SQUIRE PATTON BOGGS

2023 State Privacy Laws

How to Assess and Ensure Readiness by Year-end

September 2022

(c) 2022, Squire Patton Boggs. All Rights Reserved. Attorney Advertising. Not intended as legal counsel.

As we head into the fourth quarter, US businesses need to assess the progress they have made in preparing for sweeping changes to the California Consumer Privacy Act (CCPA) that become effective January 1, 2023, as well as for four new state consumer privacy laws (in Colorado, Connecticut, Utah and Virginia) that become effective throughout 2023 (collectively "2023 Privacy Laws"). A comparison of these laws and a set of model workstreams to help you prepare for them is at **Appendix 1** of this alert.

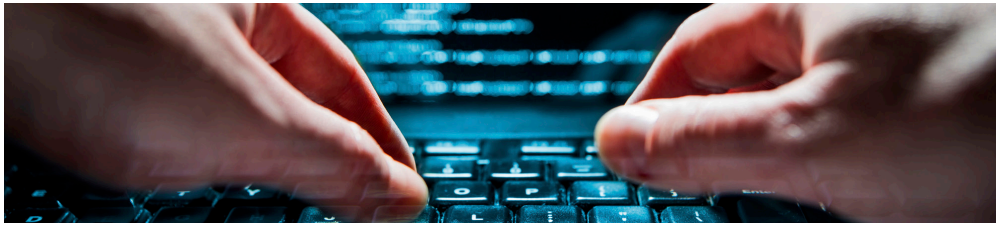
One of the biggest changes next year will bring is that HR and B-to-B communications data, the application of which under California's privacy law was largely delayed until January 1, 2023, will be coming into full scope on that date given the failure of legislative efforts to further extend that deadline. An explanation of these changes and guidance on how to prepare for this is at **Appendix 2** of this alert.

In addition to making privacy program modifications to reflect the changes required by the 2023 Privacy Laws, businesses should take note of recent CCPA enforcement actions, and particularly a recent settlement involving website analytics and advertising cookies, as well as browser privacy choice signals, that includes payment of a US$1.2 million civil penalty. Many, many websites and mobile apps will need to substantially change the way they address cookies and other tracking technologies to avoid similar penalties. In a press release announcing the settlement, the California Attorney General reminded businesses that as of January 1, 2023, the CCPA's current 30-day opportunity to cure violations and avoid civil penalties sunsets, and warned businesses not to hope for discretionary opportunities to cure. A breakdown of this case and other enforcement actions is at **Appendix 3** of this alert.

It remains unclear if we will have final revised regulations reflecting the 2023 changes to the CCPA before the end of the year. However, the California Privacy Protection Agency (CPPA) has closed public comments to its first draft of revised regulations. After it has considered the many comments filed by industry, consumers and public interest organizations, the CPPA may issue a revised set of the proposed regulations, which would start a new comment period. In addition, the CPPA noted that the new rulemaking would stage with tough issues like automated decision-making and machine learning to be addressed in a yet-to-come rulemaking. In the meantime, businesses should be considering the changes they will need to make to the extent the initial draft reg changes become final. An analysis of the current proposed regulatory changes is at **Appendix 4** of this alert.

To help businesses prepare, we have included as appendices to this alert the following guidance materials:

1. Preparing for 2023 State Privacy Laws
2. HR and B-to-B Data: CCPA/CPRA Compliance Primer
3. Lessons from the First CCPA Civil Penalty Case
4. Takeaways from the First Draft of Revised CCPA Regulations



Steps to Take By Year-end

1. Assess readiness and conduct a gap analysis and develop a project plan
2. Update data inventory
3. Revise notices, policies and procedures
4. Refine consumer request program
5. Implement impact assessment program
6. Update data protection agreements and reassess the status of data disclosures and recipients
7. Complete data retention schedule and program implementation
8. Implement reporting, record-keeping and training
9. Shore-up data security and breach preparedness
10. Determine if all US consumers will get all rights (i.e., the highest level) regardless of residency, or develop and rollout a state-by-state approach

For more information, please contact any of the partners or counsel listed on the next page, or your relationship partner at the firm.

Team

Alan Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Kyle Fath
Partner, Los Angeles
T +1 212 872 9863
E kyle.fath@squirepb.com

Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Colin Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Kristin Bryan
Partner, New York, Cleveland
T +1 212 872 9800
E kristin.bryan@squirepb.com

Glenn Brown
Of Counsel, Atlanta
T +1 678 272 3235
E glenn.brown@squirepb.com

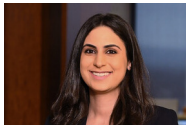
Shea Leitch
Of Counsel, Washington DC
T +1 202 457 6510
E shea.leitch@squirepb.com

Kyle Dull
Senior Associate, New York, Miami
T +1 212 872 9867
E kyle.dull@squirepb.com

Ericka Johnson
Senior Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com

David Oberly
Senior Associate, Cincinnati
T +1 513 361 1252
E david.oberly@squirepb.com

Elizabeth Berthiaume
Associate, Dallas
T +1 214 758 3448
E elizabeth.berthiaume@squirepb.com



Niloufar Massachi
Associate, Los Angeles
T +1 213 689 6580
E niloufar.massachi@squirepb.com

Gicel Tomimbang
Associate, Los Angeles
T +1 213 689 6543
E gicel.tomimbang@squirepb.com

2022 Global Data Review ranked "Elite" and top 10 advisory; #2 for litigation

Appendix 1: Preparing for 2023 State Privacy Laws

Navigating Compliance in a Patchwork of State Privacy Laws

And then there were five. Legislatures across the country have been busy in the first half of 2022 and, despite dozens of states introducing omnibus privacy bills this term, Utah and Connecticut emerged as the only two to have passed and enacted comprehensive privacy laws. They join California, Virginia and Colorado in the already vexing patchwork of state privacy laws with which organizations will have to comply starting in 2023.

Almost certainly, a greatest common factor approach may be in order with respect to certain compliance obligations. For example, the CPRA's privacy policy disclosure obligations would appear to subsume the more limited requirements under the other state laws. In addition, each of the 2023 state privacy laws' requirements as to data protection assessments are materially aligned. That said, there are a number of obligations across the 2023 state privacy laws that are sufficiently dissimilar from one another, particularly when comparing CPRA to the others, that relying on a single approach may not be possible or advisable from either a business or legal perspective. This is especially true when it comes to consumer rights more generally and also specifically with respect to digital advertising issues, where businesses are facing more than a dozen varied opt-out rights, as well as opt-in obligations for sensitive data in some states.

Another ingredient in this cocktail is the lack of regulatory certainty; the California Privacy Protection Agency (CPPA) announced that it would not meet its July 1, 2022, deadline for final regulations. In May 2022, the CCPA issued a proposed first draft of regulations and an Initial Statement of Reasons, which approved the drafts. The public comment period closed at 5 p.m. on August 23. If the CPPA makes any changes based on those comments, it will publish the changes and a new opportunity for public comment will begin. Colorado is also engaged in active rulemaking activities and we can expect to see regulations there as well. As to the other states, it is not fully clear, as their statutes do not provide direct authority to an agency to issue regulations.

That is not to say organizations should not act now. Given the expansion of consumer rights and business obligations and covered data under all laws as compared to CCPA, and the expansive proviso for regulations in the CPRA, companies should spend this time, at the very least, expanding and updating their data inventories, and understand the new obligations these laws present.

By way of example:

- HR and B-to-B information comes fully into scope under CPRA.
- Sensitive data is a new concept under each of the 2023 laws, requiring either opt-in consent or application of an opt-out right.
- Data retention schedules must be understood on a category-by-category basis for CPRA.
- Changes in the digital advertising industry (i.e., the cookieless future) will require your marketing teams to engage in more complicated and privacy-invasive advertising use cases that need to be understood sooner rather than later.
- Profiling and automated decision-making will become regulated under each law, with the CPRA providing a blank slate to the CPPA on the topic to issue potentially onerous, GDPR-inspired regulations.
- The GDPR-inspired controller/processor scheme in VA, CO, UT, and CT will be new for organizations who did not deal with GDPR and involves markedly different analysis than the business/service provider construct of the CCPA/CPRA, requiring significant work on the vendor management aspect of compliance.

In addition, as organizations prepare for compliance with the 2023 state privacy laws, they should be cognizant of any non-compliance with the currently effective CCPA. The California Attorney General has provided no indication that it plans on stopping enforcement of the law between now and January 1, 2023, when it will share enforcement authority under the CPRA with the CPPA. Among others, cookie/Do Not Sell compliance, financial incentives and technical compliance with privacy policy requirements remain as enforcement priorities for the CalAG.

Below, we provide a comparative analysis of various consumer rights and businesses' obligations – comparing the state laws as to one another and to their forerunners, the CCPA and GDPR – and a suggested roadmap toward compliance for the 2023 state privacy laws.

	California Privacy Rights Act (CPRA)	Virginia Consumer Data Protection Act (VCDPA)	Colorado Privacy Act (CPA)	Utah Consumer Privacy Act (UCPA)	Connecticut SB6 (CTPA)
Overview	Amends the California Consumer Privacy Act (CCPA).	Shares similarities with California's CPRA, with additional concepts inspired by the EU's General Data Privacy Regulation (GDPR), but is sufficiently dissimilar to require a separate compliance strategy.	Largely modeled after the VCDPA, but also overlaps with California's CCPA/CPRA, and uses categories like "controller" and "processor," similar to the GDPR and VCDPA.	Largely modeled after the VCDPA, but also overlaps with the CCPA/CPRA, and uses categories like "controller" and "processor," similar to the GDPR and VCDPA.	Largely modeled after the CPA, VCDPA and UCPA, with some similarities to the CPRA (e.g., express prohibition of "dark patterns).
Effective Date (Enforcement Date and Cure)	January 1, 2023 (Enforcement begins on July 1, 2023; 30-Day Notice and Cure Provision will remain in effect indefinitely for security breach violations only).	January 1, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect indefinitely).	July 1, 2023 (Enforcement begins on Effective Date; 60-Day Notice and Cure Provision will remain in effect until January 1, 2025).	December 31, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect indefinitely).	July 1, 2023 (Enforcement begins on Effective Date; 30-Day Notice and Cure Provision will remain in effect until December 31, 2024).
Who Is Covered?	For-profit "businesses" that meet thresholds, including affiliates, joint ventures and partnerships that: 1. Have a gross global annual revenue of > US$25 million 2. Annually buy, sell or "share" for cross-context behavioral advertising purposes personal information of US$10,000 or more California consumers or households OR 3. Derive 50% or more of annual revenues from selling or "sharing" for cross-context behavioral advertising California consumers' personal information	Business entities, including for-profit and B-to-B entities, conducting business in Virginia or that produce products or services that target Virginia residents and, during a calendar year, either: 1. Control or process personal data of at least 100,000 Virginia residents OR 2. Derive 50% of gross revenue from the sale of personal data AND control or process personal data of at least 25,000 Virginia residents	Any legal entity that conducts business in Colorado or that produces or delivers commercial products or services that intentionally target Colorado residents and that satisfies one or both of the following: 1. During a calendar year, controls or processes personal data of 100,000 or more Colorado residents OR 2. Both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents	Applies to "controllers" or "processors" who: 1. Conduct business in Utah or produce a product or service targeted to Utah residents 2. Have annual revenue of US$25 million or more AND 3. (a) Control or process data of 100,000 or more Utah residents in a calendar year OR (b) derive over 50% of the entity's gross revenue from the sale of personal data and control or process personal data of 25,000 or more Utah residents	Applies to individuals and entities that do business in Connecticut, or that produce products or services that are targeted to Connecticut residents, that in the preceding year either: 1. Controlled or processed the personal data of at least 100,000 Connecticut residents (excluding for the purpose of completing a payment transaction) OR 2. Controlled or processed the personal data of at least 25,000 Connecticut residents, if the individual or entity derived more than 25% of its annual gross revenue from selling personal data

