PROJECT CROSSWALK

Addressing CCPA Compliance within the CTV/OTT Marketplace

Sponsored by:

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Table of Contents

Acknowledgements

This report would not have been possible without the guidance and direction of the IAB Legal Affairs Council and the time, dedication, and contributions of the Project Crosswalk Working Group members and companies, and contributing law firms listed below. We extend our thanks and deepest appreciation.

We are especially appreciative to our sponsor OneTrust, as well as Alysa Hutnik, Sundeep Kapur, Tal Chalozin, and Eric John, Vice President, IAB Media Center, each of whom have been invaluable contributors to the work of the Project Crosswalk Working Group.

Sponsor

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Project Crosswalk Working Group Member Participants

ALC
Amazon.com, Inc.
Amobee, Inc.
Baker & Hostetler LLP
Big Token
BuzzFeed
CDK Global, LLC
Comcast Cable
Comscore
Criteo
Data Analysis Inc.
Dish Network LLC
Extreme Reach, Inc.
Google, Inc.
GroupM
Hearst Communications Inc
Hulu, LLC
Integral Ad Science, Inc.
JukinMedia
Kelley Drye & Warren LLP
Loeb & Loeb LLP
L'Oreal
Magnite, Inc.
MediaMath
National Cable Communications LLC
NBCUniversal Inc
OneTrust
Orrick Herrington & Sutcliffe LLP
Pluto TV
Procter & Gamble
Publicis Groupe
PubMatic, Inc.
Roku, Inc.
Samba TV
Samsung Electronics America, Inc.
Sizmek by Amazon
Sourcepoint Technologies Inc.
Squire Patton Boggs
SRAX
Technology Practice Group LLC
Tegna Inc.
The Coca Cola Company
The Hershey Company
The Trade Desk
The Walt Disney Company
Triton Digital
Verizon Media
VEVO LLC
ViacomCBS Inc.
Vizio

I. Introduction

> Over the last few years, CTV and OTT streaming services have exploded in their size and reach.

The California Consumer Privacy Act (CCPA) of 2018 was a watershed legislative event, which made California the first state to introduce generally applicable comprehensive privacy compliance obligations. The complexity of applying these obligations in digital advertising, where there is a complicated set of data flows, impacted companies throughout the distribution chain. IAB responded to this challenge with the IAB CCPA Compliance Framework and Limited Service Provider Agreement (LSPA), which has provided nearly 800 hundred member and non-member companies with scalable compliance solutions for their digital advertising. Indeed, as more companies sought operational solutions to comply with the CCPA's "Do Not Sell My Personal Information" opt-out right, IAB saw increased interest in the Framework and LSPA, with even more participants joining in response to the California Attorney General's regulatory and enforcement efforts.

IAB continues this commitment to both analyzing and providing members and non-members alike with the means of complying with the CCPA, and in due time the California Privacy Rights Act (CPRA), in as many contexts as possible, including in the connected TV (CTV) and over-the-top video (OTT) environments. Over the last few years, CTV and OTT streaming services have exploded in their size and reach. According to Nielsen, consumers watched almost 30 billion minutes of streaming content in Q1 2021 — up 122% from Q1 2018 when consumers watched 13.5 billion minutes.[1] Content that was originally distributed for viewing on TVs using broadcast, cable, or satellite channels, as well as shorter form, streaming-first content (e.g., YouTube.com), is now distributed over multiple forms of internet-connected devices. CTV's growth includes expanded use by consumers of smart TVs that stream video directly over the internet, devices that stream to a TV (e.g., Roku, Chromecast, Amazon Fire TV Stick, Apple TV, and others), and game consoles that stream to a TV (e.g., Xbox, PlayStation, Nintendo, and others). This mix of devices enabling big-screen internet-delivered TV are now in 83% of U.S. households.[2] While the majority of premium OTT viewing is currently on CTV devices (e.g., smart TVs, Roku, Chromecast, etc.) that connect directly to the internet, the rise of ad-supported video-on-demand (AVOD) and free ad supported services (FAST) are continuing to drive increased demand for viewing beyond the living room, too. We can expect mobile OTT viewing to grow as people emerge from lock-down living and as cellular connectivity and 5G continues to improve.

[1] Nielsen. Getting Ahead of the Curve in CTV Advertising. (2021, June).

