



The Oracle Data Cloud blog highlights the latest data-driven insights and trends in digital marketing and ad tech.

Register for our free virtual events



AUDIENCES ... [view more](#)

June 19, 2020



Don't Panic: Digital privacy strategies for the age of CCPA



Christian Bingham
PRINCIPAL PLATFORM ARCHITECT



Over these last few years, our industry has seen tectonic shifts in the consumer data landscape—just look at the trends: [the death of the 3rd party cookie](#), [the EU's groundbreaking GDPR regulation](#), and most recently, [California's Consumer Privacy Act \(CCPA\)](#). It's clear that privacy is becoming the new norm, but what does that mean for your business?

Glad you asked. Here is what you need to know.

First off, what is CCPA?

CCPA is a recently enacted privacy legislation that establishes new consumer protections and safeguards. Though the law itself was written specifically for California-based consumers, it's often operationally difficult to distinguish consumers on a state-by-state basis. To streamline compliance efforts, some organizations have simply started to apply CCPA's provisions to all consumers located within the U. S. In addition to the notice and nondiscrimination requirements, CCPA grants consumers three core rights:

1. A consumer's right to access his or her personal information;
2. A consumer's right to opt-out of the sale and/or transfer of personal information to third parties; and
3. A consumer's right to delete any collected personal information



In order to comply with CCPA's new rules, many companies will need to incorporate new strategies within their existing stack. Here are four important details that your company may want to consider.

Detail 1: If you haven't already, assemble a cross-functional Privacy Team

Can you name the team responsible to for your company's CCPA compliance? Spoiler: It should be broader than just the Legal Department. Build a cross-functional team spanning Governance, Product, Engineering, and Marketing, all of whom should have a role in crafting a plan of attack. Ensure that edge-cases and dependencies are accounted for (i.e., tech, people, and processes), and that clear lines of responsibility are drawn. Establish this team as a permanent organizational entity—in a future where California and other states prepare to enact [even tighter restrictions](#), agility and institutional expertise is key.

Detail 2: Streamline your databases by minimizing consumer data

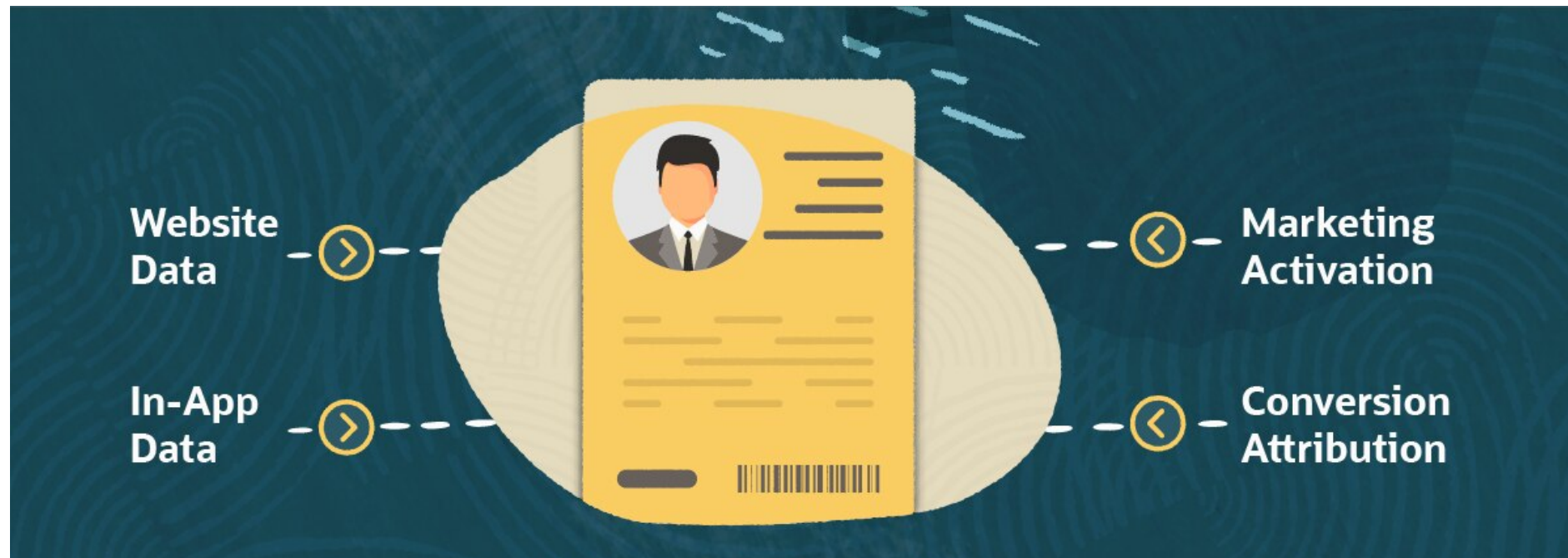
In many organizations, consumer data is spread across multiple silos—CRM, website, purchase activity, and attribution—just to name a few. Although it may sound obvious, the easiest first step toward privacy compliance often can be achieved by simply reducing the locations where consumer data resides. Is it possible that duplicative or unnecessary information is being collected?

