

Drafting Vendor Agreements to Comply With New US Privacy Laws and the GDPR

TUESDAY, SEPTEMBER 20, 2022

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Aaron J. Burstein, Partner, **Kelley Drye & Warren LLP**, Washington, D.C.

Malcolm Dowden, Partner, **Squire Patton Boggs**, London

Niloufar Massachi, Attorney, **Squire Patton Boggs**, Los Angeles

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1.**

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 ext.1 or visit Strafford's website at www.straffordpub.com.

Presenters



Aaron Burstein

Partner, Washington DC
Kelley Drye & Warren LLP
ABurstein@KelleyDrye.com



Malcolm Dowden

Partner, London
Squire Patton Boggs
malcolm.dowden@squirepb.com



Niloufar Massachi

Associate, Los Angeles
Squire Patton Boggs
niloufar.massachi@squirepb.com

Key Objectives

- Explain contract requirements based on data protection laws
- Provide a foundation for understanding what contractual terms to use in particular situations
- Outline practical approaches for:
 - Harmonization
 - Setting priorities
 - Updating or drafting agreements

Vendor Contracts: What's at Stake?

From the first CCPA enforcement action (August 2022):

13. Sephora installed and used other widely available advertising and analytics services from companies with which Sephora had the same fundamental deal: Sephora allowed the third-party companies access to its customers' online activities in exchange for advertising or analytic services. Sephora knew that these third parties would collect personal information when Sephora installed or allowed the installation of the relevant code on its website or in its app. Sephora also knew that it would receive discounted or higher-quality analytics and other services derived from the data about consumers' online activities, including the option to target advertisements to customers that had merely browsed for products online. Sephora also did not have valid service-provider contracts in place with each third party, which is one exception to "sale" under the CCPA. All of these transactions were sales under the law.

Agenda

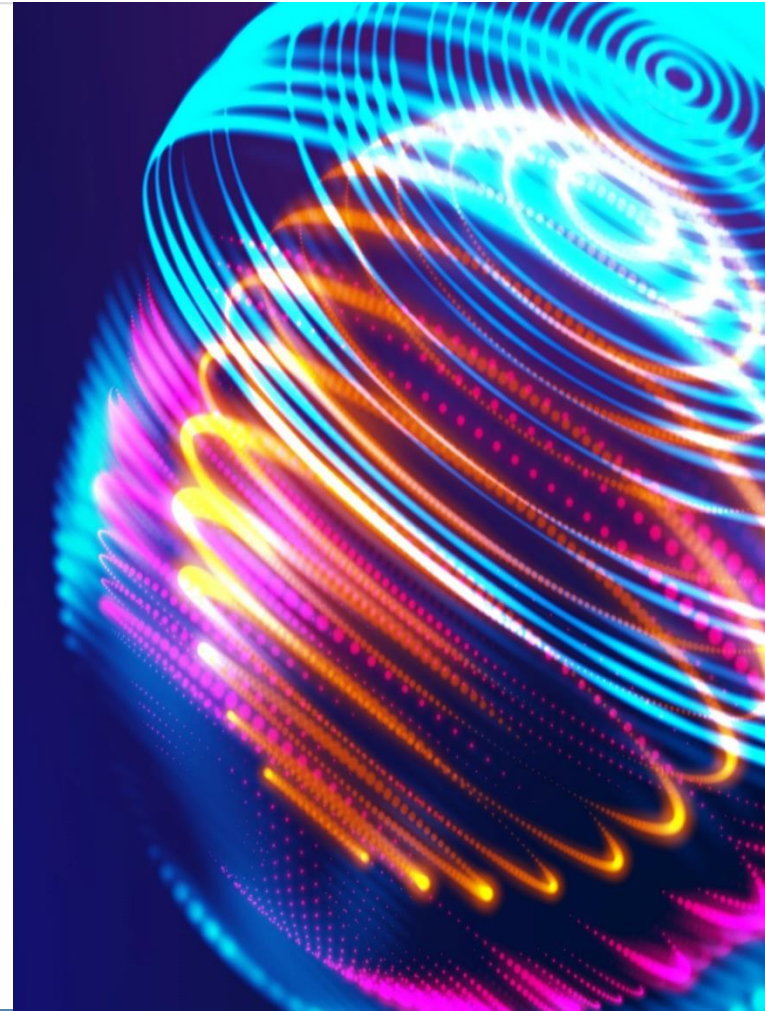
- I. Overview and Trends of Privacy Laws
- II. State Privacy Laws Through the Vendor Contract Lens
- III. Vendor Management
- IV. Questions

