CCPA and the GDPR, but 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 18% of the total US population. This means most major businesses are impacted by these regulations.

Congressional Momentum for Federal Data Privacy Regulations

Since the implementation of Europe's GDPR in 2018, momentum has been 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.

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."

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."

We can expect to see this momentum continue to build in the near future. As of March 2021, new regulations are already being proposed, like the **Information Transparency and Personal Data Control Act**. The act's goal is to provide the nation with fair and thoughtful digital consumer rights by developing a digital privacy framework that complements current global standards set by the GDPR.

The act explicitly states that individuals have the right to:

- Maintain control over the usage of the personal data companies collect
- Access easily understandable information about privacy and security practices
- Ensure companies will collect, use, and disclose data that's consistent with the context in which it's provided.
- Secure and responsible handling of sensitive personal information
- Update personal information to keep data sensitivity and consumer consequences for inaccurate data in mind
- Reasonable limits on the personal data companies collect and retain

Q&A: The Role of the Consumer

JOSEPH REID
COO
QUICKFRAME

THIS INTERVIEW HAS BEEN EDITED FOR CLARITY.

What's fueling the surge we're seeing in data privacy regulations?

I spent about five years in Europe. When I landed in England in 2017, it was super interesting because in terms of the privacy vanguard, it was nowhere to be found. People were just freely harnessing information from the internet in lots of different capacities and then using that information to understand consumer behaviors, launch products, and establish virality. It was really the wild west. But at the fringes—and this was in Western Europe—privacy regime was starting to emerge.

I was working for a data business at the time and I was starting to see obstacles being put up in certain countries. Each country had their own take on data privacy policy. And then, 2018 came along, and it reached political surfaces with the Cambridge Analytica scandal where we realized data was being siphoned off in the service of better political targeting. So then you have this emergence of scattered European privacy policy with Americans also waking up to the fact that all of the stuff we're putting into Facebook actually has utility for someone.

Up until that point, we had kind of accepted that the quid pro quo for the free internet was—ostensibly—that you could target ads at me. That was the mechanism by which we could rationalize having access to the most amazing learning tool in the history of mankind. People now started to realize that maybe it's not as evenly distributed of a relationship as that.

So we have the European legislation and the Cambridge Analtyica thing—and out of that primordial soup comes GDPR. And now the world is becoming much more aware as a result, I think, of a lot of European efforts. And we've seen it, now, kind of leak into the Americas with CCPA and talks of a federal policy regime in regards to data.

We've seen this logical push and pull in the last few years. There were a couple of consumer activists that helped governments become more aware. They helped wrestle down the idiosyncratic nature and made it cross a Pan-European policy. That Pan-European policy has now crossed the Atlantic, creating waves in terms of American consumer understanding of internet policy.

And then you have the private sector—these enormous, monolithic businesses like Apple and

Google that are the gatekeepers of the business—following suit, trying to seize the moral high ground and position themselves as a better advocate for consumers.

Why do you think this movement is happening now?
The general awareness of consumers waking up to exactly how their information is being leveraged is what's driving this movement. We've seen large swaths of consumers affected by data breaches in recent years—whether it was the Experian data breach or breaches at digital retailers, as just a couple of examples.

Consumers have become much more aware of evidence that data may be used against them. I think there is enough consumer frenzy now that these companies are responding to what they perceive to be consumer desire.

Are marketers appropriately preparing themselves for the new data privacy landscape that's on the horizon?

Marketers—now more than ever—understand that consumer engagement needs to be more personalized and more relevant. Marketers were just going through the hard work of making sense of all the data out there and consolidating it to serve up the most relevant creative possible to each target.

I think that in the new paradigm that's being presented in this cookie deprecated, iOS14-managed world, marketers will have to walk a lot of the last 5-10 years of data mastery back. They will need to repurpose their understanding of consumer engagement. It's going to look a lot different in the next couple of years because all of those discrete targeting pools of consumers that we have built up are going to be exploded.

"Now it's very much going to be a consumer-controlled conversation."