[2] The CTV Advertising Report, June 2021, TVision

I. Introduction (*cont'd*)

However, digital advertising in the CTV/OTT space has unique privacy compliance considerations. The diverse participants and their varied roles, responsibilities, and relationships to the personal information processed, as well as applicable technical standards and limitations, do not line up neatly with comparable processes for programmatic advertising for desktop and mobile. In particular, the CCPA's classifications of business entities and how to treat data flows among them raise added complexities in the CTV/OTT environment.

In response to member feedback and recognized needs within the CTV/OTT industry, IAB's Legal Affairs Council created ***Project CCPA Crosswalk***, a working group focusing specifically on CCPA compliance considerations for CTV/OTT. Project CCPA Crosswalk includes legal representatives from members across the CTV/OTT industry who met over several months with a focus on:

- **Identifying current CCPA practices in the CTV/OTT marketplace**
- **Identifying data flows that are relevant to the CCPA analysis**
- **Developing a common framework for addressing CCPA classifications**
- **Determining next steps in order to prepare scalable CCPA compliance solutions to address data sales and service provider disclosures**

The working group discussed these issues, in addition to experiences and perspectives within the industry on how to address CCPA compliance. It then prepared and put into the field a survey that further explored these areas of focus. Notably, the survey also sought to identify points of friction that make some CCPA compliance obligations particularly challenging, and to what extent workable compliance tools might include the LSPA (or modified versions of it), or other compliance tools to address CTV/OTT technical and business arrangements and consumer/household interactions that vary from traditional display advertising.

In this white paper, we examine the stakeholders within the CTV/OTT marketplace, how participants disclose and process personal information, how participants view themselves when applying CCPA definitions and corresponding compliance obligations, whether and what friction points exist when addressing CCPA compliance, and potential solutions deserving further exploration. Many of the insights included in this white paper are derived from the CTV/OTT survey responses. Additionally, we discuss the working group's next steps for expanding compliance tools to support this segment of the industry.

II. Who are the Stakeholders

To understand the CTV/OTT marketplace and how participants approach CCPA, it is important to recognize that the participants in the CTV/OTT ecosystem are wide, varied, evolving, and in some cases consolidating, in response to technology, legal, and industry changes. The main participants often include:

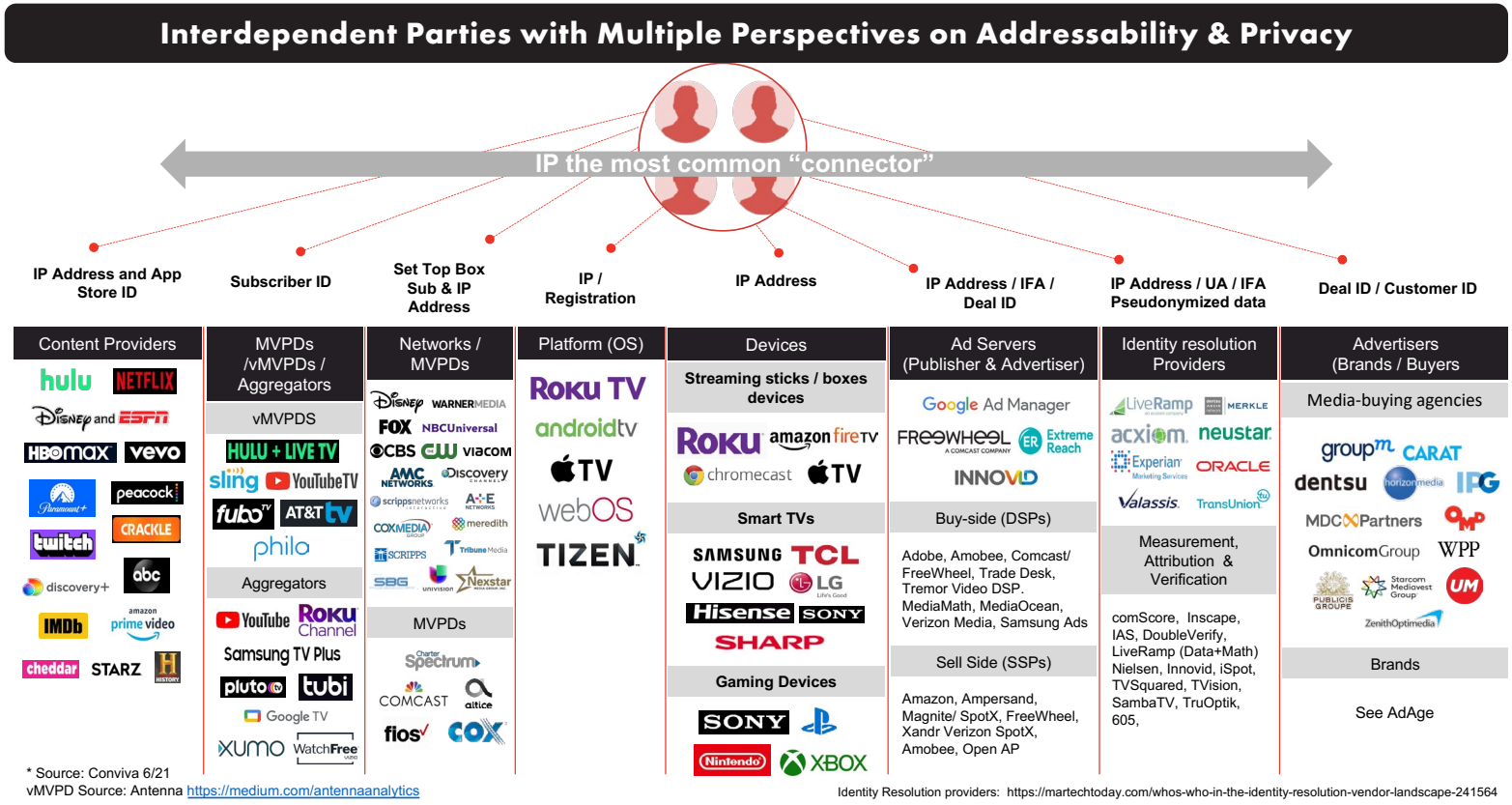
- Platforms and devices (CTVs), such as connected TVs, computers, dedicated streaming devices, and gaming consoles
- Virtual multichannel video programming distributors (vMVPDs) that aggregate live and on-demand television and deliver the content over the internet
- Subscription video-on-demand providers (SVODs) that provide streaming services requiring a paid subscription
- Advertising-based video-on-demand providers (AVOD) and free ad supported (FAST) services that provide premium streaming video content to CTV, as well as mobile, tablet, and desktop
- Content providers -- a term that can be used interchangeably with OTT providers -- that offer streaming content on a CTV platform or device, but are agnostic as to the type of device where streaming occurs
- Broadcast enablers that facilitate television broadcasting to CTV/OTT end users
- Publisher ad servers that enable ad serving on the publisher side, which in the OTT context, for example, could be supporting the CTV or content provider
- Advertiser ad servers that enable ad serving on the advertiser side
- Data management platforms (DMPs), customer data platforms (CDPs), and data clean rooms that collect, organize, and activate first-, second- and, third-party audience data for publishers, advertisers, and marketers

II. Who are the Stakeholders (*cont'd*)

- Supply side platforms (SSPs), exchanges, or other sell-side intermediaries used to coordinate and manage the distribution of ad inventories to optimize yield for publishers
- Demand side platforms (DSPs) or other buy-side intermediaries that allow the buyers of digital ad inventories to manage multiple ad exchanges via one interface
- Measurement/verification companies that provide viewability and measurement capabilities in the CTV and OTT environments
- Attribution companies that provide services that determine which ad campaigns lead to conversions
- Advertisers (brands/buyers) that are promoting their products and services across the CTV/OTT ecosystem
- Media-buying agencies that assist in the process of advertising, identifying ideal time frames, audiences, markets for reaching the target audience, and budgets for goals
- Identity resolution providers that support marketing processes around targeting, measurement, and personalization for both known and anonymous audiences across various digital and offline channels

II. Who are the Stakeholders (*cont'd*)

> The industry continues to evolve at a rapid pace, with new roles emerging



The industry continues to evolve at a rapid pace, with new roles emerging in addition to those listed above. Importantly for purposes of Project CCPA Crosswalk, most, if not all, of these entities process or have some relationship to personal information that is transmitted within the CTV/OTT ecosystem, whether because the information is necessary to perform a function, is a company asset, or is a targeted audience.

