PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

presents

Inaugural Annual Privacy Law Summit

Session 3

AdTech For Privacy Lawyers

MCLE: 1.0 Hours

Thursday, February 9, 2023

2:00 p.m. – 3:00 p.m.

Speakers:

Daniel M. Goldberg, Chair, Privacy & Data Security Group
Frankfurt Kurnit Klein & Selz
Tyler Finn, Privacy, Tech Policy & Data Strategy Leader
Todd Ruback, Managing Director, Privacy, FTI Consulting

Conference Reference Materials

Friday I'm Reading CPRA (Again)

By: Daniel Goldberg

For the second week in a row, the CPPA has dropped a bombshell on a Friday afternoon. Last week, the CPPA released a 66 page first draft of its Proposed Regs to CPRA (you can read our initial analysis here) and announced that it will be holding a public meeting on June 8, 2022. This afternoon, the CPPA released a CPRA FAQ along with another 66 page document – an Initial Statement of Reasons (ISR) that provides further insight into the Regs. We quickly reviewed the FAQ and ISR, and have provided thoughts below on what these documents add to our analysis from last week. If you haven't read our prior analysis, check it out first.

Public Comment Period Is Imminent: The FAQ states that the 45 day public comment period starts when the CPPA files and posts a Notice of Proposed Rulemaking Action (NOPA), the Regs, and the ISR. We have the Regs and the ISR, and a public meeting is scheduled for June 8th. Get your pens and keyboards ready for public comments.

Intent to Harmonize: The introduction to the ISR states that the CPPA took into consideration GDPR and other state privacy laws when crafting the Regs, and that the Regs will help simplify compliance for business and unnecessary confusion for consumers. After spending time with Regs over the past week, I disagree that the Regs will have this impact. The Regs, as written, impose highly technical contractual and disclosure obligations that differ fundamentally from other privacy laws and will confuse businesses and consumers. I hope the CPPA will reduce many of these technical requirements in the next round, or clarify that meeting GDPR standards for a DPA will suffice.

Broad Opt-in Consent Obligations: The ISR doubles down on language in the Regs that a business must obtain explicit consent in order to process personal information in a manner inconsistent with consumer expectation. Per the ISR, in such instances, a business must obtain explicit consent regardless of how it gives notice. The Regs provide examples of sales or shares as not fitting within consumer expectation. This position seems to flip Do Not Sell or Share (DNS) from an opt-out to an opt-in regime, and threatens many business models. I expect industry to push back significantly.

Do Not Sell or Share (DNS):

- **Global Privacy Control (GPC) Lives**: While GPC doesn't appear in the Regs, the ISR references GPC as a technical mechanism for opt-out signals. The ISR also states that a business is not required to process requests that are in an unusable or unfamiliar format. I anticipate significant confusion around which

signals must be recognized, and it would be preferable for the Regs to expressly name GPC as the universal recognized mechanism.

- **Opt-Out Preference Signals Can Be On By Default:** One concern I mentioned in my original post is that, unlike Connecticut, the Regs do not expressly restrict a platform or browser from setting an opt-out preference signal on by default, which effectively would make DNS opt-in. The ISR goes further in the wrong direction, stating that a consumer's selection of a privacy-by-design product is an affirmative step sufficient to express the consumer's intent to opt-out. What qualifies as a privacy-by-design product? If a global technology company advertises its browser or operating system as privacy safe, does that qualify? This could result in antitrust issues.
- **Opt-Out Preference Signals Not Required for LUDSPI**: The ISR clarifies that the Regs only require companies to address opt-out preference signals for sales or sharing. The Regs do not require companies to address signals for limiting the use of sensitive personal information or specific opt-in for minors 13 to 15 or parents or guardians of minors.
-

Automated Decisionmaking: As previously discussed, the CPPA is releasing the Regs in two packages. The second package (not yet released) will address automated decisionmaking. The ISR notes that the CPPA changed certain terms in the Regs to reduce confusion between DNS opt outs and automated decisionmaking opt outs. Expect automated decisionmaking opt outs to be a big part of the second package.

