

A low-angle, upward-looking photograph of several tall skyscrapers in a city, likely New York City, with the Empire State Building visible in the center. The buildings are made of brick and have many windows. The sky is a pale, overcast grey.

# Marketing's Privacy Mandate:

## *Navigating a Fragmented Ecosystem of Solutions and Organizational Demands*

A Winterberry Group White Paper | January 2020

# Consumers Are Growing Increasingly Concerned About Personal Privacy...

The explosive growth of digital communication and commerce over the past 25 years has driven greater awareness and anxiety about consumer privacy. Concern has been accentuated by:

- **Data breaches.** Modern commerce relies on consumers providing information to brands ranging from name and address, to social security numbers and household income. High profile breaches across industries have left consumers feeling vulnerable and exposed.
- **Backlash against being monitored or tracked.** Consumers are increasingly aware that “if you’re not paying for it, you’re the product,” yet they often show disdain for what some have come to call “surveillance capitalism.”
- **Fear of being manipulated.** As content is increasingly curated based on behaviors and attitudes, consumers worry about filter bubbles and echo chambers, fears that are compounded by media coverage of election interference and Facebook/Cambridge Analytica scandals.

In response, many consumers deploy technical solutions that limit access to their data—blocking online tracking, deleting browsing histories, using end-to-end encrypted communications tools or dabbling with emerging solutions such as personal information management systems (PIMS) and personal data management platforms (PDMs) that allow users to share specific elements of their data when and with whom they choose.



## ... Leading Regulators to Respond with a Patchwork of National, Regional, and State Legislation...

An extreme example of consumer pushback came in the form of the ballot initiative that ultimately led to the California Consumer Privacy Act (CCPA) which became law on January 1, 2020. It came less than two years after the General Data Protection Regulation (GDPR) had been enacted in the European Union, with the aim of giving individuals control of their personal data.

California wasn't alone in following the E.U.'s lead. In the past two years a slew of countries, states and regions have introduced or updated laws to apply some of the provisions spearheaded by GDPR.

These regulations differ, but most grant explicit rights to consumers—including the right to access the personal information that brands have about them, and the requirement for companies to gain consent from consumers if they wish to process their data.

And, these laws have teeth. In Europe, hefty fines have already been handed out due to failure to comply with the GDPR. By the end of December 2019, more than 130 fines (which can be 4% of annual global revenue or €20 million—whichever is higher) were levied by EU regulators totaling more than €400MM. We have yet to see what a fine might cost businesses that fail to comply with CCPA (which can be up to \$2,500 per violation or \$7,500 per intentional violation, with the opportunity for class-action lawsuits).

**One thing is clear:**

**Privacy is no longer simply the remit of the legal department;**

**It is a C-suite and board-level concern that affects every aspect of a business.**



## ... Yet, Few Firms Believe They Are Well Prepared

### Despite More Than 18 Months of Industry Attention, Few Firms Felt Ready For CCPA

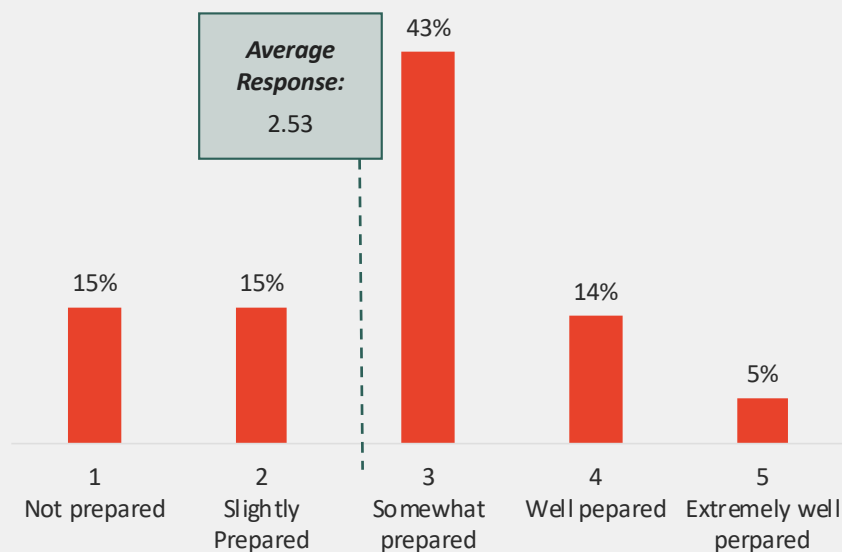
In research that Winterberry Group published in partnership with the IAB in January 2020, brands cited privacy as a top priority for their business in the year ahead.

