The Privacy Professional's Guide to Digital Advertising Across the Globe

APRIL 2021

WHITE PAPER/GUIDE

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Table of Contents

Contributors

Kai Koppoe (Fordham University School of Law), Dominique Shelton Leipzig (Perkins Coie LLP, Privacy & Security Partner, Co-Chair Ad Tech Privacy & Data Management), Scott Palmer (Perkins Coie, Beijing Managing Partner), Arsen Kourinian (Perkins Coie LLP, Data Privacy Counsel), Eduardo Paranhos (Esper, Paranhos, Gushiken Advogados, Founding Partner), Leonie Power (Fieldfisher LLP, Partner, Privacy and Information)

Kai Koppoe

Kai Koppoe is a third-year law student at Fordham University School of Law. She is a member of Fordham's Intellectual Property, Media, & Entertainment Law Journal, which is nationally ranked number one in intellectual property law. She is a certified data privacy professional and holds the CIPP/US credential through the International Association of Privacy Professionals (IAPP). She is a former Legal Policy Intern at the Future of Privacy Forum, where she worked on ad tech and global privacy issues.

Scott Palmer

Scott Palmer, Perkins Coie's Beijing Office Managing Partner and head of its China Intellectual Property practice, provides comprehensive counsel on intellectual property for foreign companies in China and Chinese companies in the U.S. Scott began his legal career in China over 19 years ago, is fluent in Mandarin Chinese and receives international recognition for his counsel to top brands and companies. He has been listed in Chambers Global and Chambers Asia-Pacific as a Leading Lawyer since 2011, and is also recognized by World Trademark Review.

Eduardo Paranhos

Eduardo Paranhos is founding partner at EPG Advogados. Before setting up the firm, he worked as General Counsel of Tetra Pak Americas, Head of Legal for HP Brazil and Commercial Lead Attorney at Microsoft Brazil. Eduardo holds an LL.M from the London School of Economics and Political Science (LSE). He was actively engaged in the industry debates around the bill of law that originated the LGPD. Eduardo received the Chevening Award from the British Government and volunteers as an Ambassador to its scholarship programs.

Dominique Shelton Leipzig

Dominique Shelton Leipzig is a Partner and Firmwide Co-Chair of the Ad Tech Privacy & Data Management Practice at Perkins Coie. Ms. Shelton is a leader in digital transformation strategies used by Fortune 100 companies and start-ups across a wide variety of industries including technology, retail, healthcare, and finance. She is ranked by Chambers & Partners in privacy & data security and is on the Executive Committee and Board of Directors of the International Association of Privacy Professionals (IAPP).

Arsen Kourinian

Arsen Kourinian is a certified data privacy professional, and holds the FIP, CIPP/US, CIPP/E, CIPP/C, CIPP/A and CIPM credentials through the International Association of Privacy Professionals (IAPP), and Privacy Management Professional certificate through OneTrust. As data privacy counsel at Perkins Coie, Arsen advises multinational corporations regarding compliance with domestic and international data privacy laws. When advising clients regarding compliance with these laws, Arsen provides practical and operational guidance on how to harmonize these laws into uniform policies, procedures, and practices.

Leonie Power

Leonie Power is a privacy specialist and has provided strategic and practical advice on the full range of privacy and data protection issues affecting business operations over a period of more than 17 years to a wide range of businesses across the retail, construction, property management and media sectors. She is a member of the Faculty of the International Association of Privacy Professionals (IAPP) and has spoken on data protection and privacy issues in the UK and abroad and provided specialist training.

The Privacy Professional's Guide to Digital Advertising Across the Globe

Around the world, countries are battling the COVID-19 pandemic and businesses are working to remain afloat and prosperous. As consumer behaviors have changed over the last year due to stay at home orders, working remotely, and efforts to limit the spread of the virus, businesses are rethinking their marketing strategies because traditional forms such as billboards or print ads reach fewer of their consumers. Among the companies that **prospered** during the pandemic were those that grasped the significance of technology, e-commerce, and digital advertising.

A key component to digital success is digital marketing and having the ability to reach customers where they are, which is now primarily at home. For companies to run successful global marketing campaigns, they must also be present where their consumers are and prioritize digital advertising. However, digital advertising creates privacy concerns for consumers. For this reason, many countries have implemented privacy regulations, with more to come this year. These regulations require that businesses protect individuals' personal information and that individuals have control over businesses sharing and using their personal information with third parties.

These concerns are critical now because of the regulatory attention surrounding browser-based tracking technologies, hereinafter called cookies, that are important to the digital advertising ecosystems. In the European Union, the use of cookies to facilitate targeted advertising has come under fire. **Multiple data protection authorities** have issued guidance about the use of cookies and other tracking technologies. Additionally, activists and groups such as Max Schrems and noyb (which filed **101 complaints** against European controllers) have been fighting against the prevalence of cookies for targeted advertising. In the United States, the California Consumer Privacy Act (CCPA) regulations require businesses to treat user-enabled global privacy controls (such as browser plug-ins, device settings, or other mechanisms) signaling consumers' choice to opt out of the sale of their personal information as a valid opt-out request. When these regulations were finalized in 2020, it was uncertain how enforcement authorities would treat such opt-out signals. This all changed on January 28, 2021, when the California Attorney General issued a **tweet** recognizing **Global Privacy Control** as a technical standard that satisfies the legal requirement, which caught businesses trying to comply with the CCPA off guard. The Federal Trade Commission has also cracked down on companies mishandling consumers' personal information, with **five privacy and security enforcement actions** reached this year, to date of publication. In addition to complying with global laws, a company may be significantly affected by the policies of the technology companies that are integral to its business structure and success. One such instance is Apple's plan, **announced last June**, to release a new feature that requires users to provide explicit opt-in consent before apps may track consumers across multiple

companies' apps, websites, or offline properties for targeted advertising. This feature will be released in the **upcoming iOS 14.5 update**, due by early spring 2021.

To help companies understand the ever-expanding opportunities and potential landmines associated with tracking technologies, this article aims to provide them with the tools necessary to run a successful global marketing campaign, while keeping compliant with the growing number of global privacy laws.

The Ecosystem

Digital advertising is the delivery of promotional materials through various online platforms, such as search engines, social media, websites, and other channels. This ecosystem can be broadly divided into three approaches to present advertising: display advertising, search advertising, and native advertising. Each of these advertising approaches provides a wide range of targeting, optimization, and performance measurement options, leveraging information about the context of the user interaction as well as information available about the specific user (for example, profiles or other information that may be linked to cookies).

Display Advertising

What It Is

Display advertising is a form of digital advertising that uses graphics and rich media to present advertisements or brand messaging to users. Display ads typically include banners, static images, videos, or text, which appear in specifically designated areas of a website or social media platform. It may appear as a full-screen ad while a page loads or until the user takes an action.

How It Works

In the most simplistic terms, advertisers contract to display their ads on publishers' websites. To streamline this highly complicated process involving many websites and advertisers, ad networks facilitate display advertising by working with both advertisers and publisher websites. The variations in service providers and solutions are vast and range over a broad spectrum of complexities to suit both advertisers' goals and publishers' requirements. Typically, ad networks and similar providers offer various platforms, technologies, and targeting capabilities to facilitate the display of ads on websites, or to specific users or groups of users.

Within display advertising, there is a variety of mechanisms an advertiser might use to reach their desired audience, such as contextual advertising, behavioral targeting

(also known as interest-based or tailored advertising), and retargeting. In contextual advertising, the ad is displayed based on the content and characteristics of the website where is it served. For example, an ad for luggage could be presented to users visiting a travel website. Behavioral advertising refers to advertisements predicted to be relevant to a user based on information collected across unaffiliated websites, such as displaying a travel ad to a 35-year-old parent on a social media website because they previously visited a travel website and it's almost spring break. Retargeting is type of behavioral marketing that results in highly relevant ads presented to a user with the goal of getting a user to re-engage with a product based on previous interactions with that advertiser. For example, a furniture ad could be presented to a user who previously shopped for furniture on the advertiser's website, but did not complete a purchase.