Financial Incentives

- **Valuing Data**. While the Regs didn't change much around financial incentives at first glance, the ISR states that the CPPA's edits were intended to clarify that only certain financial incentives require a business to provide a valuation of data. Financial incentives where there is a price or service difference require a valuation of data while financial incentives that involve a monetary or specific benefit (such as a free shirt or gift card) do not require a valuation. This is a helpful clarification.
- **Discriminatory Practices.** The ISR explains that financial incentives and discriminatory practices have been moved to separate sections because the two

often get mixed up. Per the ISR, financial incentives do not inherently invoke a discrimination analysis because there is a separate negotiation taking place for a specific incentive. Again, this is a welcome explanation.

Naming Third Parties. The Regs require a business that allows a third party to control the collection of personal information to include the name of the third party in its notice or information about the third party's business practices. Upon first reading the Regs, I wasn't clear if the second option means a business needs to expressly incorporate a third party's privacy policy into its own privacy policy or if a business could more generally disclose information about the third party's business practices. The ISR clarifies that the CPPA considered requiring the express disclosure of names as the only option, but decided against that requirement. Based on this new information, I interpret the provision to mean that disclosures around a third party's business practices can be more general in nature.

Probable Cause and Administration Hearing Process. Since the Regs were released, I've seen various posts voicing concern that the CPPA's probable cause determination is not subject to appeal. The ISR clarifies that the probable cause determination precedes an administrative hearing. Based on my reading, the CPPA must first consider whether it has probable cause to bring an administrative hearing, and it can only bring an administrative hearing once it determines there is probable cause. While the probable cause determination is not subject to appeal, I don't see any indication that the administrative hearing itself is not subject to appeal.

Immediate Thoughts on the Newly Proposed CPRA Regs

By: Daniel M. Goldberg and Maria Nava
Published: May 28, 2022

Happy Friday before a holiday weekend! This afternoon the California Privacy Protection Agency (CPPA) issued a notice that it will be holding a public meeting on June 8, 2022. Hidden within that notice was a link to meeting materials that contains the first draft of the CPPA's Proposed Regs to CPRA. We quickly reviewed the Regs (so you don't have to before the holiday weekend), and have provided our immediate thoughts below:

- **Only Part of the Story**. Earlier this week, the CPPA clarified that it is releasing the Regs in two packages. This appears to be the first package. The second package (which has not yet been released), is set to cover cybersecurity audits, privacy risk assessments, and automated decision making.
- **Not Final.** To be clear, these are only the Proposed Regs. They must still go through the rulemaking process, so we expect them to change considerably.
- **Much of the Same.** The Regs are essentially a revised version of the California Attorney General's CCPA Regs. While there are a lot of redlines, a lot has stayed the same. For example, little has changed regarding verification, authorized agents, children/minors, non-discrimination/financial incentives, training, and record keeping. We are a particularly surprised by lack of changes to financial incentives and children/minors.
- **Codifying CPRA Obligations.** The Regs dedicate a lot of space to codifying express CPRA obligations. For example, the Regs add language around the right to correct, the right to limit the use and disclosure of sensitive personal information (LUDSPI), and the obligation of a business to notify its service providers or contractors to delete personal information.
- **Investigation and Enforcement.** As promised by the CPPA, the Regs add language around investigation and enforcement, including relating to audits. This information is pretty high level, and, at least upon first review, doesn't provide much insight into the process.
- **Lots of Examples.** One thing we appreciate is that the Regs provide many examples. This gives us better insight into what the CPPA is thinking with respect to enforcement.

- **What's a Contractor?** The Regs don't clarify what constitutes a contractor versus a service provider. We still don't understand why we needed this fourth term.
- **Many New Obligations.** Let's get to the good stuff. You're here to see what the Regs added with respect to CPRA requirements. There's a lot, and we are still digesting everything. Below are some additions that jumped out at us:

DNS:

- **Opt-Out Signals Are Mandatory.** As expected, the Regs clarify that businesses must recognize Do Not Sell or Share (DNS) opt-out preference signals. While some privacy professionals have argued that businesses have a choice between posting a DNS link or honoring an opt-out preference signal, the Regs expressly state that interpretation is incorrect.
- **No Clarification About Which Signals Qualify.** Unfortunately, the Regs fail to clarify what constitutes a valid opt-out signal. They didn't even formally recognize GPC as the de facto signal. As written, businesses arguably must respond to any signal, which will create compliance hurdles. Further, unlike Connecticut, the Regs don't state that an opt-out signal cannot be set to "on" by default by a browser.
- **Opt-Out Status.** The Regs state that a business should display through an icon on its website whether or not it has processed an opt-out signal. Interestingly, this is a suggestion rather than a requirement.
- **Frictionless Opt-Out.** There is a new concept of a "frictionless" opt-out. Where a business only sells or shares information that meets the frictionless standard and the business responds to opt-out signals, the business is not required to include a DNS button on its site. However, most businesses will not qualify for this exception as the business must be able to facilitate an opt-out without requiring any further information from the consumer. This means the exception essentially only applies to businesses that use tracking technologies (like cookies or pixels) for cross-contextual advertising, and not those that also upload data files (like hashed audiences for matched audiences) or sell data offline.

- **Opt-Outs Downstream.** Per the Regs, where a person receives an opt out request, not only do they need to stop selling or sharing personal information, but they must also notify any third parties downstream to stop selling or sharing the information. This appears to be a higher burden than currently required under CCPA or the CPRA text, and reemphasizes the need for a signal that can be read by downstream parties. Contracts with third parties must also expressly require the third party to check for opt-out signals.
- **Cookie Banners are Not Sufficient.** The Regs find that a cookie banner is not itself sufficient to meet DNS obligations. This is a good clarification as too many companies still rely on cookie banners alone.
- **Your California Privacy Choices.** The Regs allow for a combined opt-out link for DNS and LUDSPI called "Your California Privacy Choice." We appreciate the homage to older California privacy law.

Contracts:

- **Not Qualifying as a Service Provider.** The Regs state that a person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor. The Regs provide an example that non-personalized advertising based on aggregated or demographic information is okay, but using a customer list to identify users and serve them ads is not okay. This example appears to be aimed at certain social media platforms, and positions they have taken around matched audiences.
- **Third Party to Service Provider.** While matched audiences may not have received favorable treatment, there is some good news in general for the advertising industry. For the first time, the Regs recognize that a third party can become a service provider after receiving an opt-out request if the third party complies with the obligations of a service provider. This supports the position of the advertising industry, in particular the Limited Service Provider Agreement (LSPA) issued by IAB, where a signatory third party becomes a limited service provider upon receiving an opt out.

- **Losing Protections of a Service Provider.** Per the Regs, a person who does not have a contract that complies with the Regs is not a service provider or a contractor under the CCPA. While we've known this for a while, the express statement reemphasizes the importance of including the relevant language in your contracts. Also, the Regs provide that if a person doesn't conduct due diligence, and it turns out the recipient violated the law, the person may not be protected under the law even if the contract technically met CPRA contractual requirements. Do your due diligence!
- **Specifying Services in Contracts.** The Regs require a contract between a business and a service provider, contractor, or third party to expressly identify the specific service for which the recipient processes information. This brings CPRA contractual requirements closer in line to GDPR and other comprehensive state privacy laws which require a controller to set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.

Consumer Requests:

- **Access Requests Beyond 12 Months.** Under the Regs, when a business receive an access request, it must by default provide the consumer all their personal information dating back to January 1, 2022. This contradicts the CPRA text where a business is only required to provide personal from the prior 12 months unless otherwise expressly requested by the consumer.
- **Retaining Corrections.** For a correction request, where a business receives a correction request and subsequently receives outdated personal information, the business has an obligation to retain the correction and not use outdated personal information.

Disclosures and Consent:

- **Consent for Incompatible Purposes.** Where a business processes information for a purpose incompatible with the original collection, it must obtain consent for the new purpose.
- **Dark Patterns**. The Regs state that a business cannot make it tougher to exercise consumer rights than to not exercise them. The Regs then provide a list of examples of what not to do, which is quite helpful. Any failure to comply will be considered a dark pattern.
- **Third Party Obligations.** The Regs include language regarding third parties that control the collection of personal information, and obligations for providing notice. This appears to be similar to the concept of a controller to controller relationship, although the obligations are not quite as robust.