I. OVERVIEW AND TRENDS OF PRIVACY LAWS



Setting the Stage

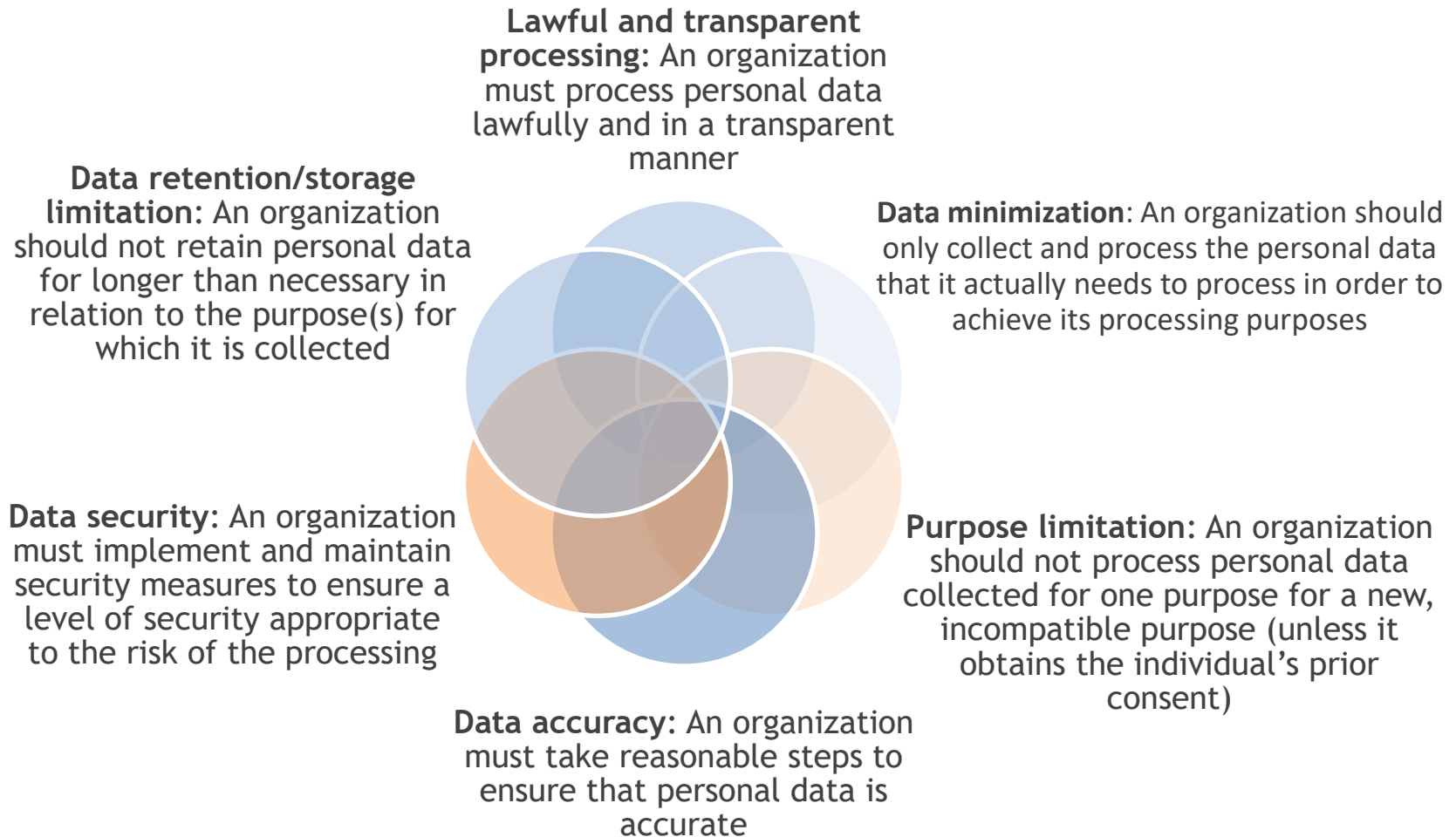
- GDPR and existing US privacy laws regulate vendor contracts
- What's new?
 - Prescriptive requirements under state privacy laws
 - Updated standard contractual clauses (SCCs) under GDPR
 - How to harmonize across states and internationally?
 - How to meet compliance deadlines?