Search Advertising

What It Is

Search advertising is a form of advertising that displays ads within search results whenever a user searches for terms related to the services or products offered by the advertiser. These ads may also be referred to as sponsored ads, search marketing, search engine marketing, pay-per-click marketing, and cost-per-click marketing. These ads are based on the explicit need of users rather than an interpretation or prediction of their preferences.

How It Works

Most search engine companies provide platforms that allow advertisers to display ads within their search results. While each company has different procedures, they share a basic format. Advertisers compete for the opportunity to show their ads on the search results page. With every search, advertisers bid on keywords so that their ads are displayed when users are looking for specifically related search results. Advertisers provide keywords for an ad campaign and provide their bid amount if those keywords are searched by users. The bid is the maximum amount the advertiser is willing to pay for a click on their ad. When a web user types keywords in search and the keywords match the advertiser's keywords, the advertiser's link is displayed within the search results as an ad. Once a user clicks an ad, the advertiser pays the bid amount to the search engine. If there is no click, the advertiser does not pay. While the bid amount is important, search engines also look for ads that will be most relevant to the search and user. Simply put, search advertising is a relationship between a search engine and an advertiser where the advertiser pays the search engine when their ad is clicked, and in return, the search engine gives priority placement to the advertisers in addition to the search results.

Native Advertising

What It Is

Native advertising is a form of advertising that matches the form and function of the platform on which it appears. These branded content ads are typically meant to mirror the format and feeling of the website. There are primarily three types of native ads: in-feed, content recommendation, and native video. In-feed ads appear within content in a news feed and match the look and feel of the platform. Content recommendation, also known as content discovery, are ads that typically appear at the end of an article, feature suggested ads or content, and are designed to appear native to the page. Native video also mimics content on the platform and can be in-feed. These ads are typically auto-start without sound and appear on social networks such as Facebook, Twitter, Instagram, Pinterest and YouTube.

How It Works

Native advertising can be conducted in many ways. Advertisers can work directly with a website to create content for the site. Alternatively, advertisers can buy placements on publishers' websites and back-end technology ensures the ad content matches the format of each site.

Major Legislation

Since the European Union's General Data Protection Regulation went into effect in May 2018, countries across the globe have passed their own data protection laws. To date, over 120 countries have put in place legislation to secure the protection of data and privacy. For the purposes of this article, the focus is on the European Union, California, Virginia, China, and Brazil.

European Union

In the European Union (EU), two main pieces of EU-level legislation impact the advertising technology industry: the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Directive (ePrivacy Directive or ePD). The GDPR went into effect May 25, 2018 and the ePD has been in effect since 2002 (updated in 2009).

General Data Protection Regulation

The GDPR regulates how organizations may obtain, use, and store the personal data of individuals whose data is processed by a person or organization that is subject to the GDPR. It requires any organization that is involved in determining the purposes and the means of processing personal data to have a valid legal basis for such processing. There are six legal bases for processing: consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest. Businesses must let individuals know why they are collecting their personal data, how long they plan on keeping it, and which organizations (or types of organization) they will share the data

with. Individuals have the right to object to the processing of their personal data in some circumstances. Under the GDPR, organizations must be transparent about their personal data collection and use and disclosure practices, and they must provide EU citizens with certain rights to their personal data, such as access, correction, deletion, objection, and data portability.

The advertising industry often relies on consent as the legal basis for processing. Article 4(11) of the GDPR defines consent as "any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." While consent is often the legal basis used, there is also a question of whether legitimate interest can be a valid basis for processing personal data for behavioral targeting advertising purposes. The current regulatory environment suggests that it will be difficult to rely on legitimate interests in the case of advertising that is based on building extensive profiles using data from a variety of sources. In December 2020, the **Austrian Superior Court** suggested that a user contract can be used to process information for personalized advertising purposes without obtaining consent from users, which effectively means that organizations can bury the information about legal basis in their terms and conditions. Doing so allows them effectively to circumvent the need to obtain consent in circumstances where it is likely to be otherwise required.

The GDPR impacts the ad tech industry as a lot of advertising relies on programmatic behavioral targeting using user data. The GDPR is designed to protect against the building of profiles around personal data without the person's knowledge or consent, using data in automated decision making without appropriate safeguards (where that decision is likely to have a legal or similarly significant effect), and with unsafe storage and leakage of personal data. While it does not outlaw personal data usage, for many scenarios involving the use of personal data for personalized ad targeting, the likely appropriate legal basis is consent so that companies will need to get permission before the personal data is used for such purposes. Ad tech companies can continue to do cookie matching, frequency targeting, programmatic ads, and more, provided that it has an appropriate legal basis under the GDPR for the relevant personal data processing (i.e., the user consents) and it otherwise complies with the GDPR.

The GDPR is intended to be technology neutral and as such applies to the treatment of personal data. For this reason, it does not directly apply to cookies per se. However, much of the information collected via cookies, including any cookie ID or data linked to cookies, is likely to be regarded as personal data, the processing of which is subject to the GDPR.

ePrivacy Directive

The Privacy and Electronic Communications Directive, often referred to as the ePrivacy Directive, is focused on protecting the privacy and security of personal data in electronic communications. In 2009, the Directive was updated and the amended version is sometimes referred to as The Cookie Law as it contains requirements that apply to all technologies used for tracking. In fact, the term "cookie" is used as shorthand for any means of accessing information on a device or storing of information on a device. The Directive explicitly requires a data controller to obtain informed consent from users in order to use cookies, but it provides an exception for cookies that are strictly necessary. It defines strictly necessary as cookies used for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by a user, e.g., of a website or mobile app. Recital 17 of the ePrivacy Directive states, "consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website." In practice, this is often implemented via a cookie banner or other interstitial notice that is displayed at a user's first visit to a website and includes a mechanism for indicating consent. Prior to obtaining such consent, no cookies, except strictly necessary cookies, can be set.

In May 2020, the European Data Protection Board (EDPB) provided an **updated guidance** on consent under the GDPR. The guidance sought to provide clarification in two areas: "cookie walls" and what constitutes valid consent. Cookie walls are mechanisms that require a user to accept the use of cookies and similar technologies as a precondition to gaining access to the website or service. The EDPB stated cookie walls do not constitute valid consent under Article 5(3) the ePrivacy Directive as the lack of options prevents consent from being freely given. The second clarification was that a cookie banner cannot rely on scrolling or swiping through a webpage as consent as it "will not under any circumstances satisfy the requirement of a clear and affirmative action." It emphasized that the action that grants consent must be distinguishable from other actions. It must be clear to data subjects what action constitutes consent and data subjects must be able to withdraw their consent just as easily as they can give it. Additionally, consent may not be "bundled", that is, presented as a non-negotiable part of terms and conditions.

Cookie compliance under the GDPR and ePrivacy Directive requires five elements. First, an organization must receive a user's consent prior to implementing the use of any cookies, except those that are strictly necessary for the basic function of the website. Second, the organization must provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received. Third, it must document and store consent received from users. Fourth, it must allow users access to its service, even if they reject the use of certain cookies. Finally, it must provide

user-friendly opt-in and opt-out options. Recent guidance from various **data protection authorities** provides different levels of granularity for the options provided to users, whether it be allowing a user to provide specific consent for each purpose or at whatever layer consent options are provided. A deadline of note: **beginning March 31, 2021**, the French Data Protection Agency, Commission Nationale de l'Informatique et des Libertés (known as the CNIL), will begin enforcing its new cookie rules. These rules require cookie banners to include the purpose for which the cookies are used and to allow users to accept or refuse cookies with the same level of simplicity.