Fortunately, there's no need to over-complicate this process: First, take an inventory of where consumer data resides within your organization's databases. Second, determine where the consumer data is absolutely necessary to achieve your organization's goals. If consumer data is unnecessary in a database, delete the consumer data and stop future transfer of consumer data into that database. Third, your organization can now focus on the limited environments where your compliance teams must pull consumer data to comply with access requests or delete data to comply with deletion requests.

Detail 3: Creating an in-house consumer ID can make compliance easier

As organizations expand the practice of digital 1st party data collection, it's critically important to scope how each of your consumers will be uniquely identified. As discussed above, consumer data may be spread across the multiple silos, even after your organization's best efforts at minimization. Such fragmentation is often a barrier to holistically understanding a single consumer's behavior and can make CCPA compliance unnecessarily difficult. Consider this: how will your organization comply with a consumer's access or deletion request if you're not even sure where that consumer's data is located in the first place?

Often, the easiest way to address such fragmentation is to first assign a unique ID to each digital consumer, then associate that ID with each of that consumer's relevant data entries. This ID can essentially function as a primary key to easily query when necessary to pull consumer data on an individual or to delete data on an individual upon request.



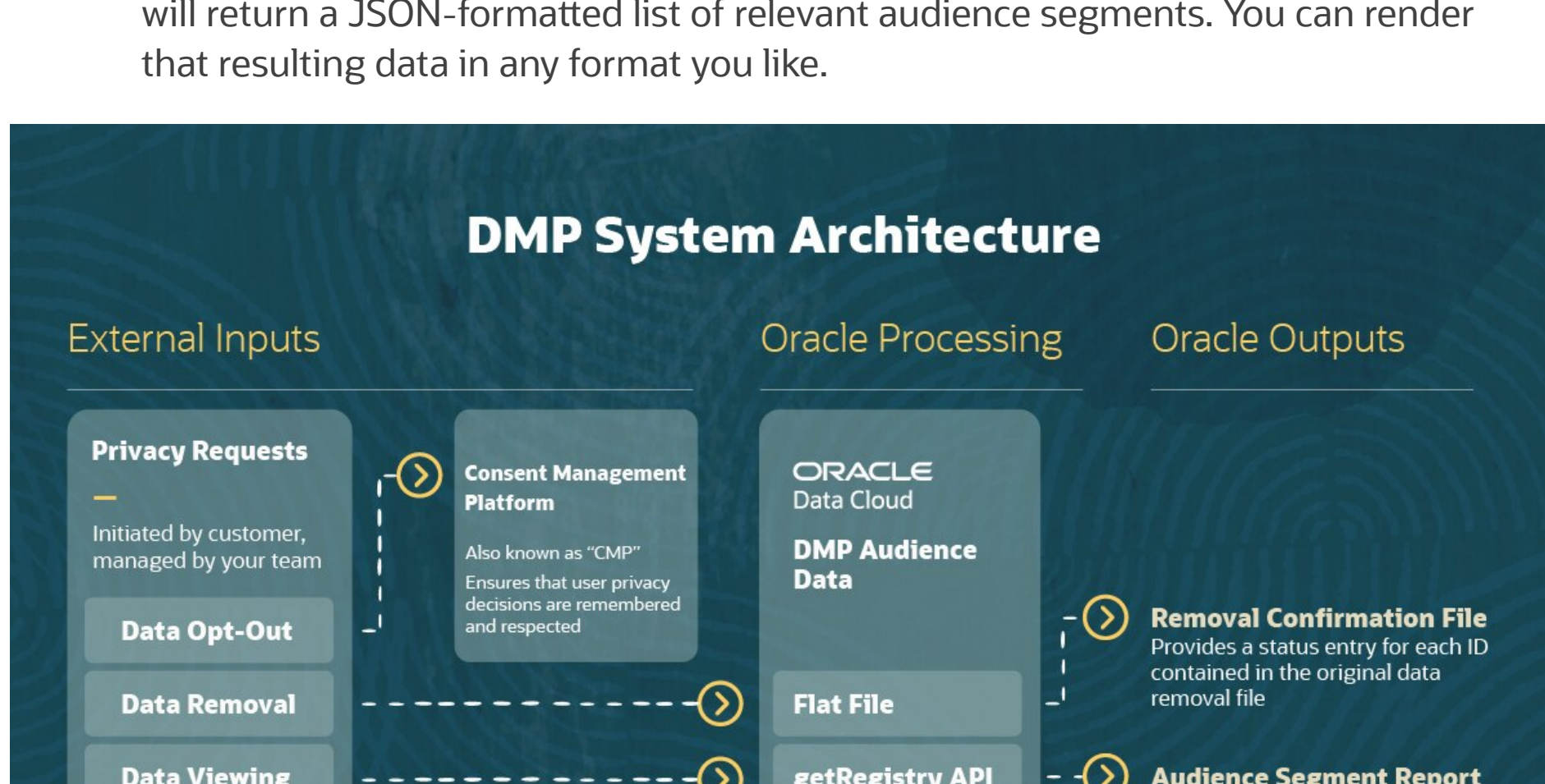
Detail 4: Where possible, leverage a Consent Management Platform