State Laws Create New Privacy Regulators

- California Privacy Protection Agency (CPPA)
 - Broad rulemaking mandate
 - Draft regulations revise existing service provider provisions
 - Timeline for final regulations unclear
- Colorado Attorney General
 - Most regulations are due by July 1, 2023
- State AGs
 - Broad enforcement authority

What core principles apply to the processing of personal data?



Overview and Trends: Historic State of Play

US data privacy laws have traditionally focused on specific sectors.

| | Laws |
|-------------|--|
| Health Care | HIPAA (including HITECH and GINA) |
| | 42 CFR Part 2 |
| | State laws governing health privacy |
| Financial | Gramm-Leach-Bliley Act (GLBA) Safeguards and Privacy Rules |
| | Fair Credit Reporting Act (FCRA) / Fair and Accurate Credit Transactions Act (FACTA) |
| | State laws (e.g., NY Dept. of Financial Services Cybersecurity Rules) |
| Educational | Family Educational Rights and Privacy Act (FERPA) |
| Other | State laws governing “personal information” generally <ul style="list-style-type: none">– Every state has “breach” laws– Roughly half of states have “security laws” (with CA, MA and NV generally more stringent than others outside financial/health)– States have varying “privacy laws” that are generally applicable (e.g., state unfair/deceptive trade practices, online privacy, etc.) |
| | COPPA/Children, Video Privacy Protection Act (VPPA), Electronic Communications Privacy Act, Cable TV Act |
| By Activity | TCPA, CAN-SPAM, Telemarketing Sales Rule |
| Standards | Payment Card Industry Data Security Standard (PCI-DSS) |

FTC Act / State UDAP Standards

The FTC and State Attorneys General have long used their consumer protection authority to bring enforcement actions against *unfair* or *deceptive* acts or practices

Unfairness

- Causes substantial injury to consumers
- Consumers cannot reasonably avoid such injury
- Injury is not offset by countervailing benefits

Deception

- A representation, omission or practice. . .
- About a material fact. . .
- Likely to mislead a consumer acting reasonably under the circumstances.