Upcoming Legislation

On February 10, 2021, the European Council agreed to its draft text of the proposed ePrivacy Regulation. The draft ePrivacy Regulation will cover electronic communications content transmitted using publicly available services and networks and related metadata. It will address cases when service providers are allowed to process electronic communications data or have access to data stored on end-users' devices. It will apply when end-users are in the European Union but will cover cases where processing of that end-user content and metadata takes place outside the EU or when the service provider is established or located outside the EU. The draft notes that end-users should have a genuine choice whether or not to accept cookies or similar technologies. Access to a website that is dependent on cookie consent for additional purposes as an alternative to a paywall is permitted provided the user is able to choose between that offer and an equivalent offer by the same provider that does not involve consenting to cookies. In an effort to prevent cookie consent fatigue, an end-user will be able to give consent to the use of certain types of cookies by whitelisting providers in their browser settings. Software providers are encouraged to make it easy for users to set up and amend whitelists on their browsers and withdraw consent at any time.

The European Commission submitted two legislative proposals: the Digital Services Act and the Digital Markets Act. The proposals are intended to modernize the EU's legal framework for online services, the e-Commerce Directive, which went into effect in 2000. The main goals are to create a safer digital space where the fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness, both in Europe and globally. The **Digital Markets Act** (DMA) is aimed at tackling large, systemic online *platforms*. It creates a narrow set of criteria for a large online platform to be deemed a "gatekeeper"—a company that controls data and access to their platform. There are three main cumulative criteria that mean a company will be within the scope of the DMA, namely that: (i) the company is of a size that impacts the internal market (there are presumptions about when that is the case, including that it provides a core platform service in at least three EU countries); (ii) the company has control of an important gateway for business users towards final consumers; and (iii) the company has an entrenched and durable position either at present or foreseeably in the near future. A company is presumed to

have control of an important gateway if it provides a core platform service and has more than 45 million monthly active users in the EU and over 10,000 yearly active business users established in the EU in the last financial year. These companies will be required to share certain kinds of data and will be prohibited from leveraging data from their platforms to compete with their business users. The **Digital Services Act** (DSA) primarily addresses online intermediaries and imposes the most extensive requirements on very large online platforms, i.e., 45 million or more active monthly users in the EU. Companies will be required to publish information about their online advertisers and provide more transparency about algorithms used for suggestions and ranking. These two proposals, if passed in their current or a substantially similar form, stand to have a major impact on online advertising companies, in addition to large technology companies.

United States

California

In the United States, there is no comprehensive federal data protection law (there are only sectorial laws) and the dominant law that affects the advertising technology industry is the California Consumer Privacy Act (CCPA). Prior to the CCPA, the dominant legal enforcement mechanism for online advertising was the Federal Trade Commission, discussed in greater detail below. Although the CCPA is a state law, companies outside of California that do business in California, collect Californians' personal information, and otherwise meet certain thresholds must comply. It is a state-wide regulation that creates new consumer rights pertaining to the access, deletion, and sharing of personal information by businesses. While the CCPA is generally an opt-out law, there are three circumstances in which a consumer must opt-in. First, a consumer who is at least 13 years old and less than 16 years old, or the consumer's parent or guardian for consumers under the age of 13, may affirmatively authorize the sale of the consumer's personal information. Second, when consumers have opted out of the sale of their personal information, a business must wait at least 12 months before requesting the consumers to opt back in. Third, a consumer may consent to participate in a financial incentive program.

Consumer rights under the CCPA impact the ad tech industry as targeted advertising often relies on consumers' personal information, including geolocation data, browsing history, cookies, and more. The CCPA includes a notion of "business purposes" which refers to situations where, even if the user opts out of the sale of their personal information, a business can continue to use their personal information. While a business purpose focuses on internal uses and not pecuniary gain, it does include digital advertising. The CCPA requires businesses to disclose to consumers, at or before collection, the categories of personal information the business collects about consumers and the purpose for which the categories of information are used. Additionally, if the

business sells consumers' personal information, the notice at collection must include a Do Not Sell link and a link to the business's privacy policy. The CCPA applies to unique personal identifiers, which includes cookies. The CCPA does not require the use of cookies to be disclosed in a cookie banner or for a business to obtain consent prior to the use of cookies.

The California Privacy Rights Act builds upon and amends the CCPA and goes into effect January 1, 2023 and will be enforced starting July 1, 2023. It includes a one-year "look-back" provision that will govern data collected starting January 1, 2022. It remains an opt-out law but allows minors under the age of 16 to opt-in. The CPRA gives consumers additional rights, including the right to correction, right to access, right to opt out of sharing, and right to limit use of sensitive personal information. The new subcategory of personal information, sensitive personal information, includes government identification numbers, login credentials and passwords, precise geolocation data, race, ethnicity, religion, union membership, sexual orientation, genetic data, and personal communications. When a consumer exercises their right to opt out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, businesses must refrain from selling, sharing, using, or disclosing that information and wait at least 12 months before requesting a consumer opt back in. Consumers have the right not to have their personal information shared for cross-context behavioral advertising. This allows consumers to opt out of any third party collection on websites and applications.

Virginia

On March 2, 2021, Virginia Governor Northam signed the **Virginia Consumer Data Protection Act** (VCDPA) into law. It will take effect January 1, 2023, the same day the CPRA goes into effect. The VCDPA applies to entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and meet one of the following prongs: (i) they control or process the personal data of at least 100,000 Virginia consumers during a calendar year; or (ii) they control or process the personal data of at least 25,000 Virginia consumers and derive at least 50% of its gross revenue from the sale of personal data. The law does not apply to Virginia state government entities, financial institutions or data subject to the Gramm-Leach-Bliley Act, covered entities and business associates governed by the U.S. Department of Health and Human Services, nonprofits, or institutions of higher education. The law defines consumers as natural persons who reside in Virginia and act in an individual or household context. It does not apply to persons in an employment or commercial context. The VCDPA concept of controller and processor is similar to the GDPR. Under the VCDPA, a controller is the party that determines the purpose and means of processing personal data and a processor is the natural or legal entity that processes personal data on behalf of a controller. The law does not provide for a private right of action.

The VCDPA protects personal data, defined as any information that is linked or reasonably linkable to an identified or identifiable natural person. The term does not

include de-identified data or publicly available information. The VCDPA covers sensitive data, a category of personal data, which includes personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, children's data (under the age of 13), and precise geolocation data. The law requires controllers to obtain affirmative opt-in consent before processing sensitive data.

Virginia consumers have rights of access, correction, deletion, portability, and opt-out for targeted advertising, sale, and profiling. Under the VCDPA, the opt-out requirements only apply if the data is exchanged by a controller to a third party for monetary consideration, unlike the CCPA, which requires monetary or other valuable considerations. Where personal data is shared but no money is exchanged between the business and the third party, a consumer cannot opt out of the sharing of their personal data. Controllers are required to conduct data protection assessments for the following categories: the processing of personal data for targeted advertising; the sale of personal data; the processing of personal data for profiling; the processing of sensitive data; and any other processing activities that involve personal data that presents a heightened risk of harm to consumers.

Upcoming State Laws

As 2021 progresses, **more states** are expected to pass data protection laws. On March 4, 2021, the Oklahoma Computer Data Privacy Act (OCDPA) was passed in the Oklahoma House of Representatives and has moved to its Senate. If passed, it would become effective November 1, 2021 and would be one of the first opt-in data privacy laws in the United States. The OCDPA would require companies to obtain explicit permission to collect and sell personal data. The law requires companies to disclose what personal information they hold about a consumer and to allow for that information to be deleted upon the consumer's request. The act also provides a private right of action.

On March 3, 2021, the Washington Privacy Act (WPA) (Senate Bill 5062), passed in the Washington Senate. If passed, it would take effect July 31, 2022. The WPA would give consumer rights of access, correction, deletion, data portability, and the right to opt out of processing for targeting advertising, sale, or profiling. It would require written agreements between controllers and processors, and would require processors to receive approval from controllers before entering into agreements with sub-processors. Companies would be required to adopt reasonable security standards and issue privacy notices. This act does not have a private right of action. While Virginia is the most recent state with a data privacy law, other states like New York (with over 50 privacy bills), Florida, and Utah have data privacy laws in the works.