III. How Personal Information Is Shared within the CTV/OTT Environment

1 Applying CCPA's "Personal Information" Definition in the CTV/OTT Landscape

The CCPA defines "personal information" as any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a *particular consumer or household*" (emphasis added). This definition encompasses both direct identifiers, such as name, email address, or physical address, and also "indirect" and digital identifiers, including those used in the CTV or OTT context, such as proprietary user IDs (e.g., TIFA from Samsung, RIDA from Roku), IP address, household IDs, mobile advertising IDs (e.g., IDFA, GAID), and precise geolocation.

CTV/OTT targeting often happens at the household level via IP address, which is why the CCPA's inclusion of "household" in its definition of "personal information" is so important. However, advertisers may also target individuals at the user level, using the proprietary digital IDs of the device, platform, or content provider. These IDs are considered personal information of a consumer under the CCPA.

The sell-side of the industry collects and uses "personal information" (as defined by CCPA). First, device providers, content providers, vMVPDs, and other CTV/OTT publishers directly collect first party data from their own users. More specifically, publishers collect "ACR data" (the content that the user is watching), unique user ID (e.g., proprietary user ID assigned by a content provider or device manufacturer based on user log-in, such as Samsung's TIFA), IP address of the user's device, and, if available, any demographic information within the user's profile (if logged in). This information is combined and analyzed to better understand the viewing habits of (a) the user itself and (b) the user's corresponding household. From this, publishers create audience segments (such as groups of users tied to specific demographics or interests) that advertisers can target for advertising.

III. How Personal Information Is Shared within the CTV/OTT Environment (*cont'd*)

The buy-side of the industry also collects and uses "personal information" (as defined by CCPA). Advertisers may rely solely on publishers' first-party data (e.g., walled gardens) and work with those publishers to target advertising based on the advertiser's criteria. Advertisers may also choose to use their own first-party data to target users on CTV/OTT publisher properties. For example, advertisers may maintain their own personal information about their consumers, such as a consumer's name, purchase history, and physical address, which is stored in the advertiser's CRM. Advertisers translate the names and physical addresses into their targetable IDs because CTV/OTT users are targeted via digital identifiers (e.g., proprietary user IDs, MAIDs, or IP addresses), typically through the use of an "identity resolution provider" -- advertisers upload their CRM data (an "input file") and then receive the corresponding IP addresses or proprietary user IDs "keyed" to that CRM data (the "output file"). Advertisers then have different choices for how to target those IP addresses or other IDs contained within the output file, such as by providing them directly to the publisher (so that the publisher can target those households or users directly) or to a DSP (such as for real-time bidding purposes).

Finally, advertisers may also leverage third-party data. For example, an advertiser may want to expand its reach to new customers that are not in its own databases. To do so, an advertiser may go to a data marketplace and license third-party segments. For example, a "guitar buyers" segment may contain IP addresses of households with guitar buyers. Then, as in the example above, the advertiser can target that segment by providing the data to a publisher or to its DSP of choice.

2 Illustration: Server-Side Ad Delivery

The typical ways that an ad is served in CTV/OTT -- both "server-side ad insertion" and "run-time ad delivery" -- illustrate not only the technical complexity, but also the complexity of applying CCPA in this environment. The user and data flow in server-side ad delivery is as follows:

1. A user opens up an OTT app and selects "play" on an episode of the user's favorite show.

III. How Personal Information Is Shared within the CTV/OTT Environment (*cont'd*)

2. The app calls the **Publisher Ad Server** with a "get ads" action.
    a. In other words, the app needs to know, "What ad am I going to display to the user when it's ad-break time?" To assist the **Publisher Ad Server** to figure this out, the app sends to the Publisher Ad Server "personal information" such as the device IP address, proprietary user ID, device type, and content being displayed.
3. Based on the "personal information" provided, the **Publisher Ad Server** determines an appropriate advertiser ad campaign for this particular ad slot (e.g., based on user or household interest or characteristics).
4. The **Publisher Ad Server** then calls a **Server-Side Ad Insertion (SSAI) Vendor** to get the specific creative for that ad campaign from the **Advertiser Ad Server**.
    a. To do this, the **SSAI Vendor** passes to the **Advertiser Ad Server** similar "personal information," such as the device IP address, proprietary user ID, device type, and content being displayed.
5. Based on the "personal information" provided, the **Advertiser Ad Server** determines the specific creative to be served (e.g., a creative more tailored to user or household interest) and returns the creative to the **SSAI Vendor**.
6. The **SSAI Vendor** "stitches" the ad within the content that the user is watching so that the user sees the ad at the appropriate time during his or her viewing experience.
7. The app tells the **Publisher Ad Server** that the ad has been served (for impression tracking purposes), and the **Publisher Ad Server** provides the same to the **Advertiser Ad Server**.
8. The **Publisher Ad Server** and **Advertiser Ad Server** obtain measurement data via a **Measurement Vendor**, which may include aggregate data or more specific data, such as viewability, timestamp of view, and potentially IP address and/or device ID.