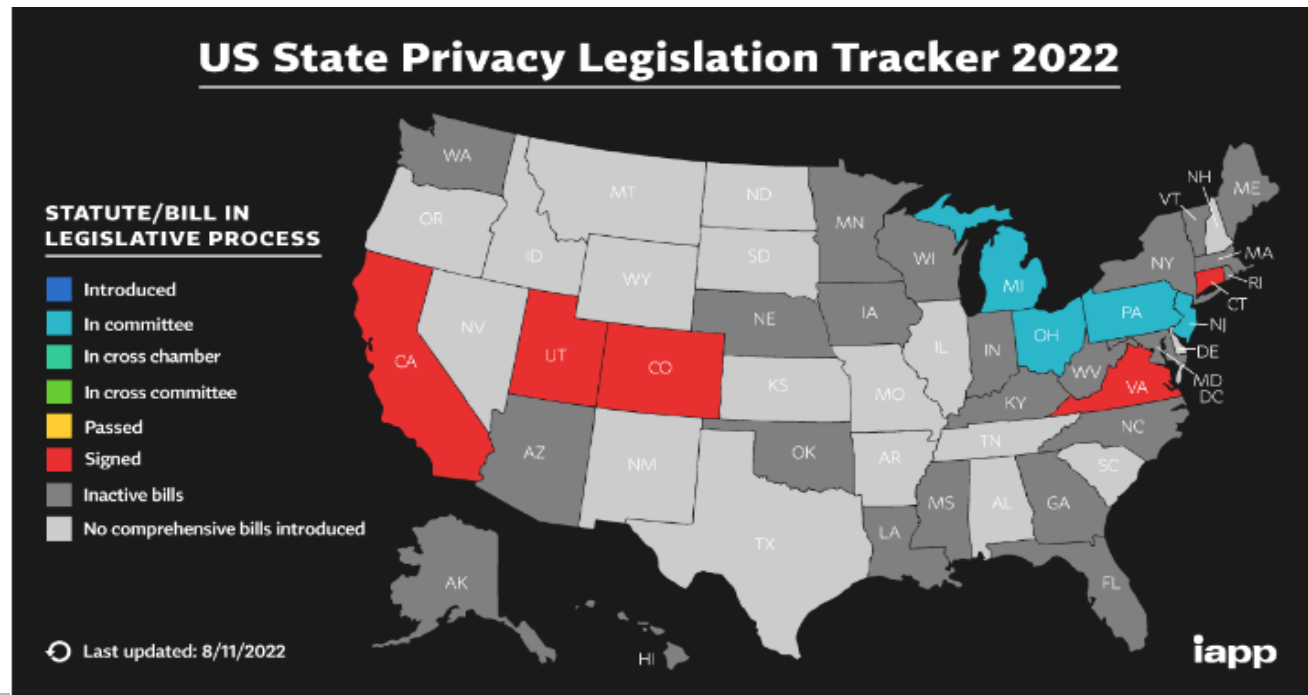
Existing Laws Regulate Vendor Contracts

- FTC Act / State UDAP laws
 - Inadequate vendor due diligence, oversight may be unfair
- GLBA Safeguards Rule
 - Amended Rule (effective Dec. 9, 2022) expands vendor risk assessment requirements
- HIPAA
 - Business Associate Agreements required under Privacy Rule

Overview and Trends of Privacy Laws

State law trend toward comprehensive privacy laws

- California Consumer Privacy Act (CCPA) - Effective since January 2020
- California Privacy Rights Act (CPRA) - Most provisions effective January 1, 2023
- Virginia Consumer Data Protection Act (VCDPA) - Effective January 1, 2023
- Colorado Privacy Act (CPA) - Effective July 1, 2023
- Connecticut Data Privacy Act (CTPA) - Effective July 1, 2023
- Utah Consumer Privacy Act (UCPA) - Effective December 31, 2023



Graphic from
International
Association of
Privacy
Professionals
(IAPP)

Vendor Contract Deadlines

- CCPA: Service provider contracts required since Jan. 1, 2020
- EU: New SCCs required since Sept. 27, 2021, with deadline for migration from old SCCs expiring on Dec. 27 2022
- UK: New SCCs have been in force since March 21, 2022, required for arrangements starting Sept. 21, 2022, with deadline for migration from old SCCs expiring on March 21, 2024
- CA and VA: Additional vendor contract requirements effective on Jan. 1, 2023
- CO, CT (July 1, 2023) and UT (Dec. 31, 2023)

STATE PRIVACY LAWS THROUGH THE VENDOR CONTRACT LENS



Key Framing Questions for Vendor Contracts

Step 1: Is the data flow covered by state privacy laws?

- Is personal data involved?
- Does an exemption apply?

Step 2: What is the relationship of the parties?

Step 3: What are appropriate contract terms?

What types of data are protected under comprehensive privacy laws?

U.S. States

- **California:** Defines “personal information” as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
- **Other states:** Define “personal data” as information that is linked or reasonably linkable to an identified or identifiable individual

Other jurisdictions around the world

- **Brazil:** Defines “personal data” as information regarding an identified or identifiable natural person
- **China:** Defines “personal information” as information related to an identified or identifiable natural person
- **European Union/United Kingdom:** Defines “personal data” as information relating to an identified or identifiable natural person

“Personal Information” Definition is Broad



THE USUAL SUSPECTS

- Name
- SSN
- Financial Information
(*exc. GLBA*)
- Contact Information
- Signature
- Physical Characteristics
- Insurance Policy Number
- Other Gov’t IDs
- Health Data
(*exc. HIPAA*)
- Passport
- Driver’s License