The Role of Government Agencies

The Federal Trade Commission (FTC), acting under the authority of Section 5 of the Federal Trade Commission Act (FTC Act), seeks to prohibit unfair or deceptive trade

practices by organizations. In 2017, the FTC released a report on **Cross-Device Tracking**, a method used for understanding a user's habits that can subsequently be used for targeted advertising. The report acknowledged the benefits for the advertising community but raised concerns with probabilistic tracking, which occurs when a company infers that a user is connected to a device through indirect means. The FTC recommended companies that engage in cross-device tracking focus on transparency, choice, sensitive data, and maintaining reasonable security of collected data.

In 2015, the FTC **denounced** native advertisements that are deceptively formatted to mislead consumers into believing they are independent, impartial, or not from the sponsoring advertiser itself, and it issued a **business guide**. The FTC places great importance on transparency and requires ads to not mislead consumers to believe the content is anything other than an ad. The guidance provides examples of when a business should disclose that content is native advertising and provides advice on how to make clear and prominent disclosures to avoid misleading consumers. The FTC's commitment to striking down deceptive native ads significantly impacted social media's use of this form of advertising. The FTC, in its **Enforcement Guides**, requires endorsers to provide clear and conspicuous disclosure of sponsorship. The FTC has the authority to impose penalties upon companies that violate the FTC Act, and companies should take care to comply with the law.

China

China has a number of laws and regulations that impact the processing of personal information, but its recent draft Personal Information Protection Law (PIPL), will be its first national-level data privacy law and is expected to pass this year. The law applies to organizations and individuals handling personal information activities of natural persons in China. It also has an extraterritorial scope and applies in the following three circumstances: where the handling activity purpose is to provide products or services to natural persons inside the borders; where conducting analysis or assessment of activities of natural persons inside the borders; and where other circumstances provided in laws or administrative regulations exist. "Handling" of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, and other similar activities. The PIPL requires the personal information handler to inform individuals, in a conspicuous way and in clear and understandable language, the identity and contact information of the personal information handler, the purpose and method of personal information processing, the type and storage period of personal information to be handled, the ways and procedures for individuals to exercise their rights, and other matters as stipulated by laws and regulations.

The PIPL has six legal bases that allow for handling personal information: having obtained consent from the person; for purposes of concluding or performing a contract; for

purposes essential to fulfilling statutory duties or obligations; for purposes essential to responding to sudden public health incidents or protecting natural persons' lives and health, or the security of their property under emergency conditions; for purposes within the reasonable scope of actions for public interest; and in other circumstances as provided by Chinese laws and regulations. It provides a number of rights, including the right to know and decide about the handling of their personal information, the right to correct or complete inaccurate personal information, and the right to deletion of personal information. Like other countries, it includes special rules for "sensitive information" which is all personal information that, once leaked or illegally used, may cause discrimination or grave harm to individuals or personal property security. This includes information on race, ethnicity, religious beliefs, individual biometric features, medical history, health, financial accounts, and individual location tracking. To process sensitive information the handler must obtain separate opt-in consent.

Brazil

Brazil's comprehensive data protection law, Lei Geral de Proteção de Dados Pessoais (LGPD) went into effect in September 2020, after a long string of congressional changes to the implementation date. The LGPD applies to any natural person or legal entity, including the government, that processes the personal data in Brazil, or data collected in Brazil, which involves processing activities targeting subjects located in Brazil, even if the entity processing the data is based outside the country. There are exemptions under Article 4 of the LGPD, determining that the law does not apply to the processing of data carried out by individuals exclusively for private and non-business purposes, for journalistic and academic reasons, or if done exclusively for public security, national defense, state security, or criminal investigations. It provides individuals with rights, including: access to data; access to correct incomplete, inaccurate, or out of date data; and ability to revoke consent. Additionally, it outlines 10 legal bases for data processing: explicit consent, contractual performance, legal obligation, legitimate interest, public policies, life protection, health protection, protection of credit, research by public study entities, and exercise of privileges in legal proceedings. Where consent is the applicable legal basis, the law states that it must be a free, informed, and unambiguous manifestation of a data subject agreeing to the processing of personal data for a specific purpose. Consent was also referenced in Article 7(IX) of Law No. 12.965, Brazil's Internet Framework. It required that express consent must be given for the collection, use, storage, and treatment of personal data and that the consent clause must be "distinguished from other clauses," thus taking a narrower approach to consent than the LGPD. Article 9 of the LGPD states data subjects must have the right to facilitated access to information, with respect to the purpose of processing, duration of processing, identity of the data controller, entities to whom the data will be disclosed, and rights of the data subject, and their right to deny consent.

The LGPD has provisions related to sensitive personal data, or data that is considered particularly susceptible to discriminatory practices. Under the LGPD, it includes personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical, or political organization membership, health or sex life, and genetic or biometric data.

The LGPD does not specifically mention cookies. However, cookies may fall under the broad definition of personal data: "any information that identifies or makes identifiable a natural person," as most cookies collect personal data. The use of cookies needs to be within one of the 10 legal bases. Most controllers are resorting to consent as the prevailing legal basis for cookies. Cookie consent must be provided by the data subject in writing or any other means that demonstrates the data holder's will. In theory, it is also possible for a data controller to rely on legitimate interest to collect data via cookies or as a part of an agreement, although this would have to be assessed vis-à-vis the concrete scenarios—for most cookie implementations, consent will likely be the applicable legal basis.

While an amendment to the LGPD postponed the implementation of the administrative fines to August 2021, this has not prevented law enforcement authorities from pursuing privacy-related cases on the basis of the LGPD, combined with remedies set forth in consumer protection laws.

The Role of Private Businesses

While companies must comply with government and global legislation, individual companies can have just as powerful of an impact on the advertising world. Last June Apple announced plans to require developers to obtain opt-in consent to track users, including via Apple's Identifier for Advertisers (IDFA). The IDFA allows advertisers to indefinitely track user interaction and use that information to build user profiles that are attached to a device. Apple's updated requirement will be implemented starting in iOS 14.5, which will be released in early spring 2021. Users will receive a one-time prompt per app, asking for their tracking preferences. With Apple's new change, app developers will be limited in their ability to track users' behaviors for advertising purposes without opt-in consent through Apple's provided framework. Google is another large platform that announced changes to its policies, which will greatly impact ad tech. Google will require third party cookies, the backbone of programmatic advertising, to be eliminated in its Chrome browser by 2022. On March 3, 2021, Google **announced** it would not build alternate identifiers to track individuals across websites or use third party cookies in their products. While the laws are working to catch up to technology and the need for greater consumer data protection, business initiatives might overtake these efforts and create regimes that restrict the use of traditional tools used by the industry to create an opt-in framework.

Display Advertising Ecosystem

Player	Player's Role	Tracking Technologies ** Used Include *broadly referred to as cookies*	Brazil's LGPD Position and Reason for Designation**	California's CCPA | CPRA Position and Reason for Designation	China's Draft PIPL Position and Reason for Designation	European Union's GDPR | ePrivacy Directive Position and Reason for Designation	Virginia's Consumer Data Protection Act Position and Reason for Designation
Advertiser	An entity that purchases inventory for the presentation of messaging to users. An advertiser is responsible for producing and organizing ad messaging, images, videos, and other creative products.	• Cookies • Web Beacons • Embedded Script • Entity Tags • Unique Device Token • Deterministic Fingerprinting Technologies • Probabilistic Fingerprinting • Device Graphs	Controller to ad agency, DSP, and ad exchange as it makes the decisions regarding the processing of personal data. Article 5 (VI).	**CCPA:** Considered a business with respect to first party data collected. Typically, not in privity with the demand side platform or ad exchange on the supply side and would be considered a third party with these players. Section 1798.140 (c). **CPRA:** Same reasoning as CCPA, except CPRA excludes cross-context advertising. If the advertiser uses third party information, then it must be considered a third party. Under Section 1780.140(d)(4)(E)(6), the updated definition of business purpose explicitly states cross-context behavioral advertising is not considered a "business purpose."	Personal information handler to ad agency, DSP, ad exchange, and DMP, as the advertiser independently determines the means of processing personal data. Articles 4 and 9.	Controller to ad agency, DSP, and data management platform as these players usually process personal data on behalf of the advertiser (albeit these players may also be controllers in their own right for other processing operations). Articles 4(7), 4(8) and 24. Depending on the relationship and the extent to which an ad agency, demand side platform or data management platform is involved in determining the purposes and means of processing in conjunction with the advertiser, the advertiser may be considered to be a joint controller with one or more of these other parties. Article 26.	Controller to ad agency, DSP, ad exchange, and DMP, as the advertiser determines the purpose and means of processing personal data. §§ 59.1-571, 574.
Ad Agency	Ad agencies help clients manage the advertising process, including the creative process, ad		Processor to advertiser, according to Article 39. When the agency processes	**CCPA:** Ad agencies may be service providers with respect to advertisers, if the contract satisfies	Entrusted party of advertiser provided an agreement is in place that includes an outline of	Generally considered a processor under Article 28 if it receives personal data	Provided there is a contract and the ad agency adheres to the advertiser's instructions, it is a processor. §§ 59.1-571, 575.

