New Approachs to Look around the Corner in Transactions Involving Privacy, Security and Related Transfer of Risk

A Conversation with ACC Charlotte

September 8, 2022

Jim Koenig
Partner

Manny Clark
Counsel

Brandon Woods
Partner

Lissette Payne
Associate

troutman pepper

Speakers

Jim Koenig
Partner
New York
Troutman Pepper

Brandon Woods
Partner
Charlotte
Troutman Pepper

Manny Clark
Counsel
Charlotte
Troutman Pepper

Lissette Payne
Associate
Charlotte
Troutman Pepper

Agenda

- Trends in Privacy and Security
- New Approaches to Due Diligence
- Transfering Risk in M&A
- Transfering Risk in Licensing

troutman pepper

Trends in Privacy & Security


Biometrics
Artificial Intelligence
Cloud Computing
Genetics
Block Chain Technology
Dry Testing
Internet of Things
Audio and Visual Technologies
Social Media
Cryptocurrency
Gaming
International Data Transfers
International Data Transfers
Financial Services
Mobile
Machine Learning
Ad Tech
Health Care
Background Screening
Autonomous Vehicles
Facial Recognition
Website and Chatbot Monitoring
Digital Health
Ransomware Attacks
Analytic

5 Key Privacy Trends in Transaction

1. **Common privacy and cyber platforms for serial aquirors** to drive consistency, compliance, and shared/reduced costs.
2. **Common platform allows for intra-portfolio information sharing** (e.g., retail, health).
3. **New laws in U.S. States (CA, VA, UT, CT, CO) and around the world** that focus beyond consumers to B2B and HR. All deals need to be reviewed because there is increased focus on new laws, B2B, and HR.
4. **Year-end deadline for major contracting (legacy EU SCCs must be updated by 12/27/22)**. Companies are using as an opportunity to (i) update all vendor contracts/DPAs to align with California and other state laws and (ii) diligence what has/hasn't been done in contracting (i.e., cost).
5. **New technologies (social, analytics, cloud, mobile, video, audio, and biometrics)** driving expenses around enforcements and for permissions.

3 Innovative Tools for Privacy in M&A and Investments

Pre-diligence essential privacy/security questions

1. **Personal Data Volume.** Does the Company process a high volume of consumer or HR data (1M+ records or 100,000+ records from CA)?

2. **High-Risk Countries.** Is data collected or processed internally or by service providers in, or does the data relate to people from, high-risk countries for privacy, security or CFIUS (e.g., EU, China)?

3. **Sensitive Data or Technology.** Does the Company collect or process sensitive data (e.g., facial recognition, location data, target is an AdTech service provider or data broker, FS/health data, other)?

4. **Data Breach History.** Has the Company experienced a prior breach or cyber event (e.g., ransomware), including disclosures to government (e.g., source code, crypto keys, customer data) if applicable?

5. **Enforcements/Class Action.** Is the Company subject to any prior or current government investigation/enforcement, consent decree or class action?

6. **Information Security.** Does the Company have a formal security program designed to reasonably protect personal and information?

7. **Target Privacy Policy Analysis.** Does the privacy policy contain: uses that are different, restrictions, right to use data for product or service improvement, sharing/selling, AI/ML?

When

- Early stage (i.e., even before a term sheet is signed)

Why

- To provide an initial, high-level assessment of the Company's privacy and security practices without dedicating substantial resources to the review

Early Due Diligence (Pre-Term Sheet) - Inherent Risk and Privacy Policy Foundation Questions

NO.	ITEM DESCRIPTION	Y/N	N/A	Provide Comments / Answers / or Dataroom Location	Complete
New	**PRIVACY & SECURITY**				
1	***Personal Data Volume.*** *Does the Company process a high volume of consumer or HR data (1M+ records or 50,000+ records from CA)?*				
2	***High-Risk Countries.*** *Is data collected or processed internally or by service providers in, or does the data relate to people from, high-risk countries for privacy, security or CFIUS (e.g., EU, China)?*				
3	***Sensitive Data or Technology.*** *Does the Company collect or process sensitive data (e.g., facial recognition, location data, target is an AdTech service provider or data broker, FS/health data, other)?*				
4	***Data Breach History.*** *Has the Company experienced a prior breach or cyber event (e.g., ransomware), including disclosures to government (e.g., source code, crypto keys, customer data) if applicable?*				
5	***Enforcements/Class Action.*** *Is the Company subject to any prior or current government investigation/enforcement, consent decree or class action?*				
6	***Information Security.*** *Does the Company have a formal security program designed to reasonably protect personal and information, including:* *1. Written information security policies* *2. 3rd party validation (e.g. pen testing, SOC or ISO certification)?* *3. SDLC/development testing process* *4. Vulnerability management program (e.g., patching, inventory, secure configuration, encryption)?*				

Inherent Risk Questionnaire

troutman pepper

3 Innovative Tools for Privacy in M&A and Investments (*cont'd*)

Inherent risk dashboard (based on responses to questionnaire)

Transaction Summary & Inherent Risk Analysis

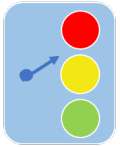
The following is a summary of the key deal points and risks.

