

Adding AdTech to the CCPA Equation: The Importance of Third-Party Vendor Compliance

December 20, 2019 – The TMCA

by Alison Hill and Cody Wamsley

The arrival of the California Consumer Privacy Act (CCPA) on January 1, 2020 brings steep risk for companies that collect information on California residents. In particular, and among other statutory penalties, a business that suffers a data breach is subject to statutory penalties of \$100-750 per consumer per incident if such data breach arises from a failure to implement "reasonable security procedures and practices." What many businesses may not realize is that this risk is present even when data processing activities are conducted by a third party on behalf of the business and with vendors that businesses may not immediately think about when considering the processing of personal data. An oft-overlooked example of this risk lies within the advertising and marketing vendor ecosystem.

Related People

- Alison Hill

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation



Advertising technology, or AdTech, is an evolving field that encompasses software and

other tools that help organizations target, deliver, and evaluate their digital advertising initiatives. It is not a secret that this technology includes tracking technologies to monitor online activity of consumers, which is then ultimately used to target consumers with tailored ads. While some organizations have the resources and personnel to undertake and oversee all of their advertising and other marketing needs, many rely on advertising vendors to fill this role. These AdTech vendors are part of the advertising vendor ecosystem, a complex, dynamic industry aimed to opportunistically deliver relevant ads to consumers. In order to accomplish this, these vendors must use consumer data.

As an example of the complexity of the AdTech space, consider the following.

Organizations hire media agencies to purchase media on behalf of their clients and ad agencies to generate creative media initiatives using that media. A media agency provides services through an agency trading desk (ATD), which gathers all available data obtained through advertising campaigns and plans and manages ads across several different platforms. Advertisers use technology platforms known as Demand Side Platforms (DSPs) to bid on and purchase ad placements through exchanges or networks using data and tools to optimize campaigns to accomplish the advertiser's goals. Advertisers rely on Data Management Platforms (DMPs) to collect data from a variety of sources, including advertising campaigns, websites, social networks, and mobile apps, and then use data analytics, artificial intelligence, and machine learning technology to analyze that data to identify trends and target specific consumers. An advertising network is a company that acts as the intermediary between advertisers and publishers, aggregating ad inventory from publishers to sell to advertisers. Ad networks operate in an ad exchange, which is either an open or private marketplace that facilitates the buying and selling of ad inventories—advertisers often select desired ad inventory using DSPs. Supply Side Platforms (SSPs) are technology platforms used by publishers to analyze demand from ad networks and exchanges and consolidate and expose their ad inventory to DSPs to ultimately earn revenue. Ad networks, ad agencies, advertisers, and publishers run ad campaigns using ad servers, which are applications to host and deliver the ads, all while tracking and collecting ad performance data.

Through these relationships, AdTech vendors may be processing a variety of personal data types on behalf of businesses, including names, physical addresses, phone numbers, email addresses, IP addresses, device IDs, behavioral, biometric, payment, social media profile information, etc. As such, companies have a responsibility to ensure the security of the information that AdTech vendors process on their behalf and may face CCPA liability in the event of a data breach for a compromise to this data if the company did not conduct proper third party security diligence and oversight of the vendor.

Performing diligence on AdTech vendors is not a materially different process from performing diligence on any other vendor that processes personal information. Companies should assess the risk associated with the vendor, which can be related to the type of information processed, volume of information, technical integrations, sophistication of the vendor, or any combination of these or other factors. Once a company has determined the risk associated with a vendor, it should determine what level of diligence it should undertake in relation to that risk. Generally, diligence levels fall

on a spectrum with bare contractual terms being the bare minimum and moving up through questionnaires, internal policy evaluations, third party artifacts, audits, all the way to even controlling the security of the vendor through various mechanisms. Whatever level of diligence a company decides to apply to a vendor, it should document that decision and the basis for reaching it. Companies should also consider including indemnity clauses in AdTech vendor contracts as a means to hold the vendors accountable for data breaches caused by unreliable data processing.

Most important of all, however, with any vendor that may be processing personal information on behalf of a business, is to ensure that the business has established an efficient incident response process with the vendor. This process should not only be codified in the vendor contract, but also in the business' own incident response plan. It is critical that a vendor understands what type of security incident it needs to notify its customers about, who to contact at the customer site regarding the incident, and on what timeline. There may be key coordination efforts that need to be mutually undertaken during an incident and trying to figure all of this out in the heat of the moment will lead to problems. Remember, as a data controller, the customer may ultimately be responsible for the protection of the data; therefore, relying entirely on a vendor to handle incidents with no oversight or other controls may not be a reasonable position.

In the end, AdTech vendors that handle personal information should be treated as any other vendor that processes sensitive information and should undergo proper diligence, oversight, and be subject to adequate contractual controls. Failure to do so could result in significant penalties under the CCPA and other emerging privacy laws.