	buying, and budget allocation.		personal data in the name of, or on behalf of, the controller, it acts as a processor.	service provider requirements. Common examples would be for conversion tracking, retargeting, or custom audiences. However, ad agencies are typically considered "third parties" under 1798.140(w) to demand side platforms and exchanges. **CPRA:** Typically considered a service provider as it processes information on behalf of the advertiser.	the rights and duties of both the agency and the advertiser, as well as the purpose and ways of handling personal information, and includes the category and protection measures of the personal information. The advertiser is obliged to monitor the personal information handling activities of the ad agency. Article 22.	from advertiser. There should be a binding contract or other legal act that satisfies the processor requirements as provided by Article 28(3). Depending on the extent to which it is involved in determining the purposes and means of processing in conjunction with the advertiser, it may be considered a joint controller with the advertiser. If it is using the personal data for any of its own separate purposes, e.g., research purposes, it is likely to be regarded as a separate and independent controller for such purposes. Article 4(7), Article 24, Article 26.	
Demand Side Platforms (DSP)	DSPs provide the technology advertisers use to manage ad inventory in an ad exchange. Advertisers and agencies work with DSPs to target ads based on defined criteria. DSPs work to buy ad space as cheaply as possible from publishers.		DSPs are considered processors to advertisers as they process information on their behalf. Article 39.	DSPs can be considered "service providers" under 1798.140(v) or "third parties" under 1798 .140(w), depending on how the DSP positions itself as using advertiser data. Certain DSPs process personal information on behalf of advertisers pursuant to contracts that limit their use of the personal	Entrusted party or third party under Articles 22 and 24. If an agreement is in place between the advertiser/ ad agency that outlines the purpose for entrusted handling, the handling method, the categories of personal information, protection measures, and the rights and duties of both sides, then the DSP will likely be considered an	DSPs may be considered processors or sub-processors on behalf of advertisers for the purposes of Article 28 but, depending on a DSP's role in determining the purposes and the means of the processing of the relevant personal data, it could be a controller or joint controller with advertisers or other ad tech players (which should be	DSPs are processors, provided there is a contract, and the DSP adheres to the advertiser's instructions. If the DSP determines the purpose and means for processing data, it will be a controller. §§ 59.1-571, 574, 575.

				information for the purpose of performing services specified in the contracts and would likely be considered "service providers." Other DSPs position themselves as third parties with respect to the data they receive because they use the data for their own commercial purposes. Note that consumer advocacy groups such as Californians for Consumer Privacy consider these entities to be third parties, for which a Do Not Sell My Personal Information link is necessary. --- **CPRA:** Considered third parties because they use first party and third-party data to create profiles.	entrusted party. In the event there is no agreement, the DSP will be considered a third party.	reflected in the relevant contract terms). Article 4(7), Article 24, Article 26, Article 28.	
Data Management Platform (DMP)	Technology platform used to consolidate audience and campaign data from various sources to help advertisers manage their audiences and marketing programs more efficiently. Used in combination with DSP on		DMPs are likely to be considered processors but if the DMP offers other services or uses consumer data for its own purposes, it could be a controller. Article 39.	**CCPA:** Depending on contract language, DMPs can be considered "service providers" under Section 1798.140(v) to the advertiser, provided the DMP does not use the data for its own commercial purposes. However, most DMPs also provide other services that may exchange	Entrusted party as it receives and uses data from other players and in accordance with those players' specifications. If the DMP offers other services, then it may be considered a third party. Articles 22 and 24.	Generally considered processors but may be joint controllers with other service providers. DMP generally uses data from DSP or SSP for a specific purpose that it does not specify or control. If the DMP uses consumer data for its own purposes or if it offers	DMPs are likely to be considered processors provided they have a written contract and follow the advertiser's or publisher's instructions. If the DMP offers other services or uses consumer data for its own services, it will be a controller. §§ 59.1-571, 575.

	advertiser's side or SSP on publisher's.			data, which would make them a third party. Individual uses of DMPs should be scrutinized in each vendor contract to ensure whether (or not) any specific DMP provider is in fact a service provider. Note that consumer advocacy groups such as Californians for Consumer Privacy consider these entities to be third parties, for which a Do Not Sell My Personal Information link is necessary. **CPRA:** DMPs could be service providers, contractors, or third parties depending on whether they combine first party and third-party data. More information will be provided in upcoming regulations.		integrations with other entities that may exchange data, it may be considered a controller or a joint controller. Article 4(7), Article 4(8), Article 24, Article 26, Article 28.	
Ad Exchange	An ad exchange is a marketplace for buying and selling ad inventory. Publishers sell ad inventory in an auction environment for advertisers to buy in real time. This is done via Real-Time Bidding, an auction that takes place in the time		Depends on the data processing activity. When the ad exchange determines what information to collect and process, it acts in the role of a controller. When it relies on information provided by other players, it is a	**CCPA:** Depending on the data-handling activities at issue, ad exchanges could be service providers but most often are treated as "third parties" under Section 1798.140(w) by the CA Attorney General's office	Depending on the data-handling activities, it can be considered a personal information handler or entrusted, under Article 4 and 22. If the ad exchange acts according to an agreement, it is an entrusted party. If the	Depends on the data-handling activities. When the ad exchange determines what data to collect and/or how to process, it is a controller because it controls the means and purpose, according to Article 4(7).	Depends on the data-handling activities, it can be considered a controller or processor. If the ad exchange determines what information to process, it is the controller. If it relies on information received from

	it takes to load a webpage.		processor. Article 5 (VI and VII).	in nonpublic enforcement actions. This is a dynamic area, and more information will be available with public enforcement actions. ——————— At times, an ad exchange determines what data to collect and how that data is processed, while in others, it acts on the instructions of its clients. Ad exchanges also act as a third party for purposes of its B2B sales and marketing. For other functions, ad exchanges are service providers, acting on behalf of and in accordance with the instructions of its clients. Note that consumer advocacy groups such as Californians for Consumer Privacy consider these entities to be third parties, for which a Do Not Sell My Personal Information link is necessary. **CPRA:** Ad exchanges are mostly businesses, contractors, or third parties, depending on data-handling practices.	ad exchange determines what data to process, it is a personal information handler.	When it acts on the instructions of its clients, it is a processor under Article 4(8). Depending on its data processing arrangements with other ad tech players, it may be regarded as acting as a joint controller with such other players. Art. 26.	other players, it is a processor. §§ 59.1-571, 574, 575.