Given the complex and ever-evolving nature of privacy regulations, many organizations opt to simply deploy a 3rd party Consent Management Platform (CMP) on top of any existing data management efforts. As its name implies, CMPs act as a "privacy firewall", orchestrating methods of capturing consumer consent, conditionally firing site tags, and preventing data re-ingestion among other things. Because we understand that your organization has its own unique requirements, Oracle Data Cloud partners with various CMP providers to offer a more seamless approach toward integration; for those with more niche needs, we also offer services on which to build upon.

Building a privacy-oriented system architecture

Let's now review a sample system architecture, one a customer can design and integrate into Oracle Data Cloud's 1st party Data Management Platform (DMP). We will discuss this architecture by breaking down the three core actions a customer might initiate to respond to a CCPA request.

1. **Data Opt-Out Request:** This flow will be triggered any time a consumer initiates a request to opt-out of the sale of personal information to a 3rd third party. In our sample architecture, the consumer's input will be captured directly by a CMP, which is then responsible for orchestrating two workstreams. These are 1) ceasing all future data collection (i.e., preventing DMP pixels from firing when that consumer visits your website), and 2) informing relevant downstream systems of the opt-out event (i.e., do not transfer data related to this opted-out consumer).
2. **Data Deletion Request:** This flow will be triggered whenever a consumer requests the deletion of any 1st party data you've gathered on that consumer. We can automate this process by leveraging tools like Oracle Data Cloud's data removal flow. Usage is straightforward. First, generate a file containing a list of consumers requesting data removal, then deposit that file onto a Secure File Transfer Protocol (SFTP) housed by your DMP instance. Once that file is processed by your DMP, Oracle Data Cloud will respond with a report containing the removal status of each received ID.
3. **Data Access:** The last part of our flow will be kick-started any time a consumer requests to view 1st party data you gathered on that consumer. This process can be executed simply by capturing the consumer ID, then calling our getRegistry API that will return a JSON-formatted list of relevant audience segments. You can render that resulting data in any format you like.



Data management can be challenging – see how Oracle Data Cloud can help

The strategies described above are not a one-size-fits-all formula for addressing your organization's privacy needs, but hopefully provide a strong starting point for how to think about the industry's ever-evolving challenges. At Oracle Data Cloud, we have the products, the experience, and the global infrastructure necessary to help move your business forward.

Contact us to learn more about how we can help.