3 Illustration: Client-Side (or "Run-Time") Ad Delivery

Run-time ad delivery is very similar to server-side ad insertion except that ad delivery and data collection are primarily executed via the user's app, as opposed to via the ad servers. The user and data flow is as follows:

1. A user opens up an OTT app and selects "play" on an episode of the user's favorite show.
2. The app calls the **Publisher Ad Server** with a "get ads" action.
    a. In other words, the app needs to know, "What ad am I going to display to the user when it's ad-break time?" To assist the **Publisher Ad Server** to figure this out, the app sends to the **Publisher Ad Server** personal information, such as the device IP address, proprietary user ID, device type, and content being displayed.
3. Based on the personal information provided, the **Publisher Ad Server** determines an appropriate advertiser ad campaign for this particular ad slot (e.g., based on user or household interest).
4. The **Publisher Ad Server** will provide to the app an "ad manifest," which is basically a set of instructions regarding the ad that should be placed in the ad slot.
5. As directed by the ad manifest, the app will make an ad call to the **Advertiser Ad Server** to get the specific creative for that ad campaign from the **Advertiser Ad Server**.
    a. To do this, the app (as opposed to the "**SSAI Vendor**" in the Server-Side Ad Insertion example) passes to the **Advertiser Ad Server** similar personal information, such as the device IP address, proprietary user ID, device type, and content being displayed.

III. How Personal Information Is Shared within the CTV/OTT Environment (*cont'd*)

6. Based on the personal information provided, the **Advertiser Ad Server** determines the specific creative to be served (e.g., a creative tailored to user or household interest) and returns the creative to the app directly.
7. The app tells the **Publisher Ad Server** and **Advertiser Ad Server** that the ad has been served (for impression tracking purposes).
8. The app or **Advertiser Ad Server** obtains measurement data via a **Measurement Vendor**, which as noted earlier, may be aggregate or individual-level data.

IV. CCPA Classifications & Obligations Among Stakeholders

Many CTV/OTT participants, given the nature of their business, may function as a "business," "service provider," or a "third party" (as those terms are defined under the CCPA) depending on the data at issue and function performed. For example, based on the CTV/OTT survey:

- **Most platforms, devices, advertisers, and content providers** primarily viewed themselves as a "**business**," although a few acknowledged they could also be a "third party" purchasing personal information, or act as a "third party" processing personal information on behalf of another "business."
- Responses from **DSPs, SSPs, and other intermediaries (e.g., ad servers)** were about **evenly divided** in describing their roles as a "business," "service provider," or "third party." It is less clear from the survey, however, whether these responses reflect different interpretations of these terms, or whether the responses turned on particular functions and data flows in particular.
- **Measurement and attribution** companies **mainly** viewed themselves as a "**service provider**" but a few indicated they viewed themselves as a "business" or "third party," too. These responses do not necessarily account for all types of measurement and attribution services, and the entity classification may turn on some of the varied types of services and data combining that occurs.

With respect to data sharing arrangements:

- **Most** participants stated that they **contracted directly** with a party to buy, sell, or deliver ads for CTV/OTT, rather than work through an intermediary.
- **Most** participants also stated that they both engaged or participated in **programmatic ad buying/selling**, as well as **direct ad buying/selling** on CTV/OTT platforms.

IV. CCPA Classifications & Obligations Among Stakeholders (*cont'd*)

- The **majority** of participants stated that **platforms, devices, and identity resolution providers** were the **main sources** of personal information disclosed to them.
- Participants **most frequently shared** personal information **with publisher ad servers, DMPs, SSPs, DSPs, measurement/attribution providers, and advertisers**.
- The **vast majority** of participants **supplemented** their first party data with third party data. Participants also had ad partners assist them in purchasing third party data, but only about **half of participants viewed such partners as service providers**, and about **one-third** stated that the **partners used** the personal information for the **partners' own purposes**.