Supply Side Platform (SSP)	SSPs provide the technology that publishers use to connect their inventory (ad space) to ad exchanges. SSPs work to sell ad space to advertisers.		SSPs are considered processors if they work on behalf of a publisher and uses the information it provides. Article 5(VII).	**CCPA:** SSPs can be considered "service providers" under 1798.140(v) or "third parties" under 1798.140(w), depending on how the SSP positions itself as using advertiser data. Note that consumer advocacy groups like Californians for Consumer Privacy consider these entities to be third parties, for which a Do Not Sell link is necessary. **CPRA:** SSPs could be service providers, contractors, or third parties depending on whether they combine first party and third party data. More insight will be provided in upcoming regulations.	Entrusted parties working on behalf of publishers. Use information provided by publisher to aid in selling ad space in the exchange. Article 22.	Often regarded as processors working on behalf of publishers because they utilize information provided by publisher. Could be a controller or joint controller based on its role in determining the purposes and means of processing (which should be reflected in the contract terms). Articles 4(7), 4(8), 24 and 28.	Considered processors working on behalf of publishers. If it determines the purpose and means of processing it could be a controller. Depends on contract terms. §§ 59.1-571, 575.
Ad Server	The entity responsible for facilitating the presentation of an ad on a website or app.		Depends on the data processing activity. When the ad server determines what information to collect and process, it acts in the role of a controller. When it relies on information provided by publisher or other players, it is a processor. Article 5 (VI and VII).	**CCPA:** Depending on the data-handling activities at issue, ad servers could be service providers under the CCPA. **CPRA:** Depending on the data-handling activities at issue, ad servers could be service providers.	Depending on the data-handling activities, it can be considered a personal information handler or entrusted, under Articles 4 and 22. If the ad server acts according to an agreement, it is an entrusted party. If the ad server determines what data to process, it is a personal information handler.	Processor to publishers because they utilize information provided by publisher. Could be a controller or joint controller based on its role in determining the purposes and means of processing (which should be reflected in the contract terms). Articles 4(7), 4(8), 24 and 28.	Depends on personal data processing. If it uses information provided by publisher and according to contract, it is a processor. May be a controller if it determines what information to collect and process. §§ 59.1-571, 574, 575.

Publisher	Publisher provides advertising space on a website or app.		Controller to SSP, ad exchange, and DMP as these players process information provided by the publisher, for its benefit. Article 5(VI).	**CCPA:** Considered a business with respect to first party data collected. Typically, not in privity with the ad exchange and would be considered its third party. Section 1798.140 (c). **CPRA:** Considered a business with respect to first party data. Section 1798.140 (d).	Personal information handler to SSP, ad exchange, and DMP, as the publisher independently determines the means of processing personal data. Article 4 and Article 9.	Controller to SSP, ad exchange, and DMP as these players process information on behalf of the publisher (although may be a joint controller with any of these entities depending on their role in determining the purposes and means of processing). Article 4(7), Article 4(8), Article 24, Article 26 and Article 28.	Controller to SSP, ad exchange, and DMP as the publisher determines the means and purpose of processing. Depending on contract terms it could be a joint controller. §§ 59.1-571, 574.

** For all players presented as processors, the designation may change if the data subject contracts directly with the player.

Search Advertising Ecosystem

Player	Player's Role	Tracking Technologies ** Used Include *broadly referred to as cookies*	Brazil's LGPD Position and Reason for Designation**	California's CCPA | CPRA Position and Reason for Designation	China's Draft PIPL Position and Reason for Designation	European Union's GDPR | ePrivacy Directive Position and Reason for Designation	Virginia's Consumer Data Protection Act Position and Reason for Designation
Advertiser	An advertiser is an entity that purchases inventory for the presentation of messaging to users. An advertiser is responsible for producing and organizing ad messaging and other creative products. Advertisers engage in auctions for specific keywords, with winning bids resulting in display of a search ad within search results.	• Cookies • Web Beacons • Entity Tags	Likely to be considered a controller because it determines the information to be used for the auction. Article 5 (VI).	**CCPA:** Likely to be considered a business. Section 1798.140 (c). **CPRA:** Likely to be considered a business. Section 1798.140 (d).	Likely to be considered a personal information handler because it determines the information to be used for the auction.	Will be considered a controller to the extent that it determines the purposes and/or means of processing of the relevant personal data, e.g., disclosure of personal data for analytics purposes by the search engine back to the advertiser. Depending on the extent to which the advertiser and search advertising network jointly determine the purposes and means of processing of personal data, it could be a joint controller with the search advertising network.	Controller as it determines the purpose and means of processing data. If advertiser and search engine collaborate on making the determination of what to process, it will be a joint controller. §§ 59.1-571, 574, 575.
Search Advertising Networks	Search engines conduct auctions to sell ad space according to bids received for specific keywords and relative relevance of user keywords to ads in the inventory.		Likely to be considered a controller if it determines the information required for the auction process directly with the data subject, or a processor if it follows directions exclusively from the Advertiser. Article 5 (VI).	**CCPA:** Likely to be considered a business. Section 1798.140 (c). **CPRA:** Likely to be considered a business. Section 1798.140 (d).	Likely to be considered a personal information handler because it determines the information to be used for the auction.	Will be considered a controller as it determines the purposes and means of processing data about its users. Likely also to be considered a controller of personal data contained in third party web pages included within search results. Depending on the extent to which the search advertising network and an advertiser/	Controller as it determines the purpose and means of processing data. If both players collaborate on making the determination of what to process, it will be a joint controller. §§ 59.1-571, 574, 575.

						website publisher jointly determine the purposes and means of processing, it could be a joint controller with the advertiser and/or the website publisher.	

** For all players presented as processors, the designation may change if the data subject contracts directly with the player.

Native Advertising Ecosystem

Player	Player's Role	Tracking Technologies ** Used Include *broadly referred to as cookies*	Brazil's LGPD Position and Reason for Designation**	California's CCPA | CPRA Position and Reason for Designation	China's Draft PIPL Position and Reason for Designation	European Union's GDPR | ePrivacy Directive Position and Reason for Designation	Virginia's Consumer Data Protection Act Position and Reason for Designation
Advertiser	An entity that purchases inventory for the presentation of messaging to users. An advertiser is responsible for producing and organizing ad messaging, images, articles, videos, and other creative products.	• Cookies • Web Beacons • Embedded Script • Entity Tags • Unique Device Token • Deterministic Fingerprinting Technologies • Probabilistic Fingerprinting • Device Graphs	Controller to ad agency, DSP, and ad exchange as it makes the decisions regarding the processing of personal data. Article 5 (VI).	**CCPA:** Considered a business with respect to first party data collected. Typically, not in privity with the demand side platform or ad exchange on the supply side and would be considered a third party with these players. Section 1798.140 (c). **CPRA:** Same reasoning as CCPA, except CPRA excludes cross-context advertising. If the advertiser uses third party information, then it must be considered a third party. Under Section 1780.140(d)(4)(E)(6), the updated definition of business purpose explicitly states	Personal information handler to DSP, ad exchange, and DMP, as the advertiser independently determines the means of processing personal data. Articles 4 and 9.	Controller to ad agency, demand side platforms, and data management platform as these players usually process personal data on behalf of the advertiser (albeit these players may also be controllers in their own right for other processing operations). Article 4(7), Article 4(8) and Article 24. Depending on the relationship and the extent to which an ad agency, demand side platform or data management platform is involved in determining the purposes and means of processing in conjunction with the advertiser, the advertiser may be considered to be	Controller to ad agency, DSP, and DMP, provided these players process personal data at advertiser's direction. §§ 59.1-571, 574.

				cross-context behavioral advertising is not considered a "business purpose."		a joint controller with one or more of these other parties. Article 26.	
Data Analytics Company (DAC)/ Technology Vendor	Entity that measures how users engage with specific content.		Likely to be considered processor but if it offers other services or uses consumer data for its own purposes, it could be a controller. Article 39.	**CCPA:** Depending on contract language, DACs can be considered "service providers" under Section 1798.140(v) to the advertiser, provided the DAC does not use the data for its own commercial purposes. However, most DACs also provide other services that may exchange data, which would make them a third party. Individual uses of DACs should be scrutinized in each vendor contract to ensure whether (or not) any specific DAC provider is in fact a service provider. Note that consumer advocacy groups such as Californians for Consumer Privacy consider these entities to be third parties, for which a Do Not Sell My Personal Information link is necessary. **CPRA:** DACs could be service providers, contractors, or third parties.	Entrusted party as it receives and uses data from other players and in accordance with those players' specifications. If the DAC offers other services, then it may be considered a third party. Articles 22 and 24.	Generally considered processors but may be joint controllers with other service providers. If the DAC uses consumer data for its own purposes or if it offers integrations with other entities that may exchange data, it may be considered a controller or a joint controller. Article 4(7), Article 4(8), Article 24, Article 26, Article 28.	Likely to be considered a processor but if it uses personal data for its own purpose or offers other services, it could be a controller. Depends on agreement. §§ 59.1-571, 574, 575.