What do you think a privacy-friendly advertising landscape will look like?

I think there's going to be a consent component, which involves having documentable, explicit, and discreet consent from consumers to talk to them in the way they want to be reached. The paradigm used to be the brand talking to the consumer—now it's very much going to be a consumer-controlled conversation.

The problem with that consent-driven architecture, though, is that brands really need scale—you need to get your message out to as many people as you can. What marketers will have to resort to is more creative iteration and testing. Ironically, I think we are going to revert back to a much wider distribution of creative assets that are going to be used to test and winnow repeatedly.

I think that's the way it seems to be going. At QuickFrame alone, we've seen a huge demand for middle-of-the-funnel creative. It's looking like marketers are going to move to creative treatments higher up the funnel, and do a lot more creative iteration and testing to get consumers from awareness to advocacy.

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'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 really the best way to describe the privacy restrictions Apple is putting in place.

Apple isn't phasing out the IDFA, rather they are providing iOS users with increased transparency into how their data is collected and used. What Apple's iOS14 update does is provide 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, will require 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, but this new feature requires users to explicitly opt-in.

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. The argument is that, with less granular data on target audiences, small businesses will have greater difficulty reaching their core consumers.

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 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 makes 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 personalised 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.

What About Android Devices?

If it wasn't plainly evident, the IDFA and App Tracking Transparency updates will only impact iOS users. Advertisers will still have access to Android's base of over 2 billion users. However, Google is in the exploratory phase to change that. There haven't been any concrete plans for anti-tracking features on Android, but Google aims to be less restrictive with its solution so as to not diminish the reach of advertisers, while still meeting demands for stricter privacy regulations.

Firefox and Safari

Mobile users aren't the only ones who will be directly impacted by the changing sensitivity towards data privacy. Web browsers like Firefox and Safari have already begun making moves 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. However, as Chrome accounts for more than half of all global web traffic, when Google's changes go into full effect by the end of 2022, the seismic impact of the third-party cookies demise will be profoundly felt across the internet. 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.

Data Sharing Solutions for Google Chrome

Google is trying to solve a challenge of their own making. Their proposed solution for limitations on granular tracking is the Google Privacy Sandbox, where non-identifiable data is stored inside the Chrome browser.

The Sandbox replaces the cookie with five application programming interfaces (APIs) that collect aggregated data, like Conversions and Attributions. These five APIs are:

1. **Trust Token:** This is Google's alternative to CAPTCHA that authenticates a user without revealing personal information. When a user completes a CAPTCHA-like program, they will receive a "trust token" that proves to advertisers they are a real-life user, and not a bot. These cryptographic tokens are anonymous, and indistinguishable from each other so they cannot be used to track users across the web.

2. **Aggregated Reporting:** This allows for ad measurements without relying on cross-site tracking by storing user data in the Chrome

browser. These data points are aggregated into a single, privacy preserving report so advertisers can see metrics for reach, views, impressions, and more.

3. **Conversion Measurement:** Similar to Apple's SKAdNetwork, this API will tell advertisers whether a user converts by clicking on an ad and purchasing the product being sold. Advertisers will be informed when a conversion happens, but they won't have access to any unique personal information about the user.

4. **Federated Learning of Cohorts (FLoC):** This API offers an alternative to interest-based targeting where businesses focus on a large cohort of users, rather than individuals. With its machine learning algorithm that stores data in the browser, FLoC develops these cohorts based on the sites that an individual user visits, the content of those pages, or other factors. No individual data is shared, only the anonymous cohorts FLoC generates.

5. **Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE):** That's a lot of words to describe a solution to retargeting! With TURTLEDOVE, advertisers can program codes on their site that assign users to specific interest groups for the purposes of retargeting. When serving an ad to these users, two requests for ads are sent: one that's based on the interest group, and the other on the context of the website they visited, but not tied to any other browsing data. TURTLEDOVE is still in its infancy, but Google has begun testing this functionality through a proposal called FLEDGE, or First Locally-Executed Decision over Groups Experiment, in 2021.