75%
of respondents stated they offered an opt-out of sales

For "Do Not Sell My Personal Information" compliance under the CCPA:

- Among those that viewed themselves as a business, about **75%** of respondents stated they **offered an opt-out of sales**.
- The **vast majority** stated they provided the opt-out by **directing consumers to their website to opt-out**.
- Some relied upon the **platform's "Do Not Sell My Personal Information" signals** or the **platform's "Limit Ad Tracking" (LAT) signals**.
- A few relied upon a **"Do Not Sell My Personal Information" option within their own app**.
- A few stated they **did not have an opt-out option within the OTT platform** (only via their web and mobile) or relied on an **option through their DMP**.

V. Whether and What Friction Points Exist in the Stakeholders' Aims to Address CCPA Compliance

As reflected in the section above, the clear theme from the survey responses was that there is a lack of consensus on which data sharing arrangements for ad purposes prompted the company to offer a "Do Not Sell My Personal Information" option, and where and how to offer such an option.

Simply put, opt-out mechanisms for "Do Not Sell" purposes are inconsistent across the participants. Many utilize a web-based "Do Not Sell" mechanism, which often does not easily apply to the CTV/OTT context without the manual suppression of identifiers. Some content providers rely on a platform/device-level opt-out or provide their own app-level opt-out (such as in the case where platforms/devices don't view the data flows above as "sales").

Additional guidance from the California Attorney General's Office may resolve some of the confusion among industry participants on these points. In the California Attorney General Office's summary of CCPA enforcement efforts over the past year,[3] the Office makes more clear that (a) use of personal information for ad targeting purposes is likely a "sale" under CCPA, and (b) "businesses" that direct users to opt-out via industry opt-out pages for general interest-based advertising is insufficient for purposes of providing a lawful "Do Not Sell My Personal Information" right under the CCPA.

The Office's enforcement summaries illustrate the need for participants in the CTV/OTT ecosystem to align with the Office's broad view of "sales." In other words, when participants act as "businesses," their disclosures of "personal information" to other participants, in nearly all cases, should be considered "sales," except when disclosing such "personal information" to their "service providers."

As such, *each* participant must provide a "Do Not Sell My Personal Information" mechanism in relation to such disclosures to non-"service providers." Furthermore, the "Do Not Sell My Personal Information" mechanism cannot direct users to opt-out on a generic industry page. Instead, users must be able to make requests directly to the "business" "selling" its personal information and that "business" must effectuate that opt-out (without further user action). Notably,

[3] Office of Attorney General. CCPA Enforcement Case Examples. State of California Department of Justice.

V. Whether and What Friction Points Exist in the Stakeholders' Aims to Address CCPA Compliance (*cont'd*)

the Office has not provided any examples of this concept as applied to a platform, such as CTV/OTT, and whether directing a consumer off-platform to a webpage to opt out of sales is sufficient.

Relatedly, the above requirements leave open whether an option such as "Limit Ad Tracking" might satisfy "Do Not Sell" obligations, but only where (a) "Limit Ad Tracking" is accessible via a link expressly titled, "Do Not Sell My Personal Information," and (b) activation of Limit Ad Tracking anonymizes information in the ad serving data flow (as opposed to allowing recipients to determine how to honor "Limit Ad Tracking"), so the business can show that the user's personal information is not sold pursuant to the CCPA.

The following examples from the California Attorney General Office's published enforcement summaries (all emphases added) underscore these points and the need for industry alignment:

"Pet Industry Website Updated its Opt-Out Webform for Consumers to Opt Out of All Sales of Personal Information"
Industry: Pet Industry
Issue: Authorized Agent; Sales of Personal Information

A business that operates an online pet adoption platform required a consumer's authorized agent to submit a notarized verification when invoking CCPA rights. The business's disclosures regarding its sale of data were also confusing, and the business did not appear to provide a mechanism for consumers to opt-out of the sale of their personal information. **The business also made consumers take additional steps to opt-out by directing consumers to a third-party trade association's tool designed to manage online advertising**. After being notified of alleged noncompliance, the business removed the notarization requirement for agents, added a "Do Not Sell My Personal Information Link", and updated its opt-out webform that allowed consumers to fully opt-out of the sale of personal information, **including personal information that was exchanged for targeted advertising**.