				More information will be provided in upcoming regulations.			
Ad Server	The entity responsible for facilitating the presentation of an ad on a website or app.		Depends on the data processing activity. When the ad server determines what information to collect and process, it acts in the role of a controller. When it relies on information provided by publisher or other players, it is a processor. Article 5 (VI and VII).	**CCPA:** Depending on the data-handling activities at issue, ad servers could be service providers under the CCPA. **CPRA:** Depending on the data-handling activities at issue, ad servers could be service providers.	Depending on the data-handling activities, it can be considered a personal information handler or entrusted, under Articles 4 and 22. If the ad server acts according to an agreement, it is an entrusted party. If the ad server determines what data to process, it is a personal information handler.	Processor to publishers because they utilize information provided by publisher. Could be a controller or joint controller based on its role in determining the purposes and means of processing (which should be reflected in the contract terms). Articles 4(7), 4(8), 24 and 28.	Depends on personal data processing. If it uses information provided by publisher and according to contract, it is a processor. May be a controller if it determines what information to collect and process. §§ 59.1-571, 574, 575.
Publisher	The entity that provides advertising space on a website or app. Publishers work with brands and agencies to create content that fits their criteria.		Controller to ad exchange, and DMP as these players process information provided by the publisher for its benefit. Article 5(VI).	**CCPA:** Considered a business with respect to first party data collected. Typically, not in privity with the ad exchange and would be considered its third party. Section 1798.140 (c). **CPRA:** Considered a business with respect to first party data. Section 1798.140 (d).	Personal information handler to SSP, ad exchange, and DMP, as the publisher independently determines the means of processing personal data. Article 4 and Article 9.	Controller to SSP, ad exchange, and DMP as these players process information on behalf of the publisher (although may be a joint controller with any of these entities depending on their role in determining the purposes and means of processing), Article 4(7), Article 4(8), Article 28, Article 24 and Article 26.	Controller to SSP, ad exchange, and DMP provided these players process personal data at publisher's direction. §§ 59.1-571, 574.

				More information will be provided in upcoming regulations.			
Ad Server	The entity responsible for facilitating the presentation of an ad on a website or app.		Depends on the data processing activity. When the ad server determines what information to collect and process, it acts in the role of a controller. When it relies on information provided by publisher or other players, it is a processor. Article 5 (VI and VII).	**CCPA:** Depending on the data-handling activities at issue, ad servers could be service providers under the CCPA. **CPRA:** Depending on the data-handling activities at issue, ad servers could be service providers.	Depending on the data-handling activities, it can be considered a personal information handler or entrusted, under Articles 4 and 22. If the ad server acts according to an agreement, it is an entrusted party. If the ad server determines what data to process, it is a personal information handler.	Processor to publishers because they utilize information provided by publisher. Could be a controller or joint controller based on its role in determining the purposes and means of processing (which should be reflected in the contract terms). Articles 4(7), 4(8), 24 and 28.	Depends on personal data processing. If it uses information provided by publisher and according to contract, it is a processor. May be a controller if it determines what information to collect and process. §§ 59.1-571, 574, 575.
Publisher	The entity that provides advertising space on a website or app. Publishers work with brands and agencies to create content that fits their criteria.		Controller to ad exchange, and DMP as these players process information provided by the publisher for its benefit. Article 5(VI).	**CCPA:** Considered a business with respect to first party data collected. Typically, not in privity with the ad exchange and would be considered its third party. Section 1798.140 (c). **CPRA:** Considered a business with respect to first party data. Section 1798.140 (d).	Personal information handler to SSP, ad exchange, and DMP, as the publisher independently determines the means of processing personal data. Article 4 and Article 9.	Controller to SSP, ad exchange, and DMP as these players process information on behalf of the publisher (although may be a joint controller with any of these entities depending on their role in determining the purposes and means of processing), Article 4(7), Article 4(8), Article 28, Article 24 and Article 26.	Controller to SSP, ad exchange, and DMP provided these players process personal data at publisher's direction. §§ 59.1-571, 574.

** For all players presented as processors, the designation may change if the data subject contracts directly with the player.

Now What?

Once an individual or entity is able to identify their designation under a country's data protection law, it is important to understand the duties associated with each role. The chart below provides guidance.

Brazil's LGPD			California's CCPA | CPRA* *specific to just CPRA			China's Draft PIPL			European Union's GDPR | ePrivacy Directive			Virginia's Consumer Data Protection Act		
Party	**Definition**	**Duties**	**Party**	**Definition**	**Duties**	**Party**	**Definition**	**Duties**	**Party**	**Definition**	**Duties**	**Party**	**Definition**	**Duties**
Controller	Natural person or legal entity in charge of making decisions regarding personal data processing (Art. 5 (VI))	• Must keep records of its personal data processing operations, especially when based on legitimate interest. (Art. 37) • National authority may require controller to conduct data protection impact assessments (Art. 38) • Records must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards, and mechanisms of risk mitigation • Must appoint a Data Protection Officer (Article 41)	Business	**CCPA:** A for-profit entity that collects consumers' personal information, determines the purposes and means of the processing of consumers' personal information, does business in the state of California and meets any of the following: o Has a gross annual revenue of over $25 million; o Buys, receives, or sells personal information of 50,000 or more California residents, households, or devices; or o Derives 50% or more of their annual revenue from selling California residents' personal information. 1798.140(c) **CPRA:** Same as CCPA but threshold requirements include: • Annual revenue exceeding $25 million in the preceding year • Buys, sells, or shares PI of 100,000 or more California consumers or households • Derives 50% or more of their annual revenue from selling or sharing consumers' PI 1798.140(d)	• Inform consumers of how they collect and use PI and how they can exercise their rights and choices • Collect consumers PI only to extent necessary for its purpose • Provide consumers with easily accessible means to exercise rights • Take reasonable precautions to protect consumer's PI from a security breach	Personal Information Handler (PIH)	Party that decides the purpose of personal information handling and the handling method (Art. 21) Personal information handling includes personal information collection, storage, use, processing, transmission, provision, publishing, and other such activities. (Art. 4)	• Adopt the necessary measures to ensure personal information handling conforms to the provisions of laws and administrative regulations (Art. 50) • Prevent unauthorized access as well as personal information leaks or theft, distortion, or deletion (Art. 50) • PIH who handle personal information reaching quantities provided by the state shall appoint persons responsible for personal information protection (Art. 51) o These persons are responsible for supervising personal information handling activities and adopted protection measures • PIH located outside of China must appoint a dedicated entity or representative in China. (Art. 52) • Conduct regular audits of personal information handling operations, protective measures, etc., to ensure compliance with laws and administrative regulations. (Art. 53) • Conduct risk assessments before five specified activities. Reports must be maintained for three years (Art. 54)	Controller	Natural or legal person, public authority, agency, or other body which determines the purposes and means of the processing of personal data (Art. 4(7) GDPR).	• Implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR (Art. 24) • Ensure an appropriate legal basis to process personal data and ensure transparency, for example via a privacy notice, in relation to such processing (Art. 6, Art. 13, Art. 14) • Ensure the integrity and confidentiality of personal data, notify personal data breaches where required, use only processors that provide sufficient guarantees to implement appropriate technical and organizational measures and ensure that such processors are subject to certain prescribed terms via a contract or other legal act (Art. 5, Art. 28, Art. 32, Art. 33 and Art. 34) • Shall maintain a record of processing activities under its responsibility (Art. 30) • Where a process uses new technologies and is likely to result in a high risk to the rights and freedoms of natural persons, before processing the controller must conduct a data protection impact	Controller	Natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data (§ 59.1-571)	• Limit personal data collection to what is adequate, relevant, and reasonably necessary in relation to the disclosed purpose, and collection must be with the consumer's consent • Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data • Obtain consumer's affirmative consent before processing sensitive data • Must have a privacy policy that includes: o Categories of personal data processed o Purpose of processing o How consumers can exercise their rights, including appeal procedures o Categories of personal data shared with third parties o Categories of third parties with whom it shares personal data **Note:** if personal data is sold to third parties for targeted advertising, controller must conspicuously disclose the processing and opt-out process § 59.1-574. • Must conduct data protection