Scope of Coverage

The following chart demonstrates the similarities and differences of the current US consumer privacy laws of general application, and compares them to the GDPR:

Consumer Right	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CTPA	PICICA (NV)
Right to access	✓	✓	✓	✓	✓	✓	✓	x
Right to confirm personal data is being processed	✓	Implied	Implied	✓	✓	✓	✓	x
Right to data portability	✓	✓	✓	✓	✓	✓	✓	x
Right to delete[1]	✓	✓	✓	✓	✓	✓	✓	x
Right to correct inaccuracies/right of rectification	✓	x	✓	✓	✓	x	✓	x
Right to opt-out of sale	✓[2]	✓[3]	✓[3]	✓[4]	✓[3]	✓[4]	✓[3]	✓[5]
Right to opt-out of targeted advertising (CO, VA, UT, CT)/cross-context behavioral advertising sharing (CA)	✓	x[6]	✓	✓	✓	✓	✓	x
Right to object to or opt-out of automated decision-making	✓	x	✓[7]	x	x	x	x	x
Right to object to or opt-out of profiling[8]	✓	x	✓	✓	✓	x	✓	x
Choice required for processing of "sensitive" personal data?	Opt-In	x	Opt-Out[9]	Opt-In	Opt-In	Notice + Opp. to Opt-Out	Opt-In	x
Right to object to/restrict processing generally	✓	x	x	x	x	x	x	x
Right to non-discrimination[10]	Implied	✓	✓	✓	✓	✓	✓	x
Notice at collection requirement	✓	✓	✓	x	x	x	x	x
Specific privacy policy content requirements	✓	✓	✓	✓	✓	✓	✓	✓
Purpose/use/retention limitations	✓	Implied	✓	✓	✓	x	✓	x
Privacy and security impact assessments sometimes required	✓	x	✓	✓	✓	x	✓	x
Obligation to maintain reasonable security	✓	Implied	✓	✓	✓	✓	✓	✓

[1] In California and Utah, deletion obligations are limited to PI collected from the consumer, but in Virginia, Colorado and Connecticut, any PI collected about the consumer is in scope of the deletion right.

[2] Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

[3] Any consideration sufficient, but required.

[4] Cash consideration required.

[5] In NV, website and online service operators are required to offer an "opt-out," but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

[6] However, certain data disclosures inherent in this type of advertising are arguably a "sale," subject to opt-out rights.

[7] Subject to substantial expansion under CPRA regulations. Based on preliminary rulemaking activities, it appears that the CPPA is contemplating a GDPR-like approach for automated decision-making and profiling.

[8] CPRA's concept of profiling subject to change under the regulations. The profiling concepts in the other 2023 state privacy laws require legal or substantially similar effects.

[9] Under the CPRA, the Sensitive PI opt-out right applies to certain processing activities beyond business purposes that are to be defined in CPRA regulations.

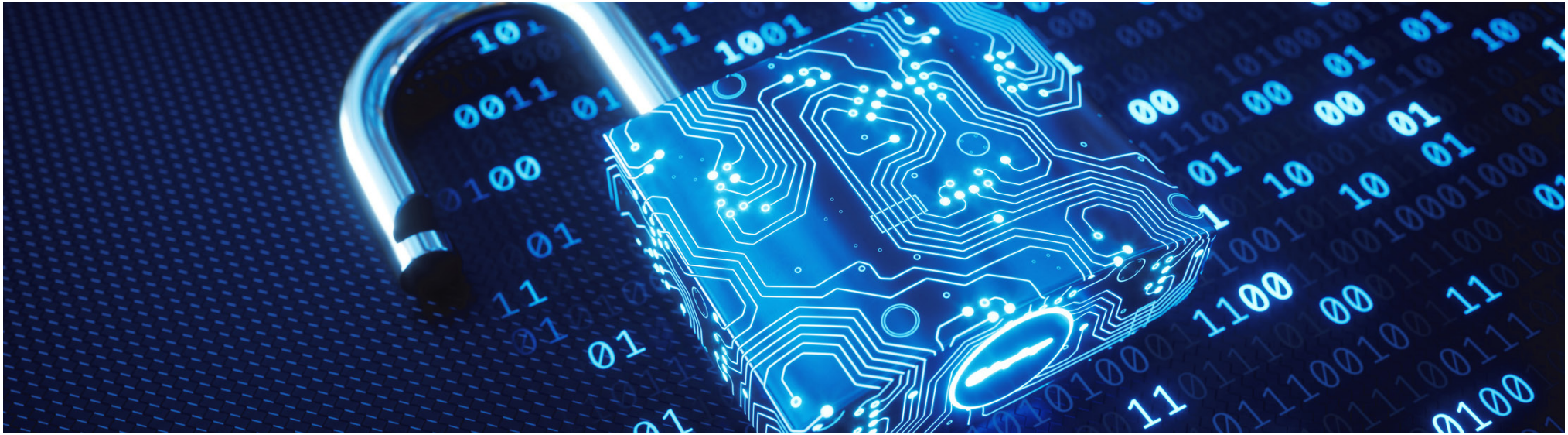
[10] The CCPA (and likely the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer's data to the business.

Exemptions and Exclusions

The 2023 state privacy laws each have exclusions and exemptions, some differing from one another in meaningful ways, as illustrated below:

Exemptions and Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
Employee/HR Data	Fully in scope as of 1/1/23.	Exempt (CCPA-like exemption).	Exempt, but only in so far as maintained as an employment record.	Exempt (CCPA-like exemption).	Exempt (CCPA-like exemption).
B-to-B Contact/ Communications Data	Fully in scope as of 1/1/23.	Specifically exempt + data subjects are only consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they act in an individual or household capacity.	Effectively exempt: data subjects are consumers in so far as they are not acting in a commercial or employment context.
Publicly Available	Information that is lawfully made available from federal, state or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer, or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. Excluded from the definition of PI.	Information that is lawfully made available through federal, state or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience. Excluded from the definition of PD.	Information that is lawfully made available from federal, state or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public. Excluded from the definition of PD.	Information that a person (a) lawfully obtains from a record of a governmental entity; (b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or (c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information. Excluded from the definition of PD.	Information that (a) is lawfully made available through federal, state or municipal government records or widely distributed media, and (b) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public. Excluded from the definition of PD.
De-identified	Excluded from the definition of PI.	Excluded from the definition of PD.	Excluded from the definition of PD.	Excluded from the definition of PD.	Excluded from the definition of PD.
Household Data	Exempt from right to delete, right to correct and right to access (Sections .105, .106, .110 and .115).	N/A.	N/A.	N/A.	N/A.

Exemptions and Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
Aggregate	Exempts aggregate consumer information from the definition of personal information.	Exempts aggregated data from the definition of personal data.	No explicit exemption, but would be exempt if failed to meet the definition of personal data.	Exempts aggregated data from the definition of personal data.	No explicit exemption, but would be exempt if failed to meet the definition of personal data.
Government Entities	Exempt as a business, but could be a service provider, contractor or third party.	Any Virginia state or local government agency or body and institutions of higher learning, as defined, are exempt.	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processors are any person processing on behalf of a controller.	Any government entity or third party under contract with a government entity when the third party is acting on behalf of the government entity, as well as any institution of higher learning, as defined, are exempt.	Any federal, state, municipal or other governmental authorities and institutions of higher education, as defined, are exempt.
Non-profits	Exempt as a business, but could be a service provider, contactor or third party.	Exempts certain types of non-profit organizations (corporations organized under the Virginia Nonstock Corporation Act and organizations exempt from taxation under §§501(c)(3), 501(c)(6) and 501(c)(12) of the Internal Revenue Code).	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processor is any person processing on behalf of a controller.	Any nonprofit corporation is exempt.	Any nonprofit organization, as defined, is exempt.



Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
GLBA/Financial Institution	The GLBA exemption in the CCPA/CPRA is data based, rather than GLBA regulated entity-based and, thus, is much narrower than the GLBA exemption in the other 2023 privacy laws.	Exempts financial institutions subject to the GLBA, plus GLBA-regulated data and "PD collected, processed, sold, or disclosed in compliance with the" FFCA.	Financial institutions subject to the GLBA, and their affiliates, plus GLBA-regulated data.	Exempts financial institutions governed by the GLBA and their affiliates, GLBA-regulated data, and personal data collected, processed, sold, or disclosed in accordance with the FFCA.	Financial institutions or data subject to Title V of GLBA exempt.
FCRA/Credit Reporting	Exempts certain activities of consumer reporting agencies, furnishers and users of consumer reports as defined by the FCRA, to the extent such activities are subject to regulation by the FCRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.	Exemption largely tracks CPRA.
HIPAA/Health	Exempts (1) medical information governed by the CA Confidentiality of Medical Information Act (CMIA), (2) protected health information under HIPAA and CMIA providers and HIPAA, (3) providers of healthcare (CMIA) and HIPAA covered entities to the extent they protect patient data as required by the CMIA and HIPAA, respectively, and (4) certain clinical trial data and biomedical research.	Exempts covered entities and business associates, as those terms are defined by HIPAA + protected health information, as defined under HIPAA, and certain other types of health-related information.	Exempts protected health information, as defined under HIPAA, and certain other types of health-related information, much more broadly than under VCDPA or CCPA/CPRA.	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
COPPA/Children	CPRA shall not be deemed to conflict with obligations under the Children's Online Privacy Protection Act (COPPA).	Exempts controllers and processors that comply with the verified parental consent requirements of COPPA.	Exempts personal data that is "regulated by" COPPA provided that it is collected, processed and maintained in compliance with COPPA.	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.

Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
FERPA/Educational	FERPA data clearly in scope, but certain exemptions regarding access to student records under the state Education Code or to opt-in use for production of physical items, such as yearbooks.	Exempts institutions of higher learning as defined by state law and personal data "regulated by" the Family Educational Rights and Privacy Act (FERPA).	Exempts personal data "regulated by" FERPA.	Exempts institutions of higher education and data regulated by FERPA.	Exempts institutions of higher education and personal data regulated by FERPA.
DPPA/Drivers Information	Exempts PI "collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act" (DPPA).	Exempts personal data that is "collected, processed, sold, or disclosed … in compliance with" the DPPA.	Exempts personal data that is "collected, processed, sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealers regarding motor vehicle repair and warrant use and no other purpose. Note: Not all motorized vehicles meet the definition of motor vehicle.	No specific exemption.	No specific exemption.	No specific exemption.	No specific exemption.
Air Carriers	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Exempt (as defined in 49 U.S.C. §§ 40101, et seq. and 41713).	Exempt (as defined in 49 U.S.C. § 40102).	Exempts personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are defined, by an air carrier subject to 49 U.S.C. § 40101 et seq.
SEC-Regulated Securities Associations	Not exempt.	Not exempt.	Exempts SEC-registered "national securities associations."	Not exempt.	Not specifically exempt.
Public Utilities	Not specifically exempt.	Not specifically exempt.	Exempts customer data maintained by certain public utilities if "not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law."	Not specifically exempt.	Not specifically exempt. Note that limits on sensitive data (e.g., precise geolocation) do not apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Exclusions	CPRA	VCDPA	CPA	UCPA	CTPA
DPPA/Drivers Information	Exempts PI "collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act" (DPPA).	Exempts personal data that is "collected, processed, sold, or disclosed … in compliance with" the DPPA.	Exempts personal data that is "collected, processed, sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."	Exemption largely tracks VCDPA.	Exemption largely tracks VCDPA.
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealers regarding motor vehicle repair and warrant use and no other purpose. Note: Not all motorized vehicles meet the definition of motor vehicle.	No specific exemption.	No specific exemption.	No specific exemption.	No specific exemption.
Air Carriers	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Exempt (as defined in 49 U.S.C. §§ 40101, et seq. and 41713).	Exempt (as defined in 49 U.S.C. § 40102).	Exempts personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are defined, by an air carrier subject to 49 U.S.C. § 40101 et seq.
SEC-Regulated Securities Associations	Not exempt.	Not exempt.	Exempts SEC-registered "national securities associations."	Not exempt.	Not specifically exempt.
Public Utilities	Not specifically exempt.	Not specifically exempt.	Exempts customer data maintained by certain public utilities if "not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law."	Not specifically exempt.	Not specifically exempt. Note that limits on sensitive data (e.g., precise geolocation) do not apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.
Activities Protected by Free Speech/First Amendment or Other Constitutional Rights	Exempt.	Exempt.	Exempt.	Exempt.	Exempt.

Recommendations

Below are high-level recommendations for adapting your current privacy program for compliance with the CPRA, VCDPA, CPA, UCPA and CTPA (collectively, the "2023 privacy laws"), and to help prepare for other potential new consumer privacy laws that may follow, along with a summary of workstreams to enable you to do so. A more detailed 40-page version of the workstreams for use with project management is available for a fixed fee.

1. Assess Compliance and Gaps, and Prepare a 2023 Preparedness Plan

Workstream 1: Preliminary Scoping and Information Gathering

- Conduct a readiness assessment and gap analysis based on existing privacy compliance materials developed for CCPA compliance (e.g., data maps, internal policies, external privacy policy, rights requests procedures, contracts, training, etc.) and practices (e.g., consumer rights response program, cookie consent management platform, etc.).
- Develop a detailed work plan listing all required/optional tasks to allocate roles and responsibilities and a way to track the status and completion of each task. We have tools available at a fixed fee to enable you to do this. Develop a budget tied to the project plan and obtain approval.

2. Create or Update Data Inventories or Maps and Develop and Deploy Data Management Capabilities

Workstream 2: Data Mapping

- Update/develop data map(s) to identify how the following categories of PI1 are collected, used, transferred or disclosed, and for what purposes:
  - Sensitive data
  - B-to-B contact data
  - Employee/contractor/applicant data
- Update data map(s) to account for digital advertising use cases involving both cookie and non-cookie technology and data flows, in view of the cookieless future and new consumer rights under the 2023 state privacy laws.
- Update data maps to account for profiling and automated decision-making processes.
- Identify categories of data that may be totally or partially exempt from the CPRA, VCDPA, CPA, UCPA or CTPA, such as data regulated by the FCRA, GLBA and HIPAA, and certain educational data.
- Determine the reasonably necessary retention period, and the processing purposes, for all data, on a category-by-category basis.

3. Update Privacy Policy(ies) and Remediate Practices

Workstream 3: Annual Privacy Policy Update and Program Audit

- Data means personal information or personal data, as defined under the 2023 state privacy laws.

4. Refine Your Consumer Request Procedure

Workstream 4: Consumer Rights

Modify processes for responding to requests to exercise existing CCPA consumer rights to address new requirements under each of the 2023 privacy laws(e.g., to reflect the longer look-back period for the right to access). In addition, you will need to expand existing rights processes to apply to B-to-B contact data and applicant/employee/contractor data for rights requests from California residents.

5. Implement Privacy-by-Design and Data Governance

Workstream 5: Privacy Impact Assessments and Cybersecurity Audits

- CPRA requires businesses that engage in high-risk processing activities to perform impact assessments that must be filed with the California Privacy Protection Agency. Similarly, the VCDPA and CPA require a controller to conduct a data protection assessment of certain processing activities, including targeted advertising, the sale of data, the processing of sensitive data and any other processing activities that present a heightened risk of harm to consumers.
- Consider a privacy impact assessment program for all data processing, to help meet purpose, proportionality, data minimization, retention and other requirements and reduce risks.

6. Update or Implement a Vendor and Data Recipient Management Program

Workstream 6: Vendor/Supplier Contracts

Review and, as necessary, amend/execute (upstream and downstream) contracts to ensure compliance with the 2023 privacy laws. This includes accounting for new requirements under all of the new privacy laws, but also to account for the differing controller/processor scheme under the non-CPRA laws.

- Identify any (upstream and downstream) contracts that involve the processing of "de-identified" data to include new contract terms required by the 2023 state privacy laws.

7. Update Policies

Workstream 7: Review/Develop/Update Policies

- Update/develop policies to support compliance, including:
  - Privacy policy(ies) and notices (traditional consumer-facing, internal and external HR-facing and B-to-B consumer-facing, as necessary)
  - Consumer rights procedures
  - Privacy impact assessments
  - Audit functions
  - Data retention policies and schedules
  - Record-keeping requirements

8. Implement Reporting, Record-keeping and Training

Workstream 8: Administration and Training

Update training materials for personnel with specific responsibilities for handling consumer requests or compliance to reflect new requirements under the 2023 privacy laws. Consider broader training, especially regarding privacy impact assessments and privacy-by-design and security.

- Confirm that record-keeping and reporting meet the requirements of the final regulations, and any new rulemaking as promulgated throughout 2022.

9. Shore-up Data Security and Breach Preparedness

Workstream 9: Other Compliance (Optional But Recommended)

Review and update a written information security program plan, including incident response plan, acceptable use policy, cookie management and vendor security program.

- Conduct privacy compliance and security breach preparedness (i.e., "tabletop") exercises.

10. Project Audit and Go-Live

Workstream 10: Final Compliance Check and Remediation

- Use a project tracker and compliance checklist to confirm that the responsible persons have signed off on the completion of each task. We have developed such a tool and provide it to clients for a fixed fee.
- Beta test and QA check the new notices and consumer rights tools before going live.

Businesses will benefit from immediately taking steps to develop and implement a 2023 state privacy laws preparedness plan and to thereafter continue to improve compliance on a risk-based basis. Doing so will further help a business prepare for additional consumer privacy laws likely to follow, at the state or federal levels, and will provide the added benefit of better understanding its data and how that can be commercially exploited in a legal and consumer-friendly manner.

Appendix 2:
HR and B-to-B Data:
CCPA/CPRA Compliance Primer

The California Consumer Privacy Act (CCPA) currently has limited carve-outs for personal information (PI) collected from a job applicant, employee, owner, director, officer, medical staff member, or independent contractor of a business acting in such capacity (including, without limitation, communications, emergency contact and benefits PI) (HR data). An even broader exception applies to B-to-B communications and related PI (e.g., vendor, supplier and business customer contacts and communications) (B-to-B data). As a result, businesses subject to the CCPA are not currently required to honor CCPA rights requests received from persons concerning HR data and B-to-B data. These carve-outs are set to sunset on January 1, 2023, when the California Privacy Rights Act (CPRA), which substantially amends the CCPA, goes into full effect, at which point HR data and B-to-B data will be fully subject to all of the requirements of the CCPA/CPRA. Many business administrators had hoped that either the California legislature would extend the HR data exceptions (or maybe even make them permanent), or a federal law that limited data subject rights to traditional consumers would pass and preempt CCPA/CPRA. It is now clear that the former is impossible and the latter is highly unlikely. Accordingly, many companies have a lot to do by year-end to prepare to stand up a CCPA/CPRA program for HR data and B-to-B data.

California Legislature Fails to Act

Bills proposing to extend the CCPA/CPRA exemptions for HR data and B-to-B data were introduced in the California legislature this session, including AB 2871, which proposed to extend the carve-outs indefinitely, and AB 2891, which proposed an extension through January 1, 2026. On August 25, 2022, six days before the legislative session adjourned, Assembly member Cooley proposed amendments (AB 1102) to the CCPA/CPRA that, among other things, would extend the HR carve-outs until January 1, 2025. As we have previously explained, the constitutionality of such amendments is questionable. To address that, AB 1102 dropped any reference to B-to-B data, added certain protections regarding employee monitoring and charged the legislature to further develop privacy protecting terms especially suited for HR data. However, the California legislative session closed on August 31, 2022, with none of these proposals having passed. Therefore, businesses should be prepared to comply with all CCPA/CPRA obligations for HR data by January 1, 2023.