Q&A: How Brands and Publishers are Responding

ALYSIA BORSA
PRESIDENT OF DIGITAL
MEREDITH CORPORATION

THIS INTERVIEW HAS BEEN EDITED FOR CLARITY.

What are the high-level changes in the marketplace that have impacted data capture and data use cases?

First and foremost is privacy. The second is browser and platform changes. Those are the two things that are impacting our ability to capture and use data the way we have been in the past.

From a privacy perspective, it all started with GDPR in Europe. It has moved to CCPA and CPRA in California and there are a number of other states that have implemented regulations, as well as conversations about federal privacy regulations that are going to potentially happen over the course of the next several years.

There's a common theme across all of these regulations. First: expanding the definition of "personal consumer data." That used to be name, address, email—those types of data points. That's now expanded to cookies and IP address—a much broader definition of what consumer data is.

There's also been a theme in all of these regulations of increasing transparency for consumers, so making sure they are more aware of what data is being captured and what data is being used.

And finally, these regulations work to increase the choice that consumers have. This includes the ability for consumers to not only know what data is being captured, but also to prevent it from being sold or shared beyond the company that captured the data.

What's having the biggest impact on our industry?

It's not the privacy regulations that I think are having the greatest impact on our ability to capture data, it's the browser and platform changes that are limiting the capture and use cases of data even more greatly.

What are brands and publishers doing in response?

What all of these changes really mean is that good, quality data and insights are going to become even more important as we go forward. As a publisher, our approach is to—first of all—make sure we advocate for all of the privacy changes. I do believe it's important for us to

be more transparent and provide consumers more choice.

I also believe that every publisher needs to have a first-party data strategy in place to make sure they are taking full advantage of the data and the insights that they have. Data is one thing, but if you can't talk about the "so what?" related to your data, your data means nothing.

I do know publishers are particularly focused on our audience insights, identifying how to preserve the ability to identify, understand, and target different audience segments. But we're also doubling-down on contextual data. Contextual data is key, taxonomy is key—those insights (again) are really key to the business. There are a ton of industry consortiums happening to try to address our overall ability to continue to capture and use data in a privacy-compliant manner.

I think brands are also building out their data strategies, but there are definitely haves and have-nots. A lot of brands have realized that they have no direct consumer data. Some do

"It's not the privacy regulations that I think are having the greatest impact on our ability to capture data, it's the browser and platform changes."

and some have been working on it, but I feel like there's quite a spectrum from a brand perspective. There seems to be a big wake up call and a big push from brands to try to get data and collect sources for insights.

What do you think the future landscape will look like?

1. We're going to continue to have more privacy regulation and likely some federal regulation in the U.S. coming soon.
2. Platforms are going to continue to try to limit data.
3. Those companies that do have compelling data and insights that can be shared effectively and in a privacy-safe manner are going to have a very big advantage as we move forward.

Privacy-Friendly Creative Approaches That Generate Insights

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.