Target & Business Description: [Insert description].

Type of Transaction: [Merger][Investment].

Deal Status: Signed on [date].

Target's Overall Inherent Risk



Higher Risk

Moderate Risk

Lower Risk

Key Risk Areas	Analysis – Identified Risk?	Risk Rating
1. Personal Data Volume *Consumer or HR data (1M+ records or 50,000+ records from CA)*	**Yes** – The company processes a high volume of personal data, but it is limited to customer business contact information (name, email) and HR.	
2. High-Risk Countries *Data collected or processed internally or by service providers in or relates to people from high-risk countries for privacy, security or CFIUS (e.g., EU, China)*	**Yes** – The company is primarily focused on U.S. customers but does process EU data.	
3. Sensitive Data or Technology *Collect or process sensitive data (e.g., facial recognition, location data, target is an AdTech service provider or data broker, FS/health data, other)*	**No** – Beyond corporate account information, the data is primarily contact information (usually business-related).	
4. Data Breach History *Prior breach or cyber event (e.g., ransomware)*	**Yes** – [Target] disclosed a recent history of breaches, including two that resulted from a known vulnerability that it had not remediated. Dark web scan did not reveal any compromised employee or customer credentials.	
5. Enforcements/Class Action *Prior or current government investigation/enforcement, consent decree or class action*	**No** – [Target] is not subject to any current investigation or enforcements, but there may be potential exposure related to a lack of investigation/notification of breaches.	

When

- Once LOI is signed

Why

- To scope diligence and gate time/resource allocation
- To assist go/no go decision-making during diligence

3 Innovative Tools for Privacy in M&A and Investments (*cont'd*)

Privacy/security issue remediation framework (and playbook)

Privacy Program & Compliance Issues (P)	Data Rights & Limitations (D)	Information Security (I)	Breaches or Incidents (B)	Enforcements or Legal Actions (E)
Key Issue	*Key Issue*	*Key Issue*	*Key Issue*	*Key Issue*
P-1 **Immature or undocumented program** (e.g., lack of DSR, ROPA, DPAs/SCCs, training)	***D-1*** **Data rights issues/limitations** (use beyond rights, retention, limits on sharing, rights for secondary uses)	***I-1*** **Immature or undocumented program**	***B-1*** **Reportable breach(es)**	***E-1*** **Regulator inquiry (industry or target)**
P-2 **Non-compliance issues** (e.g., failure to address specific laws, codes, individual rights, or contractual obligations)	***D-2*** **Limitations affecting the transaction** (lack of right or consent required to transfer to buyer)	***I-2*** **High-risk findings to be remediated pre-close**	***B-2*** **History of security incidents, ransomware, or exfiltration**	***E-2*** **Enforcement Actions**
P-3 **Employee and worker privacy issues** (e.g., lack of notice, lack of data transfer mechanism)	***D-3*** **Controller/processor issues**			***E-3*** **Lawsuit based on data practices or breach**

When
- During and after diligence

Why
- To consistently and efficiently triage and remediate companies and to move them onto a common platform

Privacy M&A Process

Key Elements

troutman pepper

New Approaches to Due Diligence

Due Diligence Room Approach

1. Check Everywhere – Not Just in the “Privacy Folder”
2. Create a written record of the documents you review and preliminary issues you spot
3. Folders
    - Corporate/Security Issuance
        - Entity structure
        - Geographic scope of the company
        - M&A history
        - Board minutes
    - Intellectual Property
        - Employee Invention Assignment Agreements
        - Consulting Agreements
        - Sometimes contains a sub-folder with privacy and cyber materials
    - Material Agreements
        - Vendor Agreements
        - Customer Agreements
        - Consulting Agreements
    - Litigation
        - Privacy/cyber litigation, inquiries, complaints
    - Insurance
        - Privacy/cyber insurance coverage
    - HR
        - Employee location
        - Employee Privacy Notice
    - Marketing
        - Information about marketing practices
    - Miscellaneous
        - Responses to due diligence questions
    - Privacy/Cyber
        - Privacy policy(ies)
        - Security policy(ies)
        - Pen Test reports
        - Vulnerability Scan reports
        - Incident reports
        - Data Maps

Where in the World Did We Find the Deal-Level Issue?