Do Not Count on a Federal Privacy Law Preempting Your CCPA/CPRA Obligations Related to HR Data or B-to-B Data

The American Data Privacy and Protection Act (HR 8152) (ADPPA), a bipartisan federal data privacy legislation, was first introduced in the US House of Representatives on June 21, 2022. We have been following the bill's advancement. On July 20, the House Committee on Energy and Commerce amended ADPPA, after which the bill became eligible for a full House floor vote, meaning that House members may debate the ADPPA before they vote on it. California has emerged as one of the leading critics of the ADPPA, notably with the California Privacy Protection Agency (CPPA) opposing the ADPPA's preemption provisions. In an August 15 letter to Speaker Nancy Pelosi and Minority Leader Kevin McCarthy, the CPPA opined that the ADPPA would "remove important protections and significantly weaken the privacy Californians currently enjoy under the [CCPA]," and presents Americans with a "false choice" by representing that strong state privacy rights "must be taken away to provide privacy rights federally." On September 1, Speaker Pelosi issued a statement on the ADPPA echoing California's concerns on the ADPPA's preemption provisions, and she has reportedly stated that she would not hold a vote on the ADPPA in its current form.

As currently drafted, the ADPPA would generally preempt any state laws that are "covered by the provisions" of the ADPPA, excepting, among other things, "[l]aws that govern the privacy rights or other protections of employees, employee information, students, or student information." See Sec. 404(b)(2)(C). Thus, even if the ADPPA were successful (which appears unlikely based on recent developments), state privacy protections for HR data would not be preempted and, therefore, businesses would still be required to comply with the CCPA/CPRA requirements for the same. While the ADPPA, as drafted, would likely preempt most B-to-B data, it is unlikely to advance without Speaker Pelosi's support.

Complying with CCPA/CPRA – HR Data and B-to-B Application

A business's current HR data obligations under the CCPA will be expanded under the CPRA, and B-to-B data will, for the first time, come into scope. This is a game changer for B-to-B companies that do not touch traditional consumer data (e.g., as a result of consumer marketing, customer service or warranty processing, even if they do not themselves sell direct to consumers) and HR departments. B-to-C companies, and B-to-B companies that process traditional consumer PI other than as a service provider for another business, will be further along, but even they will need to take steps to apply their consumer notices and rights request program to fully include HR data and B-to-B data.

- **Pre-collection notices to applicants, employees and contractors are still required.**

Covered businesses must continue to provide a pre-collection notice informing HR data subjects of the categories of PI to be collected and the purposes for collection. However, the CPRA's amendments to the CCPA, and corresponding new regulations (Regs), will expand a business's obligations regarding HR data notices. This type of pre-collection notice is required both online and offline. The proposed Regs provide that the pre-collection notice to HR data subjects does not need to link to the business's privacy policy, suggesting a separate privacy policy for HR data subjects is permissible. However, the same proposed Regs describe mandatory HR data subject notices that will now be required in the business's privacy policy, suggesting that a business must have a single privacy policy. It may be that there is no conflict and the intent is that if – for HR data subjects – businesses want to satisfy pre-collection notice obligations by means of linking to a document that includes the required disclosures, that need not be the full privacy policy (as the Regs require for pre-collection notice to traditional consumers). However, the business's privacy notice needs to compressively cover all CCPA/CPRA data subjects. Given the difference between data practices related to HR data subjects and those related to traditional consumers, separate schedules, if not separate polices, will be necessary to distinguish between the two data subject types and avoid consumer confusion. Hopefully the next set of proposed Regs will provide more clarity on this subject.

The pre-collection notice to HR data subjects must be easily understandable (i.e., written in plain language) and must inform employees of the statutorily enumerated categories of PI that are collected, including categories of sensitive PI (e.g., government ID number; race, ethnicity, religion, or union membership; contents of communications unless the business is the intended recipient; health-related information; sexual orientation; biometrics; and precise location), and the purposes for collection. Businesses must also disclose whether the categories of PI are sold or shared, the length of retention of the categories of PI and, if the business sells or shares PI, a link (or URL address) to the opt-out notice. If the business allows third parties to control the collection of PI (e.g., benefits providers), the notice shall also include the names of the third parties or information about their business practices. Accordingly, under CPRA, a much more robust notice at collection will be required compared to what was necessary under CCPA.

- **In addition, as to HR data, beginning January 1, 2023, covered businesses should also do the following:**

1. Perform a gap analysis.

As discussed, the expiration of the CCPA/CPRA carve-outs for HR data requires businesses to apply the full scope of CCPA/CPRA requirements to HR data. Therefore, businesses should conduct a gap analysis of their existing HR data privacy program, including, if not previously performed, completing a data inventory to determine where HR data is across business and vendor systems (including both structured and unstructured databases), and how it is obtained, used and disclosed, to determine how their current privacy compliance program can be built out to meet the requirements of the CCPA/CPRA. In doing so, keep in mind that HR data subjects who will soon have access rights include dependents and beneficiaries. Though the Regs are silent on the limitations on their access rights, the statute provides exceptions that may be the basis for limitation. In addition, businesses will need to accommodate new CPRA rights such as correction and limitation of certain processing of sensitive PI (e.g., for affinity and wellness programs). HR professionals will also need CCPA/CPRA training before next year.

2. Provide a full privacy policy to HR data subjects that incorporates all the content requirements for privacy policies enumerated in the implementing regulations.

The California Attorney General previously issued CCPA Regs, which went into effect on August 14, 2020, and that reflected the limited application of the law to HR data then in effect. When the CPRA amendments to the CCPA passed, the CPPA assumed CCPA/CPRA rulemaking responsibilities from the California Attorney General. At the end of May 2022, the CPPA published **Appendix 4** and issued a notice of proposed rulemaking for the same on July 8, 2022, that was followed by a 45-day public comment period that closed on August 23, 2022. Once a revised set of Regs is issued, there will be a public comment period limited to the revisions.

As to privacy policies applicable to HR data, the proposed Regs would require, among other things:

- A description of a covered business's online and offline practices regarding the collection, use, sale, sharing and retention of HR data from the preceding 12 months, including the categories of sources from which HR data is collected, and the recipients of disclosure by category of PI (this is far more comprehensive than what is required in current pre-collection notices).
- An explanation of the rights conferred by the CCPA/CPRA on HR data subjects, including the right to know what PI the business has collected about the data subject (both categories and specific pieces); the right to correct inaccuracies; the right to opt-out of the sale or sharing of HR data by the business; the right to limit the use or disclosure of sensitive HR data by the business (subject to certain exceptions that apply to some but not all HR functions – notably, diversity programs are not an exception); the right to delete PI (subject to a host of exceptions that are so far written to apply in a traditional consumer context and will need to be shoehorned into HR applications); and the right not to be retaliated against for the employee's or contractor's exercise of their CCPA/CPRA privacy rights.
- An explanation of how HR data subjects may exercise their CCPA/CPRA privacy rights and the process for the same, including how the business verifies an employee's request and how an authorized agent may submit a request on behalf of an employee.

3. Implement a mechanism through which HR data subjects may submit requests to exercise their CCPA/CPRA privacy rights.

As with traditional consumer rights requests, covered businesses must also develop and implement a mechanism for receiving rights requests from personnel seeking to exercise their CCPA/CPRA privacy rights. This means that businesses must complete a data inventory of HR data across their systems, and identify outflows to vendors and others, so they can meaningfully respond to requests. Note that although the requirements for HR data do not go into effect until January 1, 2023, the CCPA famously has a 12-month lookback period, meaning businesses must be able to account for HR data throughout 2022, both as to notices and access rights (note, however, the lookback period for access will expand over coming years). Furthermore, the CCPA/CPRA requires businesses to provide at least two designated mechanisms through which individuals, including employees, may submit their CCPA/CPRA-related requests. Most businesses (other than the narrow group that operates exclusively online) must use a toll-free phone number as one of the two designated methods for receiving such requests. If a business has a website, the proposed Regs require that one designated method for receiving such requests be accessible through the website, such as via a webform. However, businesses will likely want a different request flow, or even request process, to distinguish between HR data subject requests and traditional consumer requests. Businesses should also look at existing HR self-service tools and consider how these can be leveraged to, in part, fulfill HR data subject rights requests, keeping record-keeping obligations in mind. Of course, a "consumer" could make a request as both an

employee and a customer, so if requests are segregated by data subject status, that, and how to make requests in another capacity, must be made clear.

4. View CCPA rights requests as if they were discovery requests.

Businesses should be careful when responding to CCPA/CPRA rights requests, especially in the context of HR data, given that plaintiffs' employment lawyers may use CCPA rights requests as a tool to circumvent formal discovery requirements and go on pre-litigation fishing expeditions. Regarding this issue, the California Attorney General previously opined that "there is no exception allowing businesses to refuse to respond to a verifiable [individual] for the [individual's] personal information while litigation is pending or allowing the business to deny [an individual] request on the basis that the business suspects the request was made in lieu of discovery." Thus, plaintiffs' lawyers are not prohibited by the CCPA/CPRA from using rights requests for such purposes. However, evidentiary privileges and the protection of trade secrets and/or the privacy rights of others are grounds for limiting access requests. Essentially, businesses should treat CCPA/CPRA rights requests as akin to responding to discovery requests. In the "Next Steps" section below, we provide a link to a webinar recording that goes into how to do this in detail, applying learnings from Europe, where employees have long had broad PI access rights.

5. Shore up agreements with service providers.

Covered businesses should also shore up their agreements with vendors that process HR data to ensure they meet the CCPA/CPRA's stringent requirements for "service providers." If CCPA/CPRA-required restrictions and provisions are not incorporated into contracts with service providers, a business's transfer of HR data to such parties may constitute a CCPA/CPRA sale or share, which is then subject to a consumer's right to opt out of that disclosure and claw the PI back. Some examples of vendors that may be processing HR data that businesses should keep in mind include those that process data for employee pay, security monitoring, benefits, time keeping and training. However, some of these vendors may act as data controllers in some regards and, accordingly, not qualify as service providers. In such cases, to avoid a "sale," an exception such as disclosure at the direction of the data subject will need to be constructed. Also of importance, businesses should monitor their service provider's compliance with the CCPA/CPRA's restrictions and obligations to not be responsible for a service provider's lack of compliance.

Even if a business updated its agreements with service providers who process HR data during its CCPA compliance program, the CPRA's amendments to the CCPA set forth new additional requirements of what must be included in the written contract between a business and its service provider.