That’s it for now. As we learn more, we will be sure to keep you informed.

Privacy Considerations for 2023

By: Maria Nava

2023 is around the corner. As a refresher, on January 1, 2023, two new comprehensive privacy laws – the California Privacy Rights Act ("CPRA") and the Virginia Consumer Data Protection Act ("VCDPA") – take effect. Although businesses should be well on their way to compliance, we have compiled some last minute tips in this alert for your consideration before the year's end.

- **Update Your Privacy Policy**. Businesses should review and update their privacy policies to address new disclosure obligations. For example, CPRA requires disclosures regarding sales *and* shares of personal information, and details regarding the new right for consumers to correct their personal information. Virginia requires disclosures around the process for submitting data subject requests (including an explanation of the controller's appeal process) and the contact details for the Virginia Attorney General.

- **Address Data Subject Requests.** In connection with addressing new disclosure requirements, businesses should ensure they have tools to address new data subject rights. As mentioned above, California has added new rights to correct and opt-out of the sharing of personal information (the California Consumer Privacy Act ("CCPA"), which the CPRA replaces, already included the rights to know, access, delete, and opt-out of the sale of personal information). Virginia now grants its data subjects the rights to: (a) access, correct, and delete their personal data; and (b) opt-out of the processing of personal data for sales, targeted advertising, and certain types of profiling.

- **Respond to Preference Signals**. Businesses should implement measures to honor Do Not Sell or Share opt-out preference signals, particularly relating to Global Privacy Control ("GPC"). In August, the California AG brought the first public action under CCPA (which we blogged about) against a business for alleged failure to process Do Not Sell requests via GPC. Characterizing GPC as

a “game changer,” Attorney General Bonta has left little doubt that GPC compliance is now a requirement under California law.

- **Conduct Data Protection Impact Assessments**. Business should have a form ready and begin conducting data protection impact assessments as required by Virginia. Taking a page from GDPR, starting in January, Virginia will require controllers to assess their data practices involving certain processing operations. For example, a controller must conduct a data protection impact assessment where personal data is processed for targeted advertising or an activity that creates a “heightened risk of harm” to data subjects.

- **Revise Contracts.** Businesses should review and update their contracts (including data processing addendums) to ensure they contain language required by CPRA and VCDPA. For purposes of Virginia, a data processing addendum that complies with GDPR may be sufficient, as long as it incorporates personal data subject to Virginia. However, CPRA requires very specific language that differs from both CCPA and Virginia, and likely involves more comprehensive revisions.

- **Evaluate Sensitive Personal Information.** Businesses should evaluate whether they process any sensitive personal information, which is a new category of data under California and Virginia law. Sensitive personal information includes Social Security Number, precise geolocation, health data, genetic data, and more. Both laws require specific disclosures around sensitive personal information. In addition, under Virginia, processing of sensitive personal data is opt-in, while under California, processing of sensitive personal information is opt-out under certain circumstances.

Takeaways from the California AG's $1.2 Million CCPA Enforcement Action

By: Daniel M. Goldberg

In late August, the California AG announced its first public enforcement action and settlement for alleged violations of CCPA as well as updated its website to include new enforcement case examples. In light of these developments, here are some key takeaways for your business:

Noncompliance is Expensive. The settlement provides the first true insight into the costs of noncompliance. The settlement includes a monetary penalty of $1.2 million. In addition, the settlement requires remediation of noncompliance, implementation and maintenance of a program for two years to ensure effective processing of opt-out requests, internal reviews for two years of tracking technologies and contracts, and annual reporting to the AG.

Take Advantage of the Notice to Cure. While it may seem that there has been a lack of enforcement action for violations of CCPA, that actually isn't true. CCPA provides a 30 day right to cure, and the AG has issued numerous notices to cure over the past two years. Prior to this enforcement action, all alleged violations had been handled behind closed doors, and the AG had posted enforcement case examples without listing names. This enforcement action is the first time a business allegedly did not address the AG's notice to cure. If your business receives a notice from the AG regarding alleged CCPA violations, address it promptly.