V. Whether and What Friction Points Exist in the Stakeholders' Aims to Address CCPA Compliance (*cont'd*)

Online AdTech Service Provider/Business Corrected Privacy Policy and CCPA Request Methods

Industry: Online Advertising

Issue: Non-Compliant Privacy Policy; Non-Compliant Service Provider Contracts

A company connects streaming services and various cable channels to advertisers that want to buy targeted ad space on those outlets. **The company's privacy policy was non-compliant with the CCPA because although it was primarily a service provider, it was also a business in some contexts**. Moreover, its service provider contracts did not contain the necessary restrictions on the use of processed personal information. After being notified of alleged noncompliance, the company modified its privacy policy including clarifying that it did not sell personal information and providing an accessible means for consumers to submit CCPA requests. The company also refined its CCPA request method instructions and updated its service provider contracts to be compliant with the CCPA.

Media Conglomerate Updated Opt-Out Process and Notices

Industry: Mass Media and Entertainment

Issue: Non-Compliant Opt-Out Process; Notices to Consumers

A mass media and entertainment business did not provide consumers with any methods to opt-out of the business's sale of their personal information. **The business only directed consumers to a third-party trade association's tool designed to manage online advertising**. The business's privacy policy and notice of right to opt-out also did not include required information about how consumers or their agents could exercise their opt-out rights. The business also did not have a notice at collection and **lacked a "Do Not Sell My Personal Information" link on several of its digital properties**. After being notified of alleged noncompliance, the business updated its opt-out process, privacy policy, and notices to address these issues, and added the "Do Not Sell My Personal Information" link to all of its digital properties.

VI. Next Steps for Solutions

One of the main friction points is the lack of a common way for CTV/OTT participants to offer consumers a "Do Not Sell My Personal Information" option within the CTV/OTT space, which may be exacerbated by the lack of consensus on the role of parties with respect to various data flows. These are challenges similar to those faced by industry participants when IAB first designed and implemented the CCPA Framework and LSPA for desktop and mobile. Learning from that experience, and taking into account the feedback from the CTV/OTT survey (as well as more recent California Attorney General guidance on CCPA compliance, as described in the section above), there are considerable industry and consumer benefits to having a clear industry standard and mechanisms to support "Do Not Sell My Personal Information" options designed specifically for the CTV/OTT environment and CCPA compliance. Such efforts can also provide much needed guidance to promote consensus on who and how parties can use these standards and compliance mechanisms to alleviate some of this friction.

The CTV/OTT working group will explore whether the CCPA Framework and LSPA may be a workable solution with adjustments, as necessary, to adapt it to the CTV/OTT environment. The working group will also explore whether there are best practices or technical innovations (by IAB Tech Lab or marketplace participants) that may provide additional solutions to assist parties in operationalizing CCPA compliance, including to harmonize privacy rights options across the CTV/OTT, desktop, and mobile environments.

VII. Conclusion

The fragmented nature of the CTV/OTT ecosystem creates differing approaches to CCPA compliance. Indeed, the role of each participant (e.g., platform, content provider, vMVPD, SSAI vendor) and whether that participant "sells" personal information has not been thoroughly examined on a large scale until now. IAB sees an opportunity to adapt existing compliance tools, such as the LSPA (or modified versions of it), or create other compliance tools to address CTV/OTT compliance challenges. We welcome any feedback to move the industry to a cohesive position for CCPA compliance.

About Us

The Interactive Advertising Bureau empowers the media and marketing industries to thrive in the digital economy. Its membership comprises more than 650 leading media companies, brands, and the technology firms responsible for selling, delivering, and optimizing digital ad marketing campaigns. The trade group fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. In affiliation with the IAB Tech Lab, IAB develops technical standards and solutions. IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of its public policy office in Washington, D.C., the trade association advocates for its members and promotes the value of the interactive advertising industry to legislators and policymakers. Founded in 1996, IAB is headquartered in New York City.

For more information, visit iab.com

About Our Sponsor

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust is the category-defining enterprise platform to operationalize trust. More than 10,000 customers, including half of the Fortune Global 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across privacy, security, data governance, GRC, third-party risk, ethics and compliance, and ESG programs.

The OneTrust platform is backed by 150 patents and powered by the OneTrust Athena™ AI. Our offerings include OneTrust Privacy, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust PreferenceChoice™, OneTrust ESG, and OneTrust DataGuidance™.

To learn more: OneTrust.com and LinkedIn