- **Heed recent California Attorney General enforcement activities when building your CCPA/CPRA compliance program for HR data and B-to-B data.**

On August 24, 2022, the California Attorney General issued a press release announcing the first public settlement involving alleged violations of the CCPA, which included a US$1.2 million civil penalty payment. Among other things, the settlement emphasized the requirement for businesses to provide sufficient notice of data "sale" (or "sharing") in their privacy policy, and honor opt-out requests, including when such opt-outs are made via user-enabled opt-out preference signals, especially as to third-party website cookies not contractually restricted to the kind of limited data processing permitted of "service providers" under the CCPA. While many B-to-C companies' websites remain out of compliance in this regard, most B-to-B companies have not even begun to think about tracking technologies and digital advertising as relates to CCPA/CPRA. For more information, see **Appendix 3** to this alert.

Concurrent with the announcement of its first public CCPA settlement, the California Attorney General also published 13 new "illustrative examples" of CCPA noncompliance supplementing the 27 examples provided in July 2021. Businesses should treat these illustrative examples as a guide for what the California Attorney General is looking out for when reviewing a business's compliance with the CCPA, including for CCPA compliance related to HR data. These illustrative examples highlight CCPA compliance related to failure to honor CCPA rights requests and failure to provide CCPA-compliant privacy notices.

And Do Not Forget About B-to-B Data

Companies will need to apply their CCPA/CPRA obligations to B-to-B data, and provide B-to-B data subjects with all consumer rights as of the beginning of next year. In doing this, bear in mind that the current B-to-B exception is not for B-to-B businesses, but for B-to-B data. Accordingly, even B-to-C businesses will have previously out of scope B-to-B data that will now be subject to consumer notices and requests. Most of what we outlined above regarding new requirements for HR data applies equally to B-to-B data. Companies will need to think about how to provide the new notice and process data subject rights in a way that takes into account the differences between these data subjects and traditional consumers. For instance, the need to protect trade secrets – a basis for rejecting an access request – is more likely to arise in the B-to-B data context than in traditional consumer requests.

Additional Guidance

Please refer to these webinar materials for more information on business obligations related to employee and other HR data under the CPRA. The webinar recording is accessible here.

Appendix 3:
Lessons from the First CCPA Civil Penalty Case

On August 24, 2022, California Attorney General Rob Bonta issued a press release announcing the first public settlement by the Office of the Attorney General (OAG) involving alleged violations of the CCPA. The settlement involves a judicial judgment, civil penalties and ongoing monitoring and reporting. The use of noncompliance letters to cajole companies into compliance over many months now appears to be a closed chapter in the CCPA saga. Season 2 promises more drama, more action and more money. Entertaining unless you are the next target!

Key Takeaways

1. According to the OAG, the existence of online tracking technologies on an operator's (i.e., a business) online service (e.g., websites and mobile apps) that collect personal information by a technology provider or other third party are "sales" of personal information by the operator of the online service, because the operator of the online service makes the opportunity to collect and use the data available to the third party, unless those third parties have agreed to contractual restrictions on their use of personal information such that they qualify as "service providers" under the CCPA. If not, you must enable "Do Not Sell" (DNS) to disable the tech or have the third party contractually agree to be a service provider. Keep in mind:
   - Enabling DNS means both an affirmative opt-out mechanism and recognizing and acting on user-enabled "global privacy controls" (GPCs). See GPC.
   - If you rely on signals or settings to restrict tracking technology to service provider processing, the operator of the online service is responsible for ensuring they work and are honored.
   - Cookie banners and preference centers are only sufficient if configured consistent with the OAG's position on DNS and GPC. Many, if not most, are not.
   - What a service provider can do with personal data collected on behalf of a business is incredibly narrow and getting more narrow under the California Privacy Rights Act (CPRA).
2. Review the use of online tracking technology to see if it meets the CPRA's definition of "share" in preparation for the CPRA's amendments to the CCPA, and remember the opt-out of "sharing" goes beyond "selling" and includes cross-contextual behavioral advertising services that might have qualified under the CCPA as a service provider activity (e.g., social media platform matched audience ads).
3. The CCPA's notice and cure provision will no longer apply under CPRA and the OAG has stated that it will expire on January 1, 2023, the CPRA's operative date, although there is a basis for interpreting CPRA to maintain the opportunity to cure until the July 1, 2023 CPRA enforcement date.
4. For purposes of calculating an enforcement penalty, the OAG may consider that each "sale" is a violation, and not necessarily calculate penalties on a per-consumer, per-visit, per-day, or other less colossal measure. Thus, the OAG may seek penalties for millions of violations per day. The potential of crippling penalties raises the stakes of challenging the government's aggressive interpretations of the CCPA and CPRA. The $1.2 million penalty appears calculated to make a point to industry, but at the same time avoid litigation of the issues.
5. Ensure privacy policies and notices are complete and accurate or risk deception and unfairness claims in addition to CCPA claims.

What Happened?

The OAG's CCPA settlement resulted from enforcement efforts that started in July 2020. After settling multiple cookie DNS and GPC cases without monetary penalty or public settlements, the OAG has now required a payment of $1.2 million in a public settlement of such a case. In this game-changing cookie-related enforcement action, according to the OAG's complaint, on June 25, 2021, the OAG notified a retailer/etailer of consumer products (Retailer) about CCPA violations based on the OAG's review and testing of the Retailer's website (we have resolved noncompliance letters on behalf of many clients caught up in such sweeps). The Retailer allegedly did not cure the putative violations to the OAG's satisfaction within 30 days of the date of the notice and, on August 24, 2022, a complaint with proposed settlement and judgment was filed and announced, calling for remediation, civil penalties and ongoing compliance reporting. That is a quick turnaround, based on the time we have had to help clients resolve similar allegations. Thus, we enter a new era of CCPA enforcement where real repercussions apply.

The OAG alleges that the Retailer violated the CCPA because it failed to:

1. Disclose to consumers in its privacy policy that it sells (within the meaning of the CCPA) their personal information, notwithstanding that its website had non-service provider cookies associated with it; rather, the privacy policy affirmatively stated that the Retailer did not sell personal information.
2. Provide a "Do Not Sell My Personal Information" link on its website or in its mobile apps, and offer consumers at least two methods for exercising the right to opt out of the sale of their personal information, including in the case of non-service provider cookies.
3. Configure its website to detect or honor opt-out-of-sale requests sent via a user-enabled GPC. According to the press release announcing the settlement, a user-enabled GPC allows a consumer "to opt out of all online sales in one fell swoop by broadcasting a 'do not sell' signal across every website they visit, without having to click on an opt-out link each time." The OAG found that an activated browser GPC signal had no effect on the Retailer's site's third-party cookies and that consumer personal information continued to flow to third-party companies, including advertising partners and analytics providers.

Relatedly, the complaint also alleged violations of California's Unfair Competition Law, a consumer protection law similar to, but broader than, Section 5 of the Federal Trade Commission (FTC) Act, which prohibits deceptive or unfair commercial practices. The Retailer's privacy policy disclosed the use of online tracking technology but also stated that the Retailer did not sell personal information within the meaning of the CCPA. The OAG argued that this statement was misleading and deceptive. The complaint also alleged that the Retailer "unfairly deprived" consumers of their ability to opt out of the Retailer's sale of personal information. This reflects a more aggressive use of traditional consumer protection laws applied to advertising data practices at the state and the federal level. Indeed, the OAG, in its recent announcements, has echoed recent statements by the FTC referring to long-common digital advertising practices, self-regulated by transparency and opt-out rules, as unfair commercial deception.

To make clear that this first civil penalty is not a one-off, in the same press release announcing the settlement, Attorney General Bonta announced that the OAG sent notices on August 24, 2022, to "a number of businesses" alleging non-compliance for failure to process consumer opt-out requests made via user-enabled global privacy controls" and was conducting website sweeps, something they have been doing for months. Now, however, in the wake of these civil penalties, those letters will have more import.

Concurrently, the OAG published a new list of "illustrative examples" indicating "steps taken" by businesses after receiving one of the OAG's notices of alleged noncompliance to supplement the 27 provided in July 2021. Thirteen new examples cover an array of non-compliance, including not only the same failure to honor consumer requests to opt-out of sales related to web tracking technologies as in the settlement, but also non-compliant notices (including for financial incentive, which we discuss more below, and collection) and privacy policies; absence of required privacy rights request methods; non-compliant methods and erroneous treatment of requests; requiring consumers to waive or limit their CCPA rights; limiting requests to know; and non-compliant verification procedures.

As to the loyalty program example, as we previously covered in Consumer Privacy World, earlier this year the OAG targeted multiple business operating loyalty programs, defined as a "financial incentive" under the CCPA. Now, the OAG has published the resolutions of that sweep. In order to resolve the noncompliance letters, the businesses, depending on the alleged violation:

1. "Posted the Notice of Financial Incentives (NoFI) at cash registers where consumers would reasonably encounter the terms before voluntarily joining the loyalty program."
2. Included a deep link to the NoFI in the online sign-up process.
3. Captured express opt-in consent and "meaningfully provide consumers" with the ability to withdraw from the loyalty program at any time.
4. Included the material terms in the NoFI.

While these other new resolutions apparently did not result in civil penalties, the threat of monetary settlements is now real.

The timing of the OAG's announcement is interesting: it comes four months before the CCPA is expanded by the CPRA, which is effective from January 1, 2023, and while Congress is considering the America Data Privacy and Protection Act (ADPPA), the terms of which would preempt most of the CPRA and the other state privacy laws in Colorado, Connecticut, Utah and Virginia.

For now, the OAG makes clear that it remains committed to enforcing the CCPA and holding violators accountable.

What Was the Result of the Settlement?

The proposed settlement includes a monetary payment to California totaling $1.2 million and also specific compliance requirements that the Retailer must address within 180 days of the final settlement and for two years thereafter.

The settlement requires the Retailer to:

- Update its privacy policy and consumer-facing disclosures to make clear that the Retailer sells consumers' personal information.
- Process consumer opt-out requests received via the GPC.
- Implement and maintain a program to assess, test and monitor whether consumer opt-out requests are properly handled.
- Provide an annual report on the testing, assessment and monitoring together with analysis of errors and technical issues experienced with consumer opt-out requests and how they are remediated.
- Review its websites and mobile apps to determine the entities to which personal information is made available.
- Enter into CCPA compliant service provider agreements with vendors that process personal information, or treat the "making available" of personal information as sells.