Target had more than 10 cybersecurity breaches

A. Miscellaneous file – penetration test report.

B. Corporate file – described in minutes of Board meeting.

C. Target X voluntarily disclosed it in response to due diligence questions.

D. None of the above.

Where in the World Did We Find the Deal-Level Issue?

Target had more than 10 cybersecurity breaches.

D. None of the above.

Review of OCR website and state AG websites. OCR and some state AG websites publish breach notification letters, and you can search them to see if a target had any breaches.

Transfering Risk in M&A

Risk Sharing Strategies in M&A

1	Due diligence report/Disclosure schedules to the purchase agreement
2	Negotiation of the reps and warranties/covenants in the purchase agreement
3	Indemnification Terms/RWI Insurance

troutman pepper

Privacy M&A Process

Transactional Documents

Representation Coverage

From 2 paragraphs to 2 pages…

- Breach of laws
- Breach of policies (internal/external)
- Breach of contracts
- Ownership of data - "sufficiency of data" representation
- Security measures
- Data breaches
- International transfers
- GDPR compliance
- Lawsuits / investigations

Covenants

Anything and everything

- Purge data
- Data transfer mechanisms
- Consents
- Required government notifications

Closing Conditions

Privacy policy revisions

Remediation plan implementation:

- Implement IT safeguards
- Fix privacy and data security practices

Standard Representations and Warranties: Privacy

Target has complied with all Laws and contractual fiduciary obligations as to protection and security of Personal Data to which it is subject. Target has not received any inquiries from or been subject to any audit or Legal Proceeding by any Governmental Authority regarding Personal Data. Target has complied with its policies and procedures as to collection, use, processing, storage and transfer of Personal Data. No Legal Proceeding alleging (a) a material violation of any Person's privacy rights or (b) unauthorized access, use or disclosure of Personal Data has been asserted or thereatened to Target. Since [date], there has not been a material violation by Target of any Person's privacy rights or any unauthorized access, use or disclosure by Target of Personal Data.

- According to the ABA's 2021 Private Target Deal Points Study, this rep is used in approximately 67% of private, middle-market M&A transactions.

Standard Representations and Warranties: Cybersecurity

The information technology equipment and related systems, owned, used or held for use by Target ("Systems") are reasonably sufficient for the Businesses' immediate needs. Since [date], there has been no unauthorized access, use, intrusion, or breach of security, or material failure, breakdown, performance reduction or other adverse event affecting any systems that has caused or would reasonably be expected to cause any substantial disruption to the use of such Systems or the Business or any material loss or harm to Target or its personnel, property, or other assets.

- According to the ABA's 2021 Private Target Deal Points Study, this rep is used in approximately 67% of private, middle-market M&A transactions.

Common Red Flags – Pre-Closing Action Items

Buy Side

Things we might want seller to do pre-closing (e.g., closing condition):

- Implement material changes to the privacy policy (e.g., buyer would like to change collection/use of data)
- Delete data or cease certain data collection or marketing activities (e.g., text marketing, selling information under CCPA, collecting children's information and/or targeted marketing)
- Conduct (or let our buyer's security team conduct) a pen test
- Remediate medium, high or critical findings from testing/assessments
- Implement compliance measures for certain key laws (e.g., COPPA age gate)
- Require a special indemnity

Sell Side

Things we might want to fix for a seller:

- Update or replace privacy policy
- Document a privacy and/or security program

Transfering Risk in Licensing

Questions to Ask Before License / Services Negotiations Start

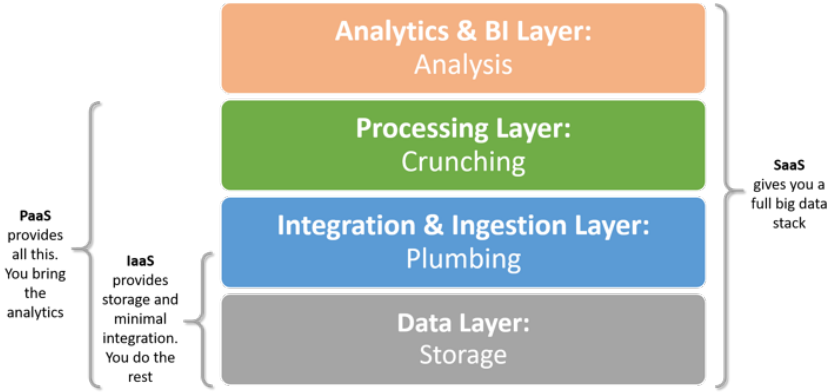
Differences in an M&A deal and a license or services agreement?