PROTECTED CLASSIFICATIONS / SENSITIVE PI

- Race
- Citizenship
- Color
- National Origin
- Military Status
- Religion
- Gender Identity and Expression
- Sex
- Medical Condition or Disability
- Marital Status
- Age
- Genetic Information



INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY

- Search History
- Browsing History
- Cookie Data
- IP Address
- Interest Data
- Online Interactions

SENSITIVE PI

- Subset of PI that each law considers sensitive



BEHAVIORAL AND PROFILING DATA

- Tendencies
- Products/Services Considered
- Inferences
- Interest Data
- Order History
- Viewing History
- Search History

BIOMETRIC AND GEOLOCATION INFORMATION



SENSORY DATA

- Audio
- Electronic
- Visual
- Thermal
- Similar Information
- Olfactory

PROFESSIONAL, EMPLOYMENT AND EDUCATION-RELATED INFORMATION



What's not subject to these privacy laws?

■ US

- De-identified or aggregate information
- Publicly available information “from federal, state, or local government records” (but not inferences based on those records)
- If a statutory exception applies (HIPAA, GLBA, FCRA)
- If the personal data is Employee or B2B Data it is exempt in VA, CO, UT, and CT
 - For California it is exempt only until Dec. 31, 2022

■ GDPR

- Fully anonymous data (“strongly pseudonymised” data remains in scope for GDPR)

Key Framing Questions for Vendor Contracts

Step 1: Is the data flow covered by state privacy laws?

- Is personal data involved?
- Does an exemption apply?

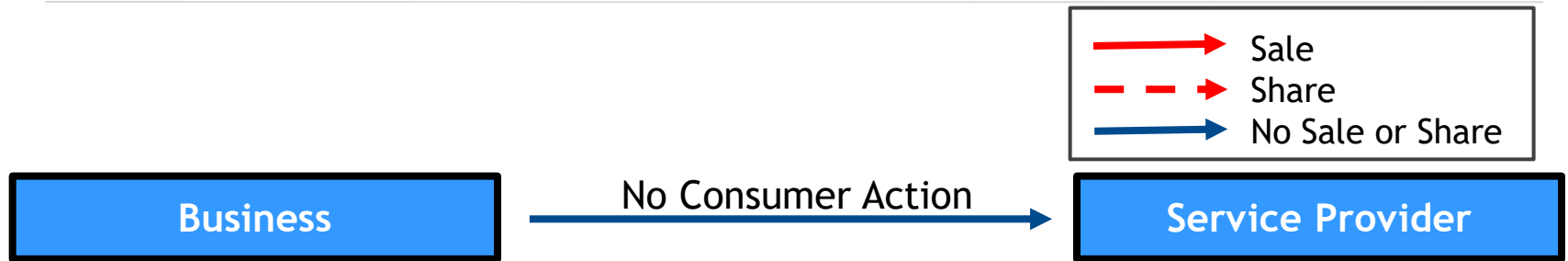
Step 2: What is the relationship of the parties?

Step 3: What are appropriate contract terms?

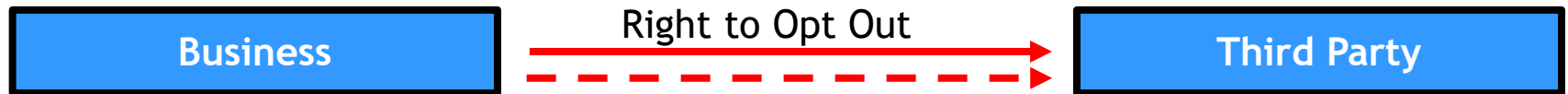
Relationship of the Parties

- Relevant Parties
 - Business/controller
 - Service provider/processor
 - Contractor
 - Third Party
- Arrangements
 - Business/controller to service provider/processor arrangements
 - Controller to controller arrangements
 - Joint controller arrangements
 - Business/controller to contractor
 - Business/controller to third party

How US Laws Regulate Data Flows



If a business transfers PI to a service provider, contractual restrictions replace consumer choice. This is a regulated transfer, so no opt out or consumer action is required to approve the transfer.