The Window to Cure is Ending. The CCPA's 30 day right to cure ends once CPRA takes effect in January 2023. Under CPRA, notice to cure is discretionary. Further, the AG has stated that not all CCPA violations are curable. Accordingly, expect to see many public enforcement actions and settlements for alleged violations of CCPA in the near future. Do not build your business's CCPA compliance relying on a right to cure.

Targeted Advertising is a Sale. Once again, the AG has made clear that it considers targeted advertising to be a "sale" under CCPA and to require an opt-out. The AG brought the enforcement action based on alleged use of tracking technologies on a website without addressing sale obligations under CCPA. If your business engages in targeted advertising, you need to address sale obligations.

Sales Require Notice and Opt-Out. Under CCPA, where a business sells personal information, it must state so in its privacy policy and provide a readily accessible Do Not Sell My Personal Information link in the footer of its website/app. According to the AG, the business in the enforcement action did neither, and stated it does not sell personal information. Stating you don't sell personal information and not providing an opt-out are low hanging fruit for the AG. If your business engages in targeted advertising, you need to provide appropriate notice in your privacy policy as well as an opt-out mechanism.

Responding to Do Not Sell Signals is Mandatory. This point is controversial. The AG has taken the position that businesses must honor global opt-out signals. That means that where a consumer activates a setting in their browser to opt-out of sales and the consumer visits a business's website, the business must read the signal and automatically treat the signal as a request to opt-out. Per the AG, the AG did a wide sweep of large retail websites to see whether they included tracking technologies, and, if so, tested whether the websites responded to global opt-out signals sent via Global Privacy Control (GPC). This enforcement action (and many of the enforcement case examples) was brought on grounds that the business failed to honor global opt-out signals. Given the AG's focus on global opt-out signals (and the CPRA Regs making honoring signals an express requirement), any businesses that don't honor signals (specifically GPC) should strongly consider changing their practices.

Google Technologies are on the Radar. In the enforcement action, the AG refers to a "widely-available" analytics and advertising service and "restricted data processing" (RDP). RDP is a term used specifically by Google for CCPA opt-outs. It is likely the AG brought enforcement actions against businesses that used Google tracking technologies on their websites. If your business uses any Google tracking technologies, you should carefully review obligations under CCPA.

Review Your Contracts. The AG repeatedly discusses the importance of executing contracts with service providers that meet all the requirements under CCPA. This means drafting contracts with CCPA-specific language, not just stating that each party will comply with applicable privacy law. If a contract requires you as the business to take specific technical measures so the recipient will act as a service provider, you need to take those measures.

Review Your Loyalty Programs. Through the examples, the AG reminds companies yet again they must comply with the financial incentive obligations under CCPA.

Takeaways from the Modified CPRA Regs

By: Daniel M. Goldberg

On October 17th, the CPPA released the modified text of proposed CPRA Regs (modified Regs) and an accompanying explanation of the modified text (EMT). We quickly reviewed the modified Regs and EMT, and have provided thoughts below. For our analysis on the original proposed Regs and accompanying statement of reasons, please visit our prior posts here and here.

Adoption of Regs is Imminent: The CPPA has scheduled public meetings for October 21-22 and October 28-29, where, per the agenda, it will discuss the modified Regs and "possible adoption or modification of the text." Given that CPRA is set to take effect in less than three months, the CPPA is under a lot of pressure to adopt the Regs. Expect (some) finalized Regs by early to mid-November.

Partial Adoption is Possible: While some portions of the Regs are complete, others likely require further modification. The EMT identifies specific sections of the Regs (highlighted in gray and with an asterisk) that the CPPA intends to discuss at the upcoming meetings. Given the pressure to adopt Regs, the CPPA may decide to adopt certain portions of the Regs while further modifying others. This would allow businesses to start working on their compliance with the Regs prior to 2023 and provide the CPPA with additional time to finalize more controversial portions of the Regs. Partial adoption is already a virtual certainty to some extent given that the CPPA has yet to release its second package of Regs set to cover cybersecurity audits, privacy risk assessments, and automated decision making. Note that partial adoption does not guarantee a grace period for CPRA enforcement. We hope to hear about a grace period at the upcoming meetings.