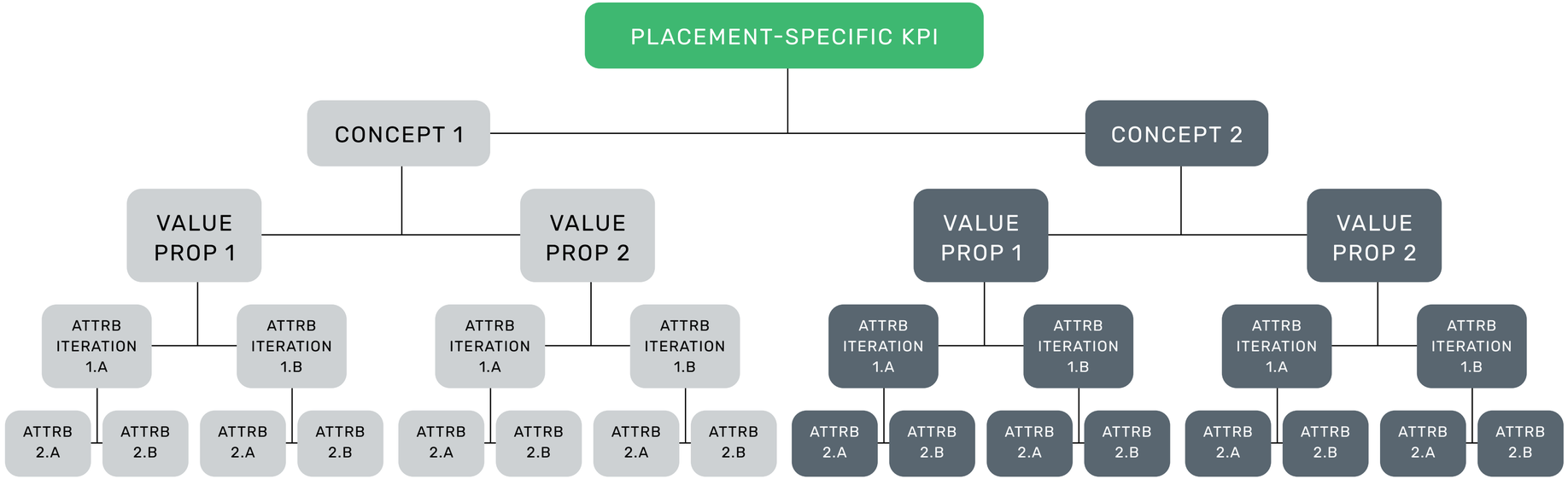
To remain effective, you must reevaluate your creative strategies. There are two clear privacy-friendly approaches that can be integrated into plans immediately: **harnessing creative-level data** and **platform diversification.**

Using Your Creative to Surface Audience Insights

As retargeting opportunities fade into the background, brand creatives will skew towards more awareness/top-of-the-funnel concepts. Because you'll know less about your audience at the targeting level, it'll likely be best to stick to more generalized creatives that you know will have a broad impact.

Still, even within a broader approach, you can start to pinpoint the creative variables that resonate most with your audiences. Over time, these data produce audience insights that can be invaluable to many aspects of your business.

Here's a step-by-step approach that outlines how you can surface insights by taking a novel approach to your creative planning and execution.



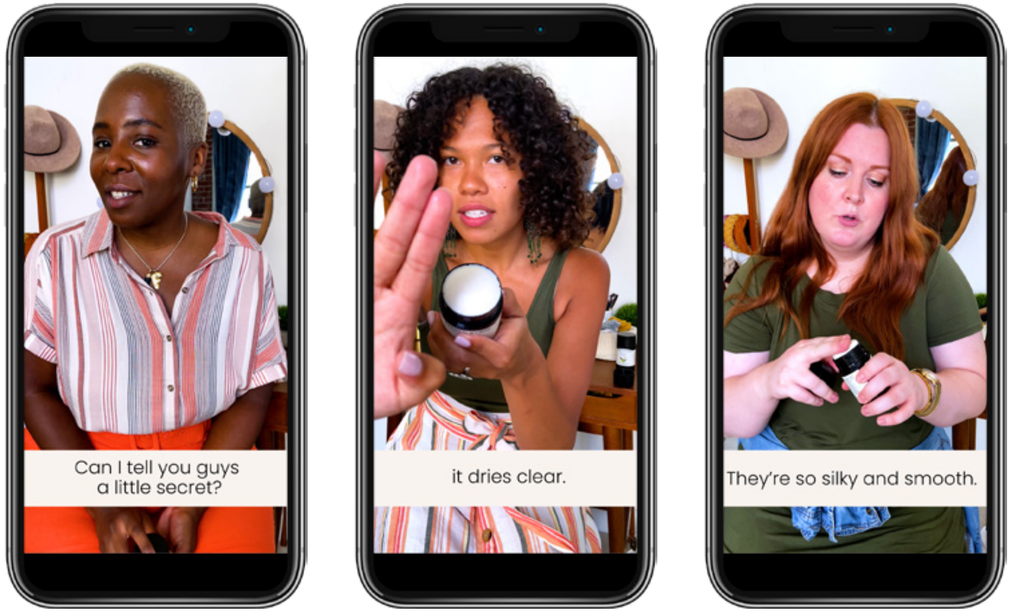
STEP 1: IDENTIFY PLATFORMS, PLACEMENTS, & KPIs

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.