As previously discussed in *Consumer Privacy World*, the OAG's GPC requirement is notable because the GPC is a "proposed specification" (like the Data Rights Protocol) and lacks technical details, or clear indication of consumer intent as a rule. The complaint states that the Retailer "wholly disregarded" sales opt-out requests made via the GPC. However, the OAG states in its CCPA FAQs that "Under law, [GPC] must be honored by covered businesses as a valid consumer request to stop the sale of personal information." Further, this is despite the fact that the OAG's rulemaking authority for requiring GPC is dubious at best, especially since the plain language of the CPRA makes GPC (now called OOPS) optional if the business has an online DNS mechanism. Likely, the fact that the California Privacy Protection Agency (CPPA), the additional privacy regulatory agency created by the CPRA, has proposed CPRA regulations with an Orwellian twist to the CPRA to conclude that GPC/OOPS is not optional. For more on this, see our analysis and a similar conclusion by the Internet Advertising Bureau. A business that wanted to challenge the OAG and CPPA on these issues would have a solid basis to do so, but how many operators of online services and retailers are prepared to dedicate resources to litigating the issue and risk reputational harm and massive civil penalties if they are unsuccessful?

It is important to note that the Colorado Attorney General's Office has engaged in pre-rulemaking listening sessions with the public about the upcoming rulemaking on the Colorado Privacy Act (CPA). One of the example topics discussed was a universal opt-out that would allow Colorado consumers "to opt out of the sale of their personal data or use of their data for targeted advertising using a single opt-out mechanism that will be honored by all covered businesses processing their personal data." By July 1, 2023, the Colorado Attorney General is required to specifically adopt rules detailing the technical specifications of one or more universal opt-out mechanisms. (6-1-1313(2), C.R.S.). Under the CPA, honoring the user-enabled opt-out is optional until July 1, 2024, at which time it becomes mandatory. (6-1-1306(1)(a)(IV)(A)-(B), C.R.S.). We have heard that the CPPA and the Colorado Attorney General are in-sync on user-enabled privacy controls and other issues, with the goal being compatibility.

What Should Retailers and Operators of Online Services Do?

The OAG views the right to opt out of sales as a "hallmark" of CCPA. As we have previously discussed, "sale" is broadly and somewhat confusingly defined under CCPA as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration" (Cal. Civ. Code 1798.140(t)). The OAG takes the "making available" language and the lack of monetary exchange to mean that retailers and other operators of online services are responsible for "selling" the personal information collected by third parties associated with their sites or facilities. This is not a new OAG position. The CPPA does the same. See our breakdown of the proposed CPPA regulations, especially regarding third parties collecting personal information in connection with another business's site or facility. Also, keep in mind that on January 1, the CPRA adds a new term, "share," "shared," or "sharing," which is really only processing for cross-context behavioral advertising without the requirement of monetary or other valuable consideration. Thus, businesses should review their advertising practices to see if they meet the OAG's and CPPA's broad definition of "sell" under the CCPA or the new term, "share." Also, operators of online services and retailers beware – the authorities will go after you directly for your adtech and other partners' practices, because you have the direct relationship.

The settlement demonstrates the authorities' broad view of "sale" under CCPA, i.e., online tracking technologies – including cookies, pixels, web beacons and software development kits (SDKs) – that "automatically send data about consumers' online behavior to third-party companies" in exchange for free or presumably discounted analytics and/or advertising services, constitutes a sale of personal information under CCPA in their minds. The OAG's complaint relays the example of a data analytics and digital advertising provider that the Retailer allowed to:

1. Collect personal information via the Retailer's digital properties.
2. Combine that personal information with data that the provider received from other sources to augment a consumer profile.
3. Provide the Retailer with opportunities to re-target the same consumer through the provider's ad network.

In doing so, the settlement clearly expresses the OAG's belief that such commonplace advertising and analytics services are sales and not service provider activities. Further, the proposed CPRA regulations expressly state that a vendor that facilitates cross-context behavioral advertising services cannot qualify as a service provider – even if they use the client's personal information only to provide services to the client (e.g., social media matched ads).

The Gloves Are Off and the Clock is Ticking

The days of genteel sparring with the OAG and having months to cure alleged violations are over. The OAG's press release regarding the settlement states, "My office is watching, and we will hold you accountable. It's been more than two years since the CCPA went into effect, and businesses' right to avoid liability by curing their CCPA violations after they are caught is expiring. There are no more excuses." And, lest you forget, there is a new sheriff in town. Soon the CPPA will also have enforcement authority. And it is clear that both see collection and commercialization of consumer data as suspect, and will err on the side of consumer privacy where statutory ambiguities exist. Well-meaning businesses have struggled with CCPA, and CPRA is far more complicated, plus HR and B-to-B personal information comes into full scope in January. Recent civil penalties suggest that companies should not be lackadaisical about CCPA compliance and 2023 CPRA preparation.

Appendix 4: Takeaways from the First Draft of Revised CCPA Regulations

Most Notable Features of the Regulations

Below we provide an overview of some of the most notable features of the draft Regs:

Opt-Out Preference Signal; Do Not Sell/Share.

The CPRA includes a Global Privacy Control concept referred to as the "opt-out preference signal" (or "OOPS"). Though the statute makes honoring OOPS optional (see Section 1798.135(b)(3) of the statute ("A business that complies with subdivision (a) [i.e., by including opt-out links] … is not required to comply with subdivision (b) [i.e., honoring OOPS]") and Section 1798.185(a)(20)(referring to an election to comply with (b)), the Agency has decidedly taken the position that honoring OOPS is mandatory. Section 7025(e) and 7026(a)(1). The Agency appears to be hanging its hat on its new concept of processing OOPS signals in a "frictionless manner"—i.e., if your business processes OOPS in a frictionless manner it can forgo the opt-out links and mechanism, but if it does not then it must have both the opt-out links and mechanism and have a process for honoring OOPs, though that may involve certain steps and conditions, as discussed in further detail in the next paragraph. Regs. Sections 7013(d), 7025 (but compare to Section 7026(a)(1), which requires, at minimum, two methods in conflict with Section 7013(d) and 7025(e)). This approach is certain to receive a lot of comments and, should it become final, likely judicial challenge.

What is a "Frictionless Manner"?

To be considered to have honored a OOPS signal in a frictionless manner, the business must not: (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; (2) Change the consumer's experience with the product or service offered by the business; or (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal (however, the business is permitted to present a pop-up or other notification asking for consent to ignore the OOPS). Therefore, for example, publishers will still have the opportunity to monetize content and present pop-ups in the way that is currently done when they detect a pop-up blocker. Section 7025(f).

The criteria for a "frictionless manner" comes from what the statute tasks the Agency to determine are part of the specification for the OOPS at 1798.185(a)(20) so there is a basis for requiring the OOPS to be "frictionless," however, that does not necessarily mean that Section 1798.135 does not permit publishers to elect between links or frictionless OOPS. In addition, to qualify under Section 7025(g) to avoid having to post the DNSale NShare link and mechanism, the frictionless OOPS must also act as a consumer opt-out of offline sales and sharing if the business has the ability to link the signal to offline consumer data (e.g., the website visitor is logged in and thereby tied to their profile). It is not clear what is meant by "offline" as it is not defined in the Regs or the statute. Finally, it is proposed that third party controllers (e.g., cookie operators) collecting personal information on a first party business' website are also required to look for and honor OOPS. Section 7052(c).

What can the opt-out link(s) say?

In terms of what links may be used, the Regs provide that they can either state: (1) "Do Not Sell or Share My Personal Information" and, if applicable, "Limit the Use of My Sensitive Information;" (2) Your Privacy Choices; or (3) Your California Privacy Choices; however, "this alternative opt-out link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise ***both*** their right to opt-out of selling/sharing, and the right to limit, instead of posting the two separate [links] " (emphasis added). That begs the question: can a company that does not use or disclose sensitive personal data in a manner that is subject to limitation still take advantage of the alternative link to address sale/share? Given that some sort of conspicuous opt-out link will be required for the other 2023 state privacy laws (e.g., Colorado, Virginia), option 2 would seem to present a clean and consumer friendly way of pointing consumers to their various opt-in and opt-out options. To emphasize, however, if the proposed OOPS provision is not reworked the processing of opt-out preference signals would still be required, they would just seemingly not have to be in a "frictionless manner." See Sections 7013(b) and 7015(b).

Combined DNSell/DNShare Requests?

The Agency appears to treat the separate opt-out from sale and sharing rights as a single, combined obligation to a business. In other words, if a business receives a "Do Not Sell" request it must also treat is as a "Do Not Share" request, and vice versa. A number of sections, including the new definition of "Opt-Out of Sale/Sharing" indicate that the Agency is not bifurcating the concepts and will seemingly require businesses to treat one as both. See, e.g., Sections 7001(z) ("neither sell nor share"), 7025(c) and 7026, among others.

While the statute speaks in terms of a combined DNSale or DNShare link, it provides that such link be "to an internet webpage that enables a consumer … to opt-out of a sale or sharing…" (emphasis added). It is conceivable that some consumers may want to opt-out of sale, but not sharing for cross-context behavioral advertising, or vice versa, and the conflation of these rights in the Regs would prevent that. This, too, is likely to receive comments, assuming the full Agency Board even votes the provision forward. Furthermore, the Regs require DNSell / DNShare opt-outs to be flowed down to third party sale / share recipients, who must honor the opt-out in the same manner as the business. Section 7052(a). There is no express authority in the statute for such a pass through of opt-outs.

No OOPS Technical Details.

Setting aside the controversy of the requirement (or lack thereof) of processing OOPS signals, the Agency provided no technical requirements on opt-out preference signal or regulations touching on the statute's requirement that the signal must be sent with a consumer's consent, which would likely require it to be a user-enabled rather than a default setting. In addition, the Regs provide no details on how a business can and should determine residency with respect to an OOPS signal. While we need significantly more detail on this, and as the debate regarding the optional nature of OOPS rages on, a few other interesting aspects the OOPS-related Regs worth raising include: (1) effectively requiring businesses to tie an OOPS opt-out to non-cookie and other non-online information where a consumer is signed into the business' account online (but not if the consumer is not signed in) (Section 7025(c)(7)(A)-(B)); and (2) displaying an online message as to whether the business has "Honored" the OOPS opt-out for a particular device/consumer (Section 7025(c)(6)). In addition, the Regs not applying the OOPS to limitation of sensitive information, as the statute provides, alone arguably causes the current proposal on OOPS to fall short of the statutory requirements.

Principles Regarding Consumer Requests and Consent.

In addition to the specific requirements regarding the various consumer request types discussed below, the Agency outlined several overarching requirements applicable to all types of consumer requests. Among these general requirements, businesses must:

1. Ensure the consumer request methods and accompanying instructions are easy to understand;
2. Offer symmetry in choice. In other words, "[t]he path for a consumer to exercise a more privacy protective option shall not be longer than the path to exercise a less privacy-protective option."
3. Avoid confusing language (including double negatives).
4. "Avoid manipulative language or choice architecture."
5. Be easy to execute.