If a business sells PI to a third party, the business must provide consumers the opportunity to opt out. This is a regulated transfer subject to consumer opt out.



A business may obtain a consumer's agreement to provide their data to a third party (such as a co-marketing partner). This is called an intentional disclosure. This is a regulated transfer subject to direct consumer approval.

Key Framing Questions for Vendor Contracts

Step 1: Is the data flow covered by state privacy laws?


- Is personal data involved?
- Does an exemption apply?

Step 2: What is the relationship of the parties?

Step 3: What are the appropriate contract terms?

Service Provider: What are appropriate terms?

Step 3

- CPRA Service Provider Terms
 - CPA Processor Terms
 - VCDPA Processor Terms
 - CTPA Processor Terms
 - UCPA Processor Terms
- 
- Generally Overlapping Terms
- CPRA Mandatory Terms for Transfers to Third Parties
 - Other Considerations
 - Indemnification and Limitation on Liability
 - Insurance
 - Data Protection Terms for Other Laws (e.g., Article 28 GDPR)

CPRA Mandatory Language

A business that collects a consumer's PI and that sells that PI to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purposes shall enter into an agreement with the third party, service provider, or contractor, that:

- (1) Specifies limited purposes for data use
- (2) Obligates compliance with CPRA
- (3) Grants the business rights to conduct reasonable oversight
- (4) Requires notification of non-compliance to business
- (5) Grants business the right to remediate unauthorized PI

DPA Requirements

- Limits vendor's use of PI to providing the contracted for services
- Restrict vendor from:
 - Selling or sharing PI
 - Processing PI outside of direct business relationship between the parties
 - Combining PI received from/on behalf of business with PI from other sources
- Require vendor to:
 - Comply with laws and notify business if can no longer meet obligations
 - Ensure PI security
 - Assist with consumer requests
 - Notify business of breach of security of PI and assist with response
 - Provide information for business to conduct data protection assessments
 - Delete PI at end of processing
 - Cooperate with audits
 - Provide business an opportunity to object to engagement of subcontractors

Additional Requirements under non-CA US Privacy Laws

- VCDPA, CPA, UCPA, and CTPA require contracts to include data processing instructions, including:
 - the nature and purpose of processing,
 - the type of data subject to processing,
 - the duration of processing, and
 - the rights and obligations of both parties.
- Requires a list of the type of data subject to processing, which can be a challenge to develop/maintain.

Summary of Vendor Contract Requirements

| CALIFORNIA | | CO | CT | UT | VA |
|--|--|----|----|----|----|
| Do not sell / share | | | | | |
| Specify business purposes | Nature/purpose of processing | Y | Y | Y | Y |
| Limit use to those purposes | Specify processing instructions | Y | Y | Y | Y |
| No retention or use for other purposes | List data types | Y | Y | Y | Y |
| No retention outside of direct business relationship | Specify duration of processing | Y | Y | Y | Y |
| Comply with CCPA | Parties' rights and obligations | N | Y | N | Y |
| Audit rights | Audit rights / demonstration of compliance | Y | Y | N | Y |
| Notification of non-compliance | Delete data at end of processing | Y | Y | N | Y |
| Right to require remediation | Duty of confidentiality | Y | Y | Y | Y |
| Inform business of DSRs | General assistance to controller | Y | Y | Y | Y |
| Subprocessor contracts | Subprocessor contracts | Y | Y | Y | Y |
| Security + breach assistance | General obligations include security | Y | Y | Y | Y |

Which Rights Requests Might Involve a Service Provider?

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 CCPA 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.