STEP 2: DRAW UP A TESTING PLAN

With your KPI in mind, construct a performance testing plan that will methodically test key variables within your creatives. To identify variables for testing, ask yourself what you want to learn about your audience. Perhaps 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.

If you don't know where to start, take a look at your historical creative performance and identify top-performing and low-performing creatives. See if you can identify commonalities amongst both sets of creatives and start your brainstorm there. 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.



Each and Every used QuickFrame's performance marketing solution to methodically test the effectiveness of different talent.

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.

EXAMPLES OF CONCEPTS YOU MAY WANT TO TEST ARE:

- Talent vs. No Talent
- Live Action vs. Animation
- Customer Testimonial vs. Lifestyle
- Product Focus vs. Brand Focus

CREATIVE VARIABLES AND ATTRIBUTES YOU MAY BE INTERESTED IN EXPLORING INCLUDE:

- Messaging
- Value propositions
- Number of talent
- Talent look/age/sex
- Order of shots
- Inside vs. Outside
- Location

STEP 3: GET READY FOR PRODUCTION

Once your testing plan is sketched out, you will have identified your creative concepts and variables of interest. This information will be key to move on 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 testing campaign. This collection of shots will be the building blocks of the video ads you'll create and iterate on.

STEP 4: CAPTURE YOUR FOOTAGE

You've got your testing plan sketched out and a shot list in place. Now, you're ready to shoot! To maximize your budget, try to capture all of the footage you'll need in a single shoot. Organize for all on-screen talent to shoot on the same day and work 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, edit together your first set of creatives and launch your campaign. In the first round, test broad, focusing on high-level attributes like concept.

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, which will be carried over into the next round.

STEP 6: ITERATE

Take the winning concept from the first round and move it on to the next stage of your testing plan: variable testing. Identify the variables you want to test in the next round and edit your creatives with that winning concept accordingly.

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

Concept: Product & Lifestyle Shots

Concept: UGC-Style Testimonial

Hairstory 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.

Everlane used QuickFrame to affordably test various messaging.

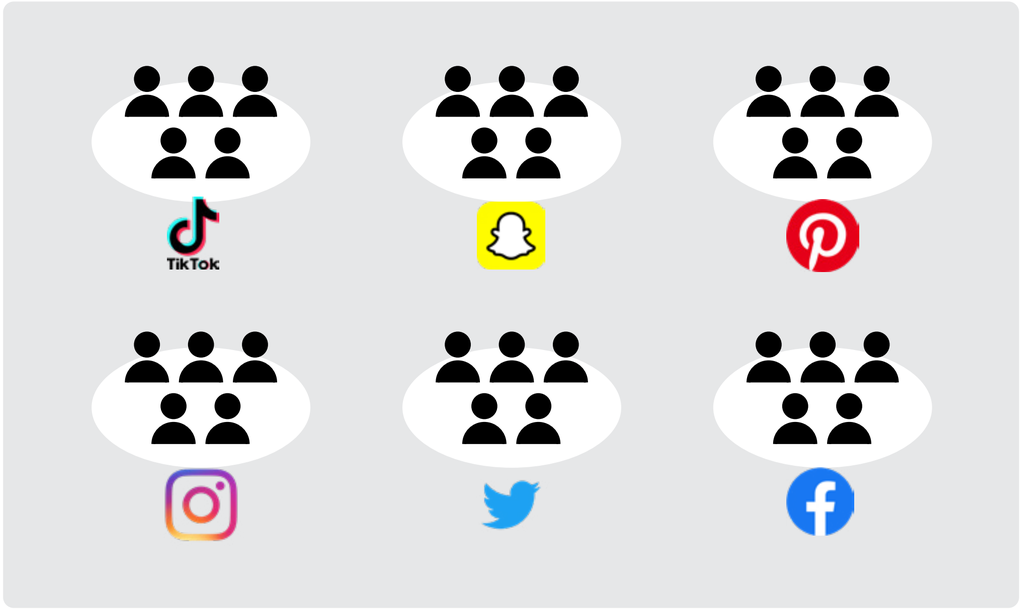
Once this round of creatives is ready, publish. Let these videos run for 1-2 weeks, monitor performance, and collect data to analyze.