Substantially Similar to the First Draft: Now that we have discussed procedural issues, let's address the elephant in the room. The modified Regs are substantively substantially similar to the first draft. If you loved the first draft, you are going to love this one. But if you found a lot wrong with that draft (see our prior posts), you are still going to find a lot wrong here. For example, the modified Regs still impose highly technical contractual and disclosure obligations that differ fundamentally from other privacy laws and will confuse businesses and consumers. The modified Regs also do not clarify obligations around opt out preference signals, and give platforms huge discretion to make decisions that impact the entire online ecosystem. I am disappointed (but not surprised) that the CPPA did not take this opportunity to better address public comments submitted over the past several months.

What You See is What You Get: Given how little the Regs changed in the last round, the modified Regs are likely a good indicator of what the final version will look like. Businesses should, at a minimum, start addressing the less controversial requirements of the Regs.

What's New: Below are some of the changes we identified in our initial review of the modified Regs:

Non-Substantive Edits. Many, if not most, of the changes to the Regs are non-substantive. The CPPA fixed typos, moved sections, and rephrased language to make the Regs more precise.

Definitions. The modified Regs add and clarify certain definitions, including "Alternative Opt-Out Link," "Disproportionate effort," "Information Practices," "Nonbusiness", and "Unstructured." These definitions place further obligations on businesses.

Reasonably Necessary and Proportionate. Perhaps the biggest change to the Regs comes in Section 7002. Under CPRA, a business's processing of personal information must be (1) reasonably necessary and proportionate to achieve (2) (a) the purposes for which the personal information was collected or processed, or (b) another disclosed purpose that is compatible with the context in which the information was collected. The Regs now dedicate multiple pages and establish three new factor tests to determine compliance with each element above. These factor tests are tied to the concept of the reasonable expectation of the consumer. Any use of personal information that does not meet these factor tests requires consent. I find these factor tests arbitrary and burdensome, and I am concerned that they potentially change CPRA's Do Not Sell opt-out regime into an opt-in regime. The CPPA has designated Section 7002 as a topic of discussion, and I expect there will be push back from industry stakeholders on this language during the meetings.

Listing Third Parties. One good change from a practical perspective is that the modified Regs remove the requirement that businesses identify in their privacy policies the names of third parties that control the collection of personal information. The EMT lists this as an example of where the CPPA tried to simplify implementation.

Opt Outs and Notifying Third Parties. The modified Regs also remove certain obligations around opt outs and notifying third parties. For example, a business is no longer required to notify all third parties to whom the business makes personal information generally available that a consumer has opted out. Also, a business is not required to include language in its contracts for third parties to check for opt out signals. And it is optional for a business to display the status of whether the business has processed an opt out preference signal.

Dark Patterns. The modified Regs add language that may help businesses when claiming they do not engage in dark patterns. There is now a knowledge requirement - businesses are responsible for a nonfunctional email address or broken link if they knew about the issue and did not remedy it. Also, intent for creating dark patterns is a factor - the CPPA may consider intent in determining whether an interface is a dark pattern.

Sensitive Personal Information. The modified Regs add an exception that a business does not need to offer an opt out for sensitive persona information where the business

only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy. This may reduce the need for businesses to provide opt outs for sensitive personal information.

Requests to Delete. The modified Regs clarify that a service provider that offers a self-service deletion option meets the deletion requirement. This is helpful for service providers that enable their clients to delete personal information through a user interface.

Requests to Correct. The modified Regs remove some of the stringent requirements around ensuring personal information remains accurate.
Service Provider Contracts. The modified Regs allow service providers to use personal information for certain internal use or to prevent, detect, or investigate security issues even if the business purpose is not specified in the written contract. I think this is a great addition, and I wish the CPPA had added similar language to more generally address highly technical contractual obligations required by the Regs.

Non-Profits. The modified Regs clarify that an entity that provides services to a Nonbusiness (e.g., non-profit) could be subject to CPRA if it uses the personal information for its own purposes.