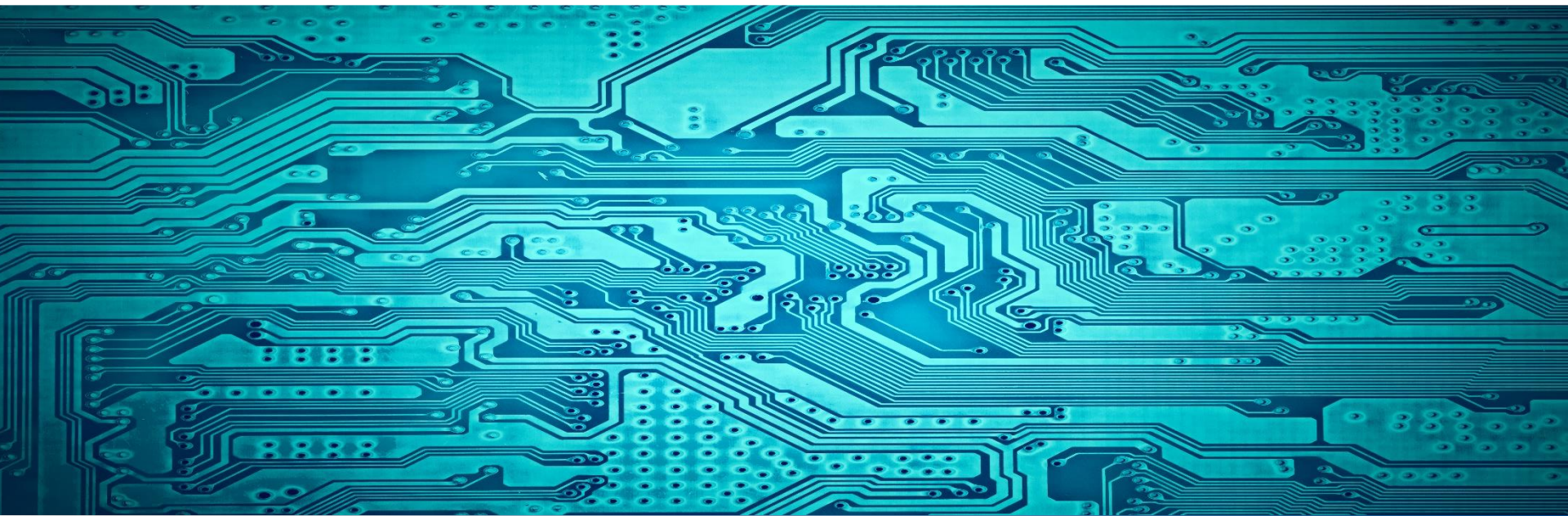
¹⁰ The CCPA (and likely the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer’s data to the business.

Commonly Negotiated DPA Provisions

- International Data Transfers
- Processing Limitations & Requirements
- Security Measures
- Data Subject Rights
- Deletion at the End of Processing
- Audits
- Breaches/Incident Notification
- Using Subprocessors
- Indemnification

Harmonization

- Key considerations
 - Take a global approach?
 - Consider processor re-use of data



VENDOR MANAGEMENT



Vendor Risk Management Program

- Consider a vendor risk management policy
 - Confirm vendor is acting a service provider/processor
 - Assess vendor's data security measures and its sufficiency
 - Policies and procedures (e.g., incident response policy, business continuity policy)
 - Protections for sensitive data
 - Following an industry standard?
 - Encryption at rest
 - History of security incidents
 - Knowing the vendor's location
 - Where is data going to be stored?
 - Will the vendor use sub-processors? If so, where are they located?
Do they have written agreements with them?
 - Regulatory investigations or security related lawsuits

QUESTIONS?



Q&A

You may use the Chat function to ask questions or email questions to lawquestion@straffordpub.com

CLE CODE: TLIGJH

Note: If you are listening to a recording of this webinar, you must include the CLE listen code on your Non-Live Affirmation form in order to receive credit for any state.

Tell us how we did!

Look for our 'Thank You' email (which you should receive within 24 hours) for details and a link to the program survey and attendance attestation.

Not a Passholder Yet?

Try the CLE Individual Annual Pass

- Attend unlimited live webinars in any of our legal practice areas – we produce over 750+ advanced live CLE webinars each year
- Get unlimited access to hundreds of recorded webinars
- Get all your CLE credits for one price

Simply respond to the email you will receive after the program and we will rebate the cost of this webinar from the pass price!

Did you know that Strafford offers **volume discounts**? Add additional attendees to your next webinar order at 25% off (30% off for 5 or more).