STEP 7: REPEAT

This process continues down your testing plan as you take the winning creative approach from one round and get more and more granular with the attributes that you test in each subsequent round. 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.

Diversifying Your Media Plans



Data privacy regulations mean that you will no longer be able to confidently target specific consumers across the funnel. But, platform-provided first-party data will still allow you to get some insight into the places where your core audiences are consuming your content.

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 that your platform distribution needs to triple or quadruple in size. Consumers are increasingly using more platforms (for varying purposes) on a daily basis. So, your audience is likely 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 that work best on each one.

Your audience is likely not homogenous. And, they're having unique content experiences across each platform—the worlds of TikTok and Facebook (or Hulu and YouTube) are markedly different from one another. Even within a platform, experiences vary from one placement to another (e.g, Instagram Stories vs. Feed).

So, a testing plan built for one platform will likely not seamlessly translate to another. Instead, you must pursue testing plans that are platform- and placement-specific. By executing multiple plans, you increase the granularity of the data you generate.

Q&A:
Data Privacy & Performance Marketing

BRANDON ORR
DIRECTOR OF PERFORMANCE VIDEO
QUICKFRAME

Which of the coming privacy changes do you feel will have the greatest impact?

The greatest impact is the loss of the third-party cookie. But we're not really changing anything—we're just moving the onus. Right now we've got Facebook, we've got Google, we've got these big walled gardens… they all have their own little cookie worlds within them which are pre-gathered so you can buy and educate on them. Now, since the big boys and big girls are getting in trouble with all of their data issues over the last few years, we're basically moving that onus. That same experience—that same toolset—is going to become available, but on a much smaller level. There will be first-party cookies (and things like it) that will be available for purchase that will come down the pipeline, so I don't really feel like we're fixing anything—we're just kicking the can down the road.

How do you see marketers' day-to-day jobs changing?

Before, businesses were able to grow by finding a niche. It was easier to find our targets and reach them. Now we're going to have to just throw a bigger net. The actual tactics don't really change, but you've got to appeal to a larger audience. That's now the name of the game—versus finding your micro-audience and then expanding it. You're going to have to work with these big pulls, these big sweeps.

The last 7-10 years of marketing have been all about getting more personalized and data-driven, but now that we're at a point where we can't necessarily transact on the same kind of data, those lines aren't as valuable. So we have to not necessarily start from square one, but start from square three. We have to go back and find those least common denominators again. Our creative is going to have to do the work that our targeting used to do.

Before, we could at least get a sense of the audience of a media target—you could lay third-party data over it to get insights at the frontend. That could almost have set you up for a creative strategy that would fit inside your media. But since that is no longer available, you don't have as many things to start with. So, you kind of have to throw more things against the wall because we're just going to have fewer flags and identifiers.

What other strategies can performance marketers harness to succeed in a privacy-friendly manner?

Creative itself is going to burn out so much more quickly just because you won't have any of the frequency controls that a typical DMP (data management platform) would give you. To battle creative fatigue, you'll need to iterate on your creative and put new stuff out into the market at a much more regular basis.

QuickFrame | NURX

Online healthcare services provider NURX needed a scalable solution to improve DR performance and increase brand awareness. Our brand video production solution was built on learnings from ongoing creative variable testing, reducing CPA well below initial expectations.

SEE THE RESULTS