Frictionless Opt Out. The modified Regs now state that if a business asks an opted out consumer to opt back in to sales after 12 months, the business cannot rely on the frictionless opt out exception set out by the Regs.

Third Parties. The EMT reaffirms that a person can be a third party in one context and a service provider or contractor in another. This is helpful for ad tech purposes, as discussed in our prior posts.

What's Missing: As noted above, the modified Regs do not cover cybersecurity audits, privacy risk assessments, or automated decision making. That being said, one of the factor tests discussed above incorporates language generally found in privacy risk assessments.

Daniel M. Goldberg

T (310) 579 9616
F (347) 579 9616
dgoldberg@fkks.com

Practice Areas:
Privacy & Data Security
Technology & Digital Media
Advertising, Marketing & Public Relations
Advertising Technology
Branded Entertainment
Interactive Entertainment
Social Media

Daniel M. Goldberg is Chair of the Privacy & Data Security Group, and a leader in Ad Tech. He has been consistently recognized by top legal rating organizations including *Chambers USA* (20202022), *Chambers Global* (2020-2022), *Law360* ("Top Attorneys Under 40" in Cybersecurity & Privacy – 2020), *The Legal 500* (for Cyber Law (including Data Privacy and Data Protection) – 2020-2021), and *Super Lawyers* ("Rising Star" for Southern California – 2020-2022).

Mr. Goldberg counsels clients on all matters involving data – from collection and monetization to storage and security. He helps clients evaluate the legality of their proposed projects and products, develop data protection programs and policies, conduct due diligence on fundraising and acquisitions, and respond to data breaches and regulatory inquiries. He is at the forefront of privacy and data security law, regularly advising clients on the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). He is now preparing clients for the wave of new state privacy laws taking effect in 2023, including the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), and the Utah Consumer Privacy Act (UCPA).

Mr. Goldberg has special expertise in ad tech and technology transactions. He routinely negotiates complex deals on behalf of top agencies, brands, and technology providers involving media buys, programmatic advertising, customer matching, data clean rooms, and data licensing. He helps clients navigate legal concerns around sensitive data (such as geolocation and health data) and emerging technologies (such as facial detection/recognition and NFT/blockchain), and across devices and platforms (such as mobile and social). He also represents many companies in the video game sector, helping them address industry-specific concerns around data processing.

Mr. Goldberg helped lead the effort to publish GALA's "Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising & Marketing." The book is the first-ever guide to how privacy laws affect marketing and advertising around the world.

Mr. Goldberg frequently speaks at conferences and programs, including those sponsored by South by Southwest (SXSW), Social Media Week (SMW), International Association of Privacy Professionals (IAPP), Children's Advertising Review Unit (CARU), Entertainment Software Rating Board (ESRB), Media Law Resource Center (MLRC), Global Advertising Lawyers Alliance (GALA), Interactive Advertising Bureau (IAB), International Advertising Association (IAA), Brand Activation Association (BAA), Association of National Advertisers (ANA), and many others. He routinely guest lectures at top universities, including University of Southern California (USC) and New York University (NYU), and contributes to the Firm's *Advertising Law Updates* blog. He also takes on leadership roles, including as a Vice President on the Board of Directors for IAA, a CCPA Roundtable Co-Leader for IAB, Founding Member and Co-Chair of the MLRC Data Privacy Committee, Founding Member of the Privacy/Cyber Section of the LA County Bar Association (LACBA), former KnowledgeNet Co-Chair for the Los Angeles Chapter of IAPP, and Founding Member and Former Chair of the USC Alumni Entrepreneurs Network.

Prior to joining Frankfurt Kurnit, Mr. Goldberg worked at BakerHostetler and Bryan Cave, where he litigated in federal and state courts. He also helped launch a fintech startup, which was acquired by a multi-national corporation. Mr. Goldberg combines his litigation roots, technical understanding of technology, and insider's perspective on entrepreneurship to deliver cost-effective representation for his clients.

Mr. Goldberg is a graduate of UCLA and USC School of Law. He is certified as an Information Privacy Professional (CIPP/US) and admitted to practice in California.