However, despite their reported concern, most data users felt ill-prepared for the then-fast-approaching California Consumer Privacy Act deadline.

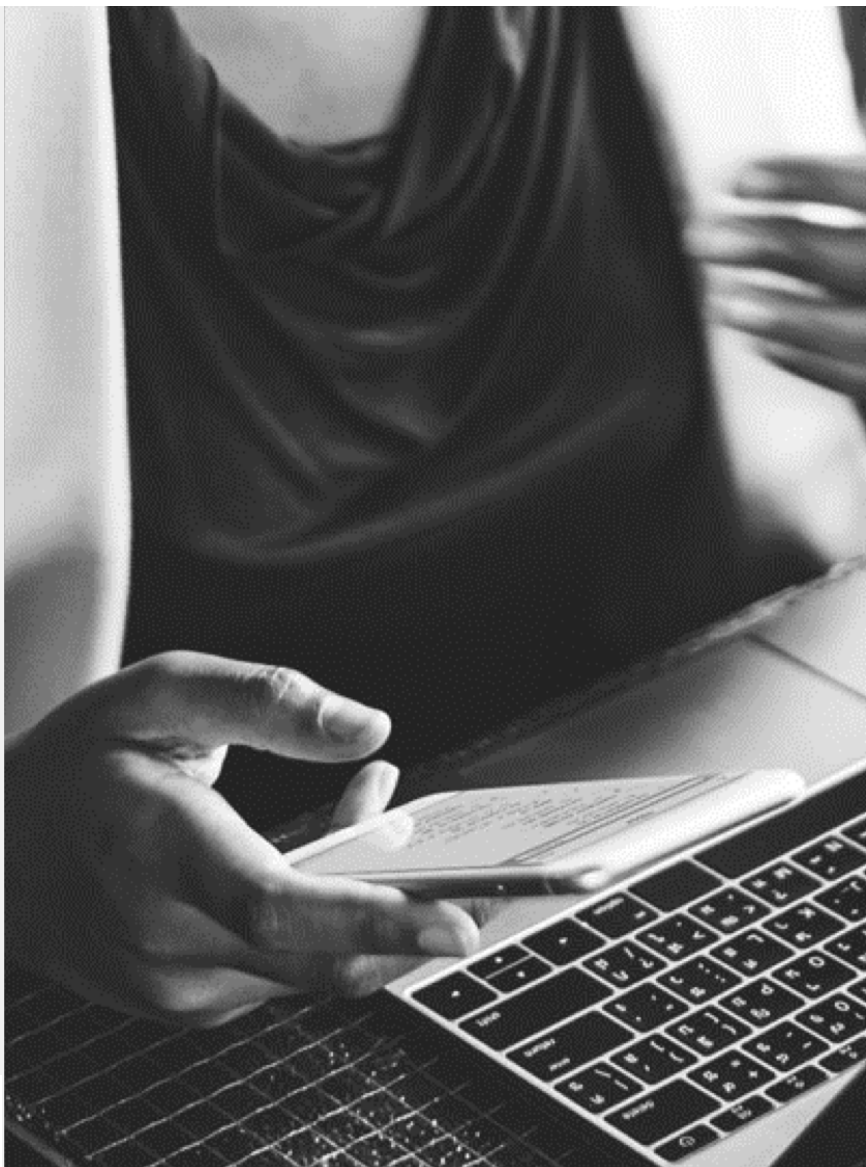
Our research points to this gap partly as a function of CCPA's short implementation window, but also as a result of gaps in existing strategy and infrastructure geared to support data governance.

And even in Europe, almost two years since the introduction of GDPR, researchers at MIT, UCL and Aarhus University found in January 2020 that **only 11.8 percent of more than 10,000 websites in the U.K. comply with European consent laws.**

*"How prepared is your organization to deal with recently passed and/or enacted regulation relating to individual consumers' personal data?"*



Source: IAB-Winterberry Group Data Centric Organization Report (2020)



## Navigating The Evolving Vendor Landscape



# An Array of Solution Providers Target Different Buyers With Diverse Offerings

More than 200 vendors, ranging from bootstrapped startups to enterprise software vendors, specialize in privacy solutions. These firms sell to three primary groups:

- **Legal, privacy and compliance** teams that typically invest in impact assessment management, incident response solutions and policy management tools;
- **IT, data management and information security** teams that invest in data discovery and mapping solutions, activity monitoring, enterprise communication tools, exposure scanning and incident monitoring solutions; and
- **Marketing and business** teams that often invest in subject access request management and consent management solutions.