Disclaimer

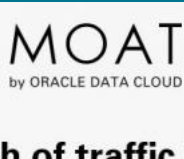
This information is not intended to be, nor may be interpreted as, legal advice. Any entity or consumer with questions about the applicability of the CCPA to them or their rights or obligations under the CCPA should engage legal counsel or reach out to the California Attorney General's office. The information provided in this document is for informational purposes only, on an "AS-IS" basis subject to change and without warranty of any kind.

Be the first to comment

Comments (0)

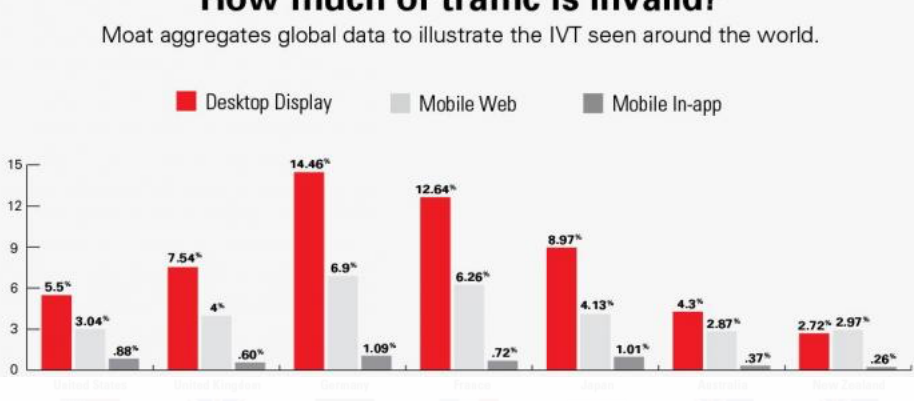


Recent Content



How much of traffic is invalid?

Moat aggregates global data to illustrate the IVT seen around the world.

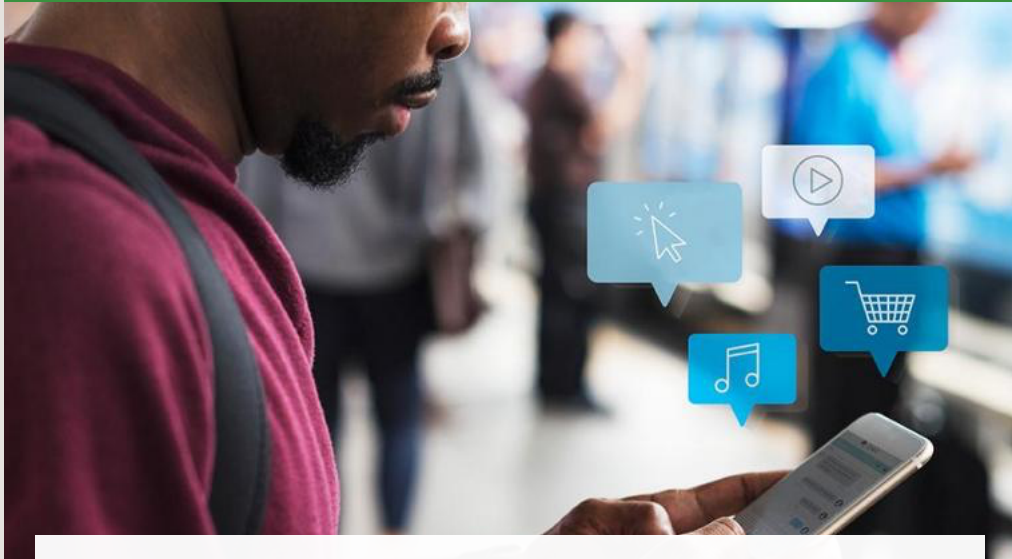


■ Desktop Display ■ Mobile Web ■ Mobile In-app

INDUSTRY INSIGHTS

How much ad traffic is invalid? Moat quarterly benchmarks break it down

Check out the below infographics pulled from the robust metrics available through Moat. This data surfaces the rates of invalid traffic (IVT)...



AUDIENCES

Is there a future for 3rd party audiences without cookies?

The dust has settled on Google's announcement that they will be deprecating 3rd party cookies within two years—a move that has left many...



INDUSTRY INSIGHTS

How to measure consumer attention, and why it matters

There's a process—well known in start-up and entrepreneurship circles—that every product goes through to reach mass adoption. Author...