											assessment (Art. 35) • Designate a data protection officer in certain circumstances (which are likely to apply if the core activity involves the regular and systematic monitoring of the behavior of individuals on a large scale) (Art. 37) • Retain personal data for no longer than is necessary for the purposes for which personal data are processed (Art. 5) • Ensure data protection by design and by default (Art. 25) • N.B. To the extent that two or more ad tech stakeholders act as joint controllers, there must be an "arrangement" between them which sets out their respective responsibilities for compliance with the GDPR (Art. 26)			assessment for the following activities (§ 59.1-576.): o Processing personal data for targeted advertising purposes o Processing personal data for profiling o Processing sensitive data o Any processing that presents a heightened risk of harm to consumers • Must identify and weigh benefits against risks

Processor	Natural person or legal entity of either public or private law that processes personal data in the name of the controller (Art. 5(VII))	• Must keep records of its personal data processing operations, especially when based on legitimate interest (Art. 37) • Carry out the processing according to the instructions provided by the controller (Art. 39)	**Service Provider**	**CCPA:** A for-profit entity that processes information on behalf of a business and to which the business discloses a consumer's PI for a business purpose pursuant to a written contract. 1798.140(v) **CPRA:** person that processes PI on behalf of a business and which receives from or on behalf of the business a consumer's PI for a business purpose pursuant to a written contract. 1798.140(ag)	**CCPA:** process information on behalf of a business **CPRA:** • Process personal information on behalf of a business 1798.140(ag)(1) • Must notify business if it engages another person to assist in processing PI on behalf of the business and the engagement must be pursuant to a written contract that binds this party to the same requirements as the service provider (1798.140 (ag)(2)) • In addition, a business that discloses PI to a service provider for a business purpose must enter into an agreement with the service provider that includes the following: o Specifies that the PI is sold or disclosed by the business only for limited and specified purposes; o Obligates the service provider to comply with applicable obligations under the CPRA and obligate those persons to provide the same level of privacy protection as is required by this title; o Grants the business rights to take reasonable and appropriate steps to help to ensure that the service provider uses the PI transferred in a manner consistent with the business's obligations under the CPRA;	**Entrusted Party**	Party entrusted by PIH to handle personal information (Art. 22)	• Must handle personal information according to the agreement (Art. 22) • May not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement (Art. 22) • After the contract is fulfilled and completed or the entrusting relationship dissolved, entrusted party must return personal information to the personal information handler or delete it. (Art. 22) • Must receive consent of PIH to further entrust personal information handling to other persons. (Art. 22)	**Processor**	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4(8) of the GDPR).	• Must receive prior specific or general written authorization of the controller before engaging another processor • Must be governed by a binding contract or other legal act that sets out, amongst other matters: o The subject-matter and duration of the processing o The nature and purpose of the processing o The type of personal data and categories of data subjects, and o The obligations and rights of the controller (Art. 28) • Must designate a data protection officer in certain circumstances (which are likely to apply if the core activity involves the regular and systematic monitoring of the behavior of individuals on a large scale) (Art.37) • Maintain a record of the processing activities it carries out on behalf of a controller (Art 30). • Implement appropriate technical and organizational measures to ensure a level of security that is appropriate to the risk (Art 32) and report personal data breaches to the controller without undue delay (Art 33(2)).	**Processor**	A natural or legal entity that processes personal data on behalf of a controller (§ 59.1-571)	• Must have a binding contract with controller that details the instructions for processing data, its nature and purpose, type of data processed, duration, and parties' rights and obligations. Contracts must meet the following conditions: o Every person processing must be subject to duty of confidentiality o At controller's direction, processor must delete or return all personal data requested at the conclusion of contract, unless retention is required by law o Contract must provide controller with information to show processor's compliance with its obligations o Contract must allow and cooperate with assessments of processor's policies and technical and organizational measures o Any subcontractor must comply with processor's obligations • Shall assist controller by utilizing appropriate technical and organizational measures to hold respond to consumer rights requests • Shall securely process personal data and assist controller with breach notification obligations • Shall provide controller with information to conduct and document data protection assessments § 59.1-575

					o Requires the service provider to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA o Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use PI 1798.100(d)									
			Third Party	**CCPA:** A person who is not any of the following: • The business that collects PI from consumers • A person to whom the business discloses a consumer's PI for a business purpose pursuant to a written contract 1798.140(w) **CPRA:** A person who is not any of the following: • The business with whom the consumer intentionally interacts and that collects PI as part of the consumer's current interaction • A service provider • A contractor 1798.140(ai)	**CCPA:** • Unlike service providers, third parties are not restricted in how they must handle PI. However, it is best practice to include contractual provisions with the third party regarding data-handling. **CPRA:** A business that sells or shares PI with a third party must enter into an agreement with the third party that does the following: • Specifies that the PI is sold or disclosed by the business only for limited and specified purposes • Obligates the third party to comply with applicable obligations under the CPRA and obligate those persons to provide the same level of privacy protection as is required by this title • Grants the business rights to take reasonable and appropriate steps to help to ensure that the third party uses the PI transferred in a manner consistent with the									

					business's obligations under the CPRA • Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use PI 1798.100(d)									
			Contractor*	**CCPA:** Not applicable **CPRA:** A person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract 1798.140(j)	**CCPA:** Not applicable **CPRA:** • Must have a written contact with the business • Prohibited from o Selling or sharing PI o Retaining, using, or disclosing PI for any purpose outside written contract o Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and business o Combining PI received under written contract with PI it received from other persons or collected on its own									

Acknowledgements:

Thank you to Xinlan Liu, Senior Legal Consultant at Perkins Coie and Christy Harris, Director of Technology at the Future of Privacy Forum for their invaluable contributions to this article.

OneTrust

PRIVACY, SECURITY & GOVERNANCE

About OneTrust

OneTrust is the #1 fastest-growing company on Inc. 500 and the category-defining enterprise platform to operationalize trust. More than 8,000 customers, including half of the Fortune 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 140 patents and powered by the OneTrust Athena™ AI and robotic automation engine. Our offerings include OneTrust Privacy Management Software, OneTrust DataDiscovery™ AI-powered discovery and classification, OneTrust DataGovernance™ data intelligence software, OneTrust Vendorpedia™ third-party risk exchange, OneTrust GRC integrated risk management, OneTrust Ethics ethics and compliance software, OneTrust PreferenceChoice™ consent and preference management, OneTrust ESG environmental, social and governance software, and OneTrust DataGuidance™ regulatory research.

According to the IDC Worldwide Data Privacy Management Software Market Shares Report, 2019, "OneTrust is leading the market outright and showing no signs of slowing down or stopping." In December 2020, OneTrust raised a $300 million Series C funding from TCV, Insight Partners, and Coatue, bringing total funds raised to $710 million at a $5.1 billion valuation.

OneTrust's fast-growing team of 1,500 employees is co-headquartered in Atlanta and London with additional offices in Bangalore, Melbourne, Seattle, San Francisco, New York, São Paulo, Munich, Paris, Hong Kong, and Bangkok.

To learn more, visit OneTrust.com