A limited number of vendors offer solutions that span multiple buyer groups. These multi-solution vendors typically evolved from a focus on the legal, privacy and compliance teams, and have grown (or “been dragged” as one playfully described it) into extending their focus to marketing teams. In the case of at least one of these vendors, it recently introduced a sub-brand to focus on marketing as a buying audience – bundling solutions and hiring teams that understand the need of the marketing buyer.

## Within The Fragmented Privacy Solution Market, Marketer-Focused Tools Emerge

All major new and updated legislation, including the GDPR and CCPA require firms to obtain a consumer’s consent either before capturing and/or processing their data.

## Consent Management Emerges As A Category

Although definitions differ by legislation, most describe consent as pertaining to consumer choice and control of the personal information that a company gathers and uses.

If you have multiple sites, multiple purposes for processing data (which each need their own consent), allow advertising on your site, are a data controller, provide data to other third parties or engage with customers across multiple touchpoints, managing consent gets complicated quickly.

Consent Management Platforms (CMPs) have emerged as a vendor category designed to help marketers manage the consent process.

Similarly, both GDPR and CCPA include what’s known as a right of access, giving consumers (known as data subjects) the right to obtain a copy of their personal data from a company.

## Subject Access Requests Have To Be Managed Carefully

These access requests allow consumers to understand how and why a company is using their data, and to check they are doing so lawfully.

Depending on the complexity of a company’s data and their ability to authenticate that the data subject is who they say they are, dealing with a subject access request can be onerous and time-consuming.

Vendors that support subject access management, sometimes referred to as SAR or DSAR portals, have emerged as a category to help marketers manage the subject access request management process.

# Existing Marketing Solution Providers Want a Piece of the Privacy Action

In addition to the emergent specialist providers, vendors from several existing marketing technology categories look to support marketer needs in managing subject access requests and/or consent management.

- **Email Service Providers (ESPs)** frequently provide preference centers, which could be extended to consent, and often host and sometimes integrate customer data, opening the opportunity to assist with subject access requests.
- **Mobile Marketing Platforms** typically manage mobile engagement, data and SDKs, and are well positioned to support with mobile consent.
- **Personalization engines** capture and sometimes manage customer data, opening the opportunity to assist with subject access requests.
- **Data Management Platforms (DMPs)** capture and manage data for use in identifying audiences for online advertising. An increased focus on first-party data opens the door to assist or lead consent management efforts.
- **Customer Data Platforms (CDPs)** ingest customer data and manage customer profiles providing the opportunity to support subject access requests as well as the possibility to add 'customer consent' as an element of profiles.
- **Marketing Clouds** promise integrated suites of (often acquired) tools, including ESPs, DMPs, and self-proclaimed CDPs. They have access to lots of data and could assist with subject access requests as well as consent management.
- **Identity Management Solutions** support the persistent recognition of audience members across devices and touchpoints, providing the opportunity to support subject access reporting through the creation of persistent profiles from a variety of data.



## Preference vs. Consent

*Although the terms “preference” and “consent” are sometimes used interchangeably, the concepts are distinct. “Consent” confers to consumers ultimate control of their data and requires firms to gain permission to use that information. “Preference,” by contrast, infers that marketers maintain control of data and affords the consumer the opportunity to state whether and how they prefer that data to be used across various use cases and touchpoints.*

# Deeper Dive: Managing Consent

## How Complex is Consent Management?

Different regulations dictate how consent may be granted (for example via an active opt-in, a pre-checked box, or other method of default consent), how clear and specific statements of consent must be (for example, about what is captured and the specificity of how the data will be used and shared), how consent can be granted or denied, and what the implications might be of denying consent.

Depending on the legislation, firms must keep evidence of consent – who consented, how, when, and to what specifically. This consent must then inform future communications with consumers to ensure marketers comply with each individual's stated consent.