Section 7004(a). Failure to comply with the requirements above may be considered a "dark pattern" under the CPRA. Additionally, the Regs clarify that "[a] user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking [sic], or choice, regardless of a business's intent." Section 7004(b) and (c).

Right to Delete.

The draft Regs make explicit businesses' obligations to flow down requests to delete to service providers, contractors, and third parties. Specifically, the Regs instruct businesses to notify contractors and service providers delete PI on request from an eligible consumer, and also require service providers and contractors to comply with those requests and pass the request down to subprocessors. Section 7022(b)(2) and (c). Additionally, third parties to whom a business has shared or sold PI must be instructed to delete the PI(Section 7022(b)(3)), and the Regs add that they must comply (Section 7052(a)). The former is required by the statute, but the latter is not explicitly stated.

Right to Correct.

The Regs' provisions regarding requests to correct primarily revolve around issues of contested data, as well as how businesses are expected to effectuate correction requests. On the former point, the Agency instructs businesses to consider the "totality of the circumstances" when determining whether to accept new PI presented by a consumer, or to reject the request. Factors to consider include:

(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) How the business obtained the contested information.

(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).

Section 7023(b)(1). Helpfully, the Regs add that "[i]f the business is not the source of the personal information and has no documentation to support the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate." Section 7023(b)(2).

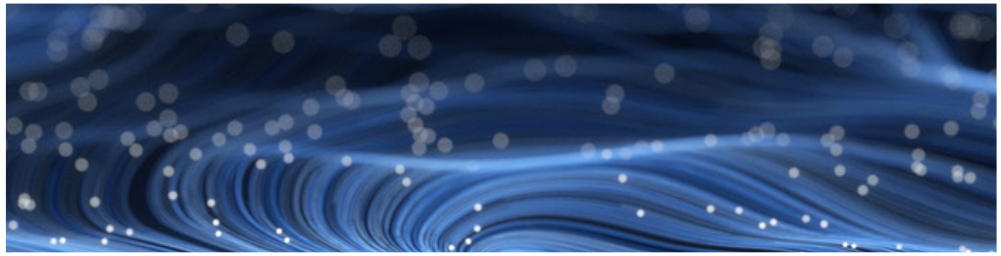
With respect to the implementation of correction requests, the Regs advise that businesses should update the PI on existing systems, and also take measures to ensure that the information stays accurate. Essentially, the CPPA is telling businesses to make sure that corrected information is not subsequently overwritten by incorrect information. Additionally, businesses are obligated to pass along correction requests to contractors and service providers. Section 7023(c).

Limit the Use of My Sensitive Personal Information.

In a regulatory scheme rife with difficult acronyms, we have to compliment the Agency here for coining the phrase "right to limit" to refer to a consumer's right to limit the use or disclosure of sensitive personal information. As promised by the statute, the Regs provide the purposes for which a business can use or disclose sensitive PI without offering the right to limit, including performing services reasonably expected by an average consumer, fraud prevention, ensuring physical safety of natural persons, short term transient use for nonpersonalized advertising, and other routine business purposes. In addition to enumerating such business purposes, the Agency provides helpful examples within each one. See Section 7027. The Regs also require that the privacy notice and retention schedule break out disclosure of sensitive personal information collected into the nine subcategories set forth in the statute.

Verification.

Interestingly, these regulations provide few revisions to the sections relating to verification of requests.



Right to Know (access).

Consistent with the statute's expansion of the lookback period for access requests beyond 12 months after January 1, 2022, the Regs do so, but clarify that they may limit such requests where compliance would involve disproportionate effort, measured by a balancing test of the time and resources against the benefit to the consumer. Section 7001(h) and 7024(h). "For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, **and** would not impact the consumer in any material manner." Section 7001(h)(emphasis added). However, failure to put appropriate systems in place to reasonably fulfill requests will negate a claim of disproportionate effort. *Id.*

Purpose Limitation. "Reasonably Necessary and Proportionate" Defined.

The Regs provide helpful guidance on the purpose limitation requirements in the statute, namely, by defining "reasonably necessary and proportionate." The Regs provide that this limitation means that collection, use, retention, and sharing of PI must be "*consistent with what an average consumer would expect when the personal information was collected*" or "*for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.*" Section 7002(a). This section also provides examples of what may or may not be reasonably necessary and proportionate. However, the examples suggest that certain advertising and marketing practices, particularly regarding geolocation and third party marketing, would not be permissible without specific notice and express consent.

Notice at Collection.

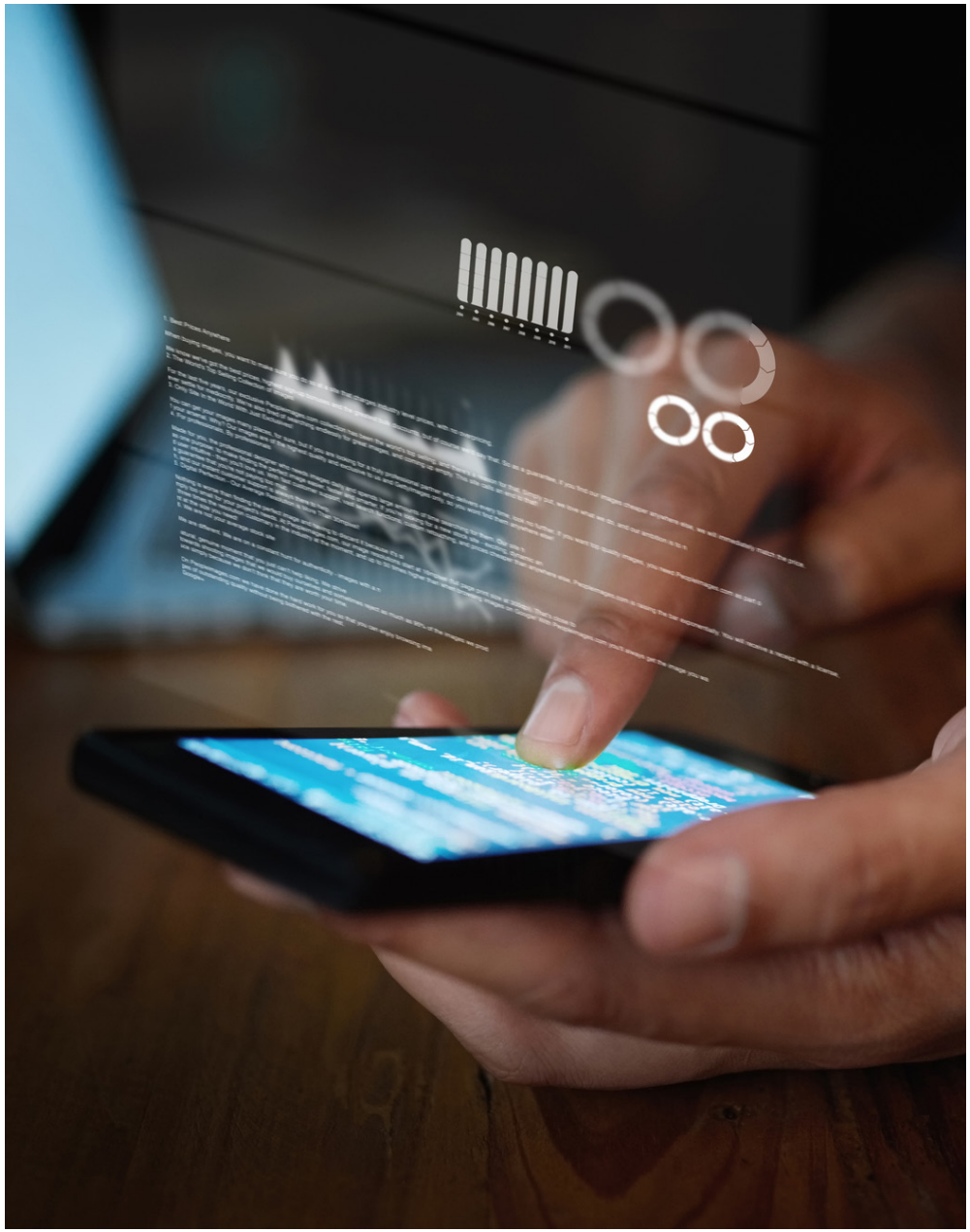
Along with the statutory additions to the notice at collection requirements—most notably, retention details on a category basis (and for sensitive personal information, subcategories)—the Regs have added significant substance, particularly as it relates to third parties controlling the collection on a first party's website or premises. *See* Section 7012. In particular, the Regs require, among other things:

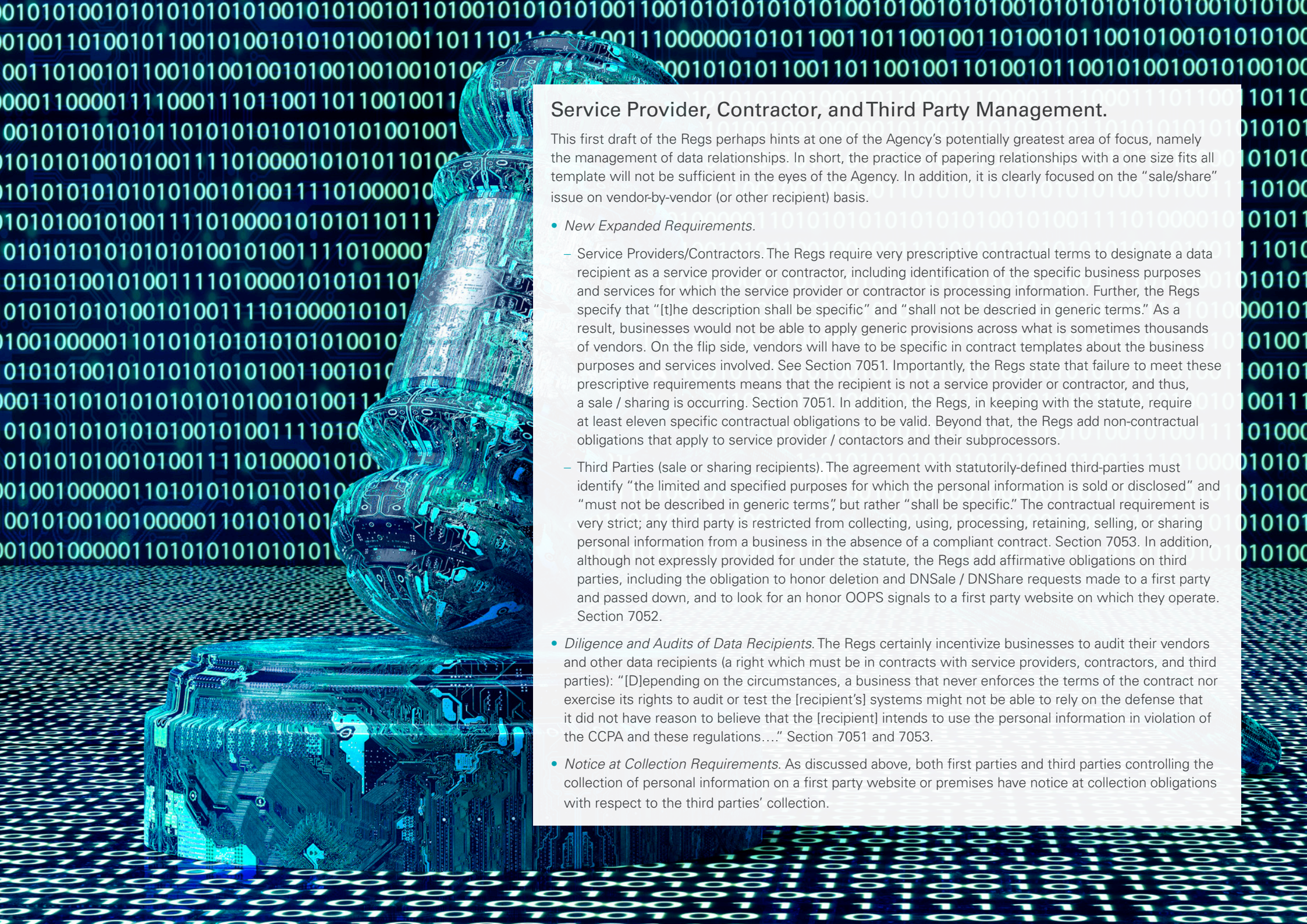
- The first party business to include in its notice at collection names of all such third parties, or in the alternative, information about the third parties' business practices. Section 7012(g)(2).
- The third party businesses that control the collection on another business's website or physical premises, such as in a retail store or in a vehicle, must still provide a notice at collection in a conspicuous manner, though it can do so as part of the first party's notice (e.g., the first party provides notice at collection of where the third party's notice can be found online). Section 7012(g)(1)-(4).
- However, these provisions explicitly do not relive the first party of its obligations "to comply with a consumer's right to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subdivision (f) (honoring opt-outs) and 7052, subdivision (a) (passing opt-outs down to the sale/share recipient). Section 7012(g)(1)(A).

There is no discussion on how this relates to the broadening of the exemption to sale/sharing under the statute where the consumer "uses or directs the business to: (1) intentionally disclose personal information; or (2) intentionally interact with one or more third parties," Section 1798.140(ad)(2)(A) and (ah)(2)(A), and the Regs do not provide any guidance on this type of disclosure.

Notice of Financial Incentive.

While few changes and details are provided in relation to financial incentives (such as loyalty programs, discounts in exchange for email sign-ups, etc., which have been a focus of CCPA enforcement), the Regs remove the requirements of personal information valuation and explaining how that value is reasonably related to the program benefits, unless the program requires waiver of consumer rights to avoid a price or service difference. Sections 7016(d)(5), 7080 and 7081.





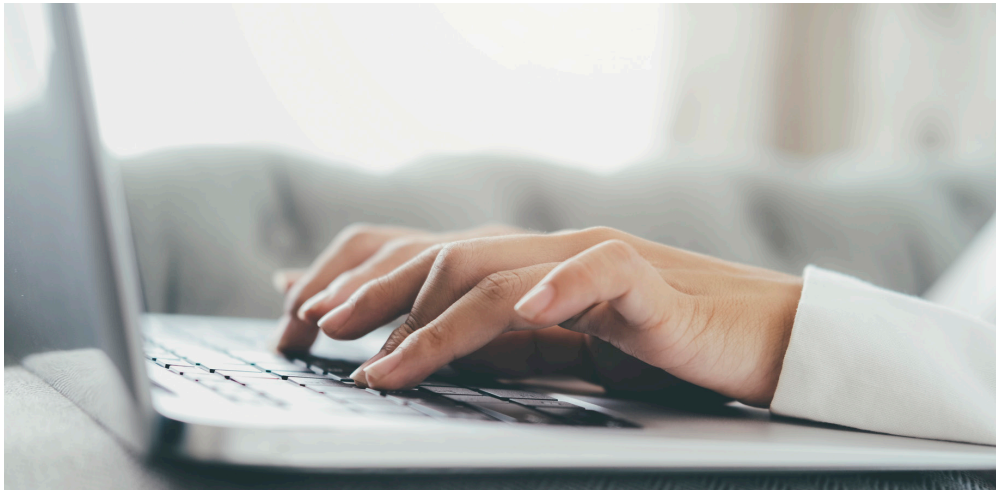
Service Provider, Contractor, and Third Party Management.

This first draft of the Regs perhaps hints at one of the Agency's potentially greatest area of focus, namely the management of data relationships. In short, the practice of papering relationships with a one size fits all template will not be sufficient in the eyes of the Agency. In addition, it is clearly focused on the "sale/share" issue on vendor-by-vendor (or other recipient) basis.

- *New Expanded Requirements.*
  - Service Providers/Contractors. The Regs require very prescriptive contractual terms to designate a data recipient as a service provider or contractor, including identification of the specific business purposes and services for which the service provider or contractor is processing information. Further, the Regs specify that "[t]he description shall be specific" and "shall not be descried in generic terms." As a result, businesses would not be able to apply generic provisions across what is sometimes thousands of vendors. On the flip side, vendors will have to be specific in contract templates about the business purposes and services involved. See Section 7051. Importantly, the Regs state that failure to meet these prescriptive requirements means that the recipient is not a service provider or contractor, and thus, a sale / sharing is occurring. Section 7051. In addition, the Regs, in keeping with the statute, require at least eleven specific contractual obligations to be valid. Beyond that, the Regs add non-contractual obligations that apply to service provider / contactors and their subprocessors.
  - Third Parties (sale or sharing recipients). The agreement with statutorily-defined third-parties must identify "the limited and specified purposes for which the personal information is sold or disclosed" and "must not be described in generic terms", but rather "shall be specific." The contractual requirement is very strict; any third party is restricted from collecting, using, processing, retaining, selling, or sharing personal information from a business in the absence of a compliant contract. Section 7053. In addition, although not expressly provided for under the statute, the Regs add affirmative obligations on third parties, including the obligation to honor deletion and DNSale / DNShare requests made to a first party and passed down, and to look for an honor OOPS signals to a first party website on which they operate. Section 7052.
- *Diligence and Audits of Data Recipients.* The Regs certainly incentivize businesses to audit their vendors and other data recipients (a right which must be in contracts with service providers, contractors, and third parties): "[D]epending on the circumstances, a business that never enforces the terms of the contract nor exercise its rights to audit or test the [recipient's] systems might not be able to rely on the defense that it did not have reason to believe that the [recipient] intends to use the personal information in violation of the CCPA and these regulations…." Section 7051 and 7053.
- *Notice at Collection Requirements.* As discussed above, both first parties and third parties controlling the collection of personal information on a first party website or premises have notice at collection obligations with respect to the third parties' collection.

Enforcement.

The Regs contain a procedure for consumers to submit requests to the Agency, including the information that must be submitted in connection with a complaint. In its Regs, the Agency commits to notifying complainants "in writing of the action, if any, the Agency has taken or plans to take on the complaint," as well as the Agency's rationale for action or inaction. When the Agency initiates an enforcement action, it will issue a probable cause notice to the alleged violator. The Agency will conduct a Probable Cause Proceeding in a closed hearing (unless a public hearing is requested by the alleged violator at least 10 days prior to the proceeding), in which it will evaluate evidence presented by the alleged violator (with counsel) and the CPPA Enforcement Division. The Agency will issue a written Probable Cause Determination based on evidence presented, which will not be a public document. The decision "is final and not subject to appeal." Section 7302. Alternatively, the Enforcement Division and the subject of the complaint may enter into a stipulated order, prior to the entry of a Probable Cause Determination, which will be a public document. Section 7303. Finally, the Regs also empower the Agency to conduct audits, "to investigate possible violations of the CCPA" and also where "the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law." Section 7304. Presumably this means entities which have been subject to significant enforcement actions (for example, by EU supervisory authorities) may expect to be audited by the CPPA.



Notable Regs–Cookies and AdTech.

- *Non-First Party Cookies are deemed a sale or sharing if not qualified as service providers/contractors.* The Regs do not specifically state that the collection of personal information by third-party cookies on a first party site constitute a sale/sharing by the first party site. However, the statute changed the definition of third party to exclude service providers and contractors. The Regs provide that "[a] third party shall comply with a consumer's request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information." Section 7052(a). Further, the Regs make clear that a first party that allows third-party businesses to collect personal information are not thereby relieved from passing DNSale / DNShare opt-out to those third parties. Combined, this implies that absent an exception from sale / share, such as an express direction / interaction (i.e., opt-in) opt-outs apply to third party controllers such as third party cookie operators.
- *Cookie Banners alone are not sufficient for Do Not Sell/Share Opt-Outs.* While this point seems obvious given the growing reliance on cookieless technology and identifiers to target advertisements, it underscores a potential enforcement priority for the Agency of looking beyond facial compliance. The Agency emphasizes that cookie controls like cookie banners only address the "collection" and not the sale or sharing of personal information.
- *Turning off Cookies Will Not Be Sufficient for Honoring a Do Not Sell/Do Not Share Request.* In addition to its statements regarding cookie banners, the Regs require businesses to notify sale/sharing recipients of the request, and require such sale/sharing recipients to notify other downstream recipients, Section 7026(f)(3), and requires third parties to do so, Section 7052(a). In effect, the Regs require a signal-based opt-out system, much like the one that was developed by the Interactive Advertising Bureau (IAB) for the CCPA, and that such signal also trigger a downstream opt-out and not just a termination of ongoing sales / shares. It remains to be seen how organizations outside of the AdTech ecosystem will pass such signals or otherwise provide notifications in relation to DNSell / DNShare requests for more traditional types of PI.
- *Any use cases involving cross-contextual behavioral advertising will prevent a vendor from being considered a service provider or contractor.* In addition, routine activities that are able to fit under the service provider role under the current CCPA, such as custom audiences or email matching for advertising purposes, are stated explicitly in the Regs to fall outside of service provider permitted purposes (and thus would constitute a sale/sharing). Section 7050(c)(1).

2022 Global Data Review ranked "Elite" and top 10 advisory; #2 for litigation

SQUIRE PATTON BOGGS

squirepattonboggs.com

52596/09/22