## What's Needed To Manage Consent?

Solutions that help marketers and publishers manage consent enable this process across different legislative frameworks and requirements. Typical components may include:



**Console/portal:** a marketer-friendly dashboard for managing the consent process;



**Consent collection:** e.g. banners on websites that provide consent details and allow consumers to provide or deny consent;



**Consent storage and management:** documentation and verification of elements such as prompt wording, privacy notice accepted by user, opt-levels, etc.;



**Mobile SDK** (for mobile apps);








**Third-party solution integration:** to enable compliance across cookies, mobile apps and ad solutions.



# Marketers Should Match their Consent Management Needs With Vendor Sophistication

Several categories of provider support consent management. In collaboration with the legal/privacy and IT organizations, marketing teams need to assess their consent management complexity, understand where there are gaps, and determine whether a third-party solution is the most effective way to close the gap – and if so, whether a specialist CMP is necessary, or whether leveraging existing providers might suffice.

	 Console/ Portal	 Consent Collection	 Storage/ Management	 Mobile SDK	 Solution Integration
Consent Management Platforms	●	●	●	●	●
Email Service Providers	◐	◐	◐	◐	◐
Mobile Marketing Providers	◐	◐	◐	●	◐
Personalization Engines	◐	◐	◐	○	◐
Data Management Providers	◐	◐	◐	○	◐
Customer Data Platforms	◐	◐	◐	◐	◐
Marketing Cloud Providers	◐	◐	◐	◐	◐
Identity Management Solutions	○	○	○	○	○

○ Little/No Capability

◐ Partial Capability

● Full Capability

# Deeper Dive: Subject Access Requests

## What's So Complicated About Managing Subject Access Requests?

Different regulations call for different obligations within a request, such as requiring a company to inform consumers of the source of data (when not obtained directly from the consumer); how long the data is stored; with which other entities the data has been shared; the safeguards the company provides if transferring personal data to another country or international organization; and the length of time the company has to respond and deliver the requested information.

## What do Subject Access Requests Typically Require?

Solutions that are designed to help firms manage Subject Access Requests provide a central location to manage the access rights process across different legislative frameworks and requirements. Typical components include:



**Portal/front-end:** to set-up and manage the process;



**Verification and authentication:** often leveraging third-party verification to confirm identity and location;



**Process management:** Ticketing requests (including timestamps, locations, etc.) and managing the data collection;



**Review and approve:** often with a holding stage that requires human review and approval;









**Delivery:** usually in PDF form and usually sent in the manner/channel in which the request was received (web portal, email, in-person);



**Management and/or coordination of any exercise of rights:** as previously outlined, different laws provide consumers with additional rights such as the right of removal, rectification or portability.

# Marketers Should Match Their Subject Access Management Needs With Vendor Sophistication

Several categories of provider support access request management in different ways. Once again, marketing teams need to assess the complexity of their requirements – evaluate data complexity and the real or expected high-volume of access requests. If managing the process manually, expect that managing the workflow and reporting will be cumbersome. Once again, assess any are gaps, and determine whether a third-party solution is the most effective way to close the gap – and if so, whether a vendor specializing in subject access request management is necessary, or whether leveraging existing providers might suffice.

	 Portal/ Front-End	 Verificat./ Auth.	 Process Mgmt.	 Review & Approve	 Delivery	 Rights Mgmt.
Consent Management Platforms	●	●	●	●	●	●
Email Service Providers	◐	◐	◐	◐	◐	○
Mobile Marketing Providers	◐	◐	◐	●	◐	○
Personalization Engines	◐	◐	◐	○	◐	○
Data Management Providers	◐	◐	◐	○	◐	○
Customer Data Platforms	◐	◐	◐	◐	◐	◐
Marketing Cloud Providers	◐	◐	◐	◐	◐	◐
Identity Management Solutions	○	○	○	○	○	◐

○ Little/No Capability    ◐ Partial Capability    ● Full Capability

# How Will The Privacy Technology Market Evolve?

Given the fact that multiple U.S. States and various federal legislators are discussing potential regulation, the frenetic pace of the market shows no signs of slow-down. Similarly, other countries continue to evaluate and enact new laws – with ePrivacy a major focus on the horizon in Europe.

Privacy solutions targeted at marketers will play a role in the immediate, medium and long term. But their role will change as the market matures, marketer engagement evolves and as enterprise software providers pay greater attention to the privacy needs of marketing departments. It's unlikely that all of today's standalone CMPs and SAR platforms will survive. So, what will happen to them?

## Expand beyond their core

Several CMP and SAR solution providers are already extending their capabilities beyond their heritage. And, some of those that remain standalone are partnering with one another to compete. These vendors will continue to expand from their core, and the successful ones will enter non-marketing privacy adjacencies such as data mapping, impact assessment management or policy management.

## Extend beyond privacy

As privacy and trust continue to grab the spotlight within brands, vendors that help to manage privacy will be highly valued and trusted. Should those vendors see an opportunity to extend their offerings to help marketers engage with customers in a privacy-first manner, it's hard to imagine marketers not considering their solution.

## Absorbed by strategic buyers

A market as hot as privacy management won't stay standalone for long. At some point the marketing clouds will probably look to buy their way in to the market, while data cloud providers, MDM vendors and point solution engagement providers could all recognize the opportunity to expand into this market. Others may see a need to protect their flank should the privacy vendors begin to consider engagement offerings.

## Dissolve or Pivot

Despite the heat in the market, there are too many providers for long-term demand. Those that fail to expand, grow or merge may be forced to pivot to new offerings, while others simply won't make it.

# Service Providers Offer Various Levels of Support

For marketers with limited internal resources, complex needs or a desire to tap into best practices or industry expertise, service providers can provide highly valued capabilities for short, medium and long-term engagement. We typically segment service providers into those that provide technical support, such as managing and hosting solutions, writing APIs, or integrating solutions, and those that provide advisory services such as strategy, assessments, and training.

While many service providers focus on supporting legal and IT departments, vendors such as marketing service providers (MSPs), consulting firms, and CRM agencies understand the needs of, and offer support for, marketers.



## Technical support – Consulting firms, data and marketing service providers, agencies

- Install, host and/or manage solutions
- Data mapping
- Vendor management
- Data protection support



## Advisory services – including law firms, consulting firms

- Assessments and audits, risk analysis
- Strategy/planning/policy department
- Breach response
- Training

*“Our clients range from the sophisticated to the absolute novice. The sophisticated clients typically want a trusted partner to support their efforts, but they already have a clear sense of what they need. The novices are like the proverbial deer in the headlights. They don’t know where to start – and they don’t even know what they don’t know. Job one for us in these situations is to help them identify their needs and become a more educated buyer so that we can even begin to see where we can deliver value.”*

SVP & Privacy Lead  
Marketing Service Provider



**Marketers Must Define  
Their Role and Align  
With Peers**



# Marketing's Privacy Mandate: Engage and Clarify

The pace of regulatory change makes it challenging to predict future developments. For example, while we anticipate a U.S. Federal privacy law at some point in the future, the current political environment and upcoming Presidential election makes it particularly tough to predict when that might occur.


Despite the uncertainty, there are actions that every marketer can take to prepare for the future of privacy, regardless of how it evolves.

## Start By Recognizing That Privacy Is No Longer Simply The Remit Of The Legal Department

- ✓ **Establish a marketing privacy team and leader.** Without specific individuals that own responsibility and accountability for privacy within the marketing department, the lack of ownership will make privacy an afterthought and a hindrance. And, the marketing department will be out of sync with their colleagues in other departments. Clear ownership and responsibilities is critical to ensure success.
- ✓ **Treat privacy as a (non-exclusive) marketing discipline.** Marketers should hire with privacy in mind, examine workflows and pay attention to privacy when integrating solutions. Enterprise marketers tell us that they struggle without a marketing privacy head or committee that represents marketing when working with peers in legal and IT.

## Clarify Marketing's Role And Align With Other Functions And Departments

- ✓ **Understand roles and responsibilities.** While marketing has a critical role to play, marketers must work with peers in legal, IT, and elsewhere to clearly define roles, delineate areas of responsibility and establish standard operating procedures for working together.
- ✓ **Provide support where it's needed.** Marketers can and should support other functions as the owners of technology where consumer data often sits, in complying with consumer preferences and consent and in providing communications support to soften legalese and tech-speak in privacy policies, consent requests, subject access reports and incident or breach reports.



*"It took us a long time to identify owners of privacy within marketing. We now have a dedicated taskforce that works with Legal, Privacy, IT and others. Their job is to both represent marketing and to communicate back to the rest of marketing about all-things related to privacy. Before we had the taskforce, nobody was responsible. It was a disaster."*

Global Consumer Engagement Leader Sportswear Manufacturer


# Marketing's Privacy Mandate (cont.): Learn and Elevate

## Learn The Landscape And Language To Earn Your Seat At The Table

- ✓ **Educate yourself about the continuously evolving regulation.** Consumers are more privacy aware than ever before, and as the most consumer-facing department, marketers play a key role in ensuring communication is both compliant and compelling. Join and support industry associations and understand the recommendations and frameworks relating to self-regulation and compliance.
- ✓ **Stay informed about technical developments** that may affect privacy, such as developments in authentication and blockchain. Develop a point-of-view to prepare for a potential cookie-less future and monitor the role of Mobile Advertising IDs and other Personal Identifiers.

## Drive The Company To Evolve

- ✓ **Elevate the perspective of privacy from compliance to opportunity.** Given the immediacy of adhering to a bevvy of new laws, compliance is obviously a critical immediate focus for brands. But, when the dust settles – post-compliance – marketing should be in the driving seat encouraging the company to treat privacy less as a threat and more as a differentiator.
- ✓ **Center the focus on trust.** As the advocate of the customer, marketing is uniquely positioned to help the organization to see privacy as an attribute that will drive better customer experience, relationships and trust. When consumers see value in sharing data – due to convenience or direct benefits, they don't just value the firm's privacy team. They value the relationship. They value the company thinking of things from their perspective. They begin to build trust – and that's a priceless commodity.



*"Right now, every customer is focused on making sure that they meet the demands of each of these new regulations. We've already begun the conversation with them to think of consent management as a function of customer experience. We're encouraged by the general reaction, but it's clear that we have to get through the next few years of compliance before they can give anything more than lip-service to things like giving customers control in order to transform their business."*

CEO

European Consent Management Platform

# Clarify Roles and Responsibilities with Other Functions and Departments

Firms that struggle to determine which departments and functions should own which aspects of their privacy program complain that elements fall through the cracks or they see efforts duplicated, and even contradicted, by different internal groups.

Firms must invest the time and organize cross-departmental task forces to delineate roles, responsibility and “ownership” of program elements. Consider building a RASCI matrix to clarify, assign and align each department or functions’ responsibilities, and who specifically will be Responsible, Accountable, Supporting, Consulted and Informed about which elements of the privacy program.

Sample RASCI Matrix – For Illustrative Purposes					
	Responsible	Accountable	Supporting	Consulted	Informed
Privacy Operations	Legal	Dir Privacy	Compliance		
Policy Management	Legal	CPO	Privacy, Compliance	GC	IT, Marketing
Internal Procedures/Training	Legal	VP Compliance	HR	CPO, Privacy	IT, Marketing
Impact Assessments	Legal	Dir Privacy	IT, Marketing	Legal, Compliance	
Vendor Risk Management	IT	VP Channel Partners		Legal, Marketing	
Information Security	IT	CIO	InfoSec	Marketing	Legal
Data Mapping	IT	VP Sys Admin	Marketing		Legal
Incident Monitoring & Response	IT	CTO	InfoSec	Legal, Marketing	
Consent Management	Marketing	VP Digital Marketing	Privacy, Compliance	IT, Legal	
Subject Access Reporting	Marketing	VP MarTech	Data Management	IT	Legal
Preference Management	Marketing	VP Digital Marketing	Email Mktg Director	IT	

# Research Methodology

The findings within this White Paper are based on in-person and telephone interviews with more than 40 marketing, business, privacy and product leaders. Interviews were conducted between September and December 2019.



# About Our Sponsor

## **ALLANT**<sup>®</sup> Presenting Sponsor

Allant delivers data, robust insights and technology services allowing emerging and mid-market brands to understand their customers, optimize their marketing spend, and provide exceptional experiences. Blending strategy, omni-channel data science with agile execution services across digital and offline channels, Allant has been helping marketers drive revenue growth for over 30 years. For more information, visit [www.allantgroup.com](http://www.allantgroup.com).

Whether you are struggling to understand the impact of CCPA on your existing data assets or need assistance with deploying a solution, Allant can help. We have done the research and can help you quickly and cost effectively. Learn more about integrating consent and preference management into your marketing efforts to meet CCPA and other consumer privacy requirements with Allant. <https://www.allantgroup.com/consumer-privacy-allant.html>

# About Winterberry Group

A specialized management consultancy that offers more than two decades of experience and deep industry experience in the intersecting disciplines of **advertising, marketing, data, technology** and **commerce**.

Helps brands, publishers, marketing service providers, technology developers and information companies—plus the financial investors who support these organizations—**understand emerging opportunities, create actionable strategies** and **grow their impact and value** on a **global basis**.



**Dave Frankland**  
Managing Director  
[dfrankland@winterberrygroup.com](mailto:dfrankland@winterberrygroup.com)

[www.winterberrygroup.com](http://www.winterberrygroup.com)  
115 Broadway, 5<sup>th</sup> Floor  
New York, NY 10006  
[@WinterberryGrp](https://www.instagram.com/WinterberryGrp)