Identify the entities and data involved

- Does personal data need to be involved? (It may be ok to send only aggregate data)
- Who and where are the data subjects? (North America? EU? California?)
- Is the data highly sensitive and subject to additional laws? (e.g., health data, financial data, biometric data, etc.)

Who is the Controller vs. Processor? (Any Subprocessors?) (won't always be one controller and one processor)

Will any personal data leave the EEA, Switzerland, or the UK? If so, a transfer mechanism is needed- *STANDARD CONTRACTUAL CLAUSES (more on them later)*



Initial Consideration – The Players

Include Terms and Conditions Regarding Data and Obligations

Historically, in U.S.-styled agreements, handling of data not separated from the statement of work or master agreement. Shift to using more express terms related to data.

Will the parties include a data processing addendum (DPA) to detail the obligations and rights of each party for processing of data?

Controller = Determines why and how of the processing

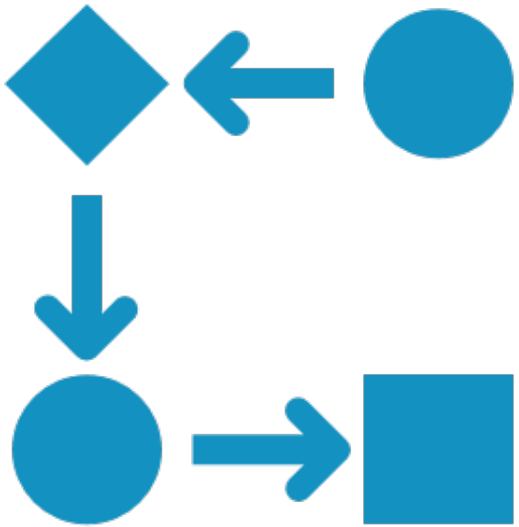
Processor = Processes data on behalf of a Controller

Where is the data going?

B to B

B to C

B to B to C



Minimum Viable Checklist for Agreements (C-2-P Perspective)

Topic	Processor Obligations	Notes
Scope of DPA	**Controller:** Scope of DPA should be all personal data processed anywhere in the world **Processor**: Limit scope to required personal data	If needed for CCPA and other jurisdictions, don't limit to EU
Use Limits	**Controller:** Only use on behalf of Controller as necessary to perform services **Processor:** And, to the extent permitted, to improve services, detect fraud, comply with law, etc.	EU "on instructions of Controller"
Compliance with Law	Process personal data in accordance with applicable law	Check main agreement
Confidentiality	Employees, agents, subs, etc. contractually bound to maintain confidentiality	Check main agreement but verify definition of CI
Information Security	**Controller:** Implement appropriate technical, administrative, and physical measures *that protect* data including specific controls in an exhibit **Processor**: General security controls commensurate with nature of the data *designed to protect* data	See GDPR Art 32 or CIS 18 for standards
Subprocessors	**Controller:** Only engage subprocessors with specific Controller authorization and approval **Processors:** Generally authorized to engage subs	May be general or ad hoc

Minimum Viable Checklist (C-2-P Perspective) Cont.

Topic	Obligations	Notes
Data Subject Rights	**Controller:** Assist in responding to DSRs; promptly forward **Processor:** Make information available through service and get reimbursed for extra work	
Breach Notification and Remediation	**Controller:** Notify Controller promptly (24-48 hours) with all necessary info. Take all actions necessary or requested to remediate the breach. **Processor:** Notify without undue delay when breach confirmed. No breach remediation obligations.	Many different DPA variations
Impact Assessments/Consults	**Controller**: Assist with DPIA and prior consultations with regulators **Processor:** Make information available through service and get reimbursed for extra work	
Return/Deletion of Data	**Controller:** Automatically return or delete at termination **Processor:** Return or delete upon written request, except where can't	Consider triggers

Minimum Viable Checklist (C-2-P Perspective) Cont.

Topic	Processor Obligations	Notes
Demonstrate Compliance	**Controller:** On-site audit rights and provide all info necessary to demonstrate compliance **Processor:** Annual review of policies and procedures	Scope: GDPR and Addendum
Int'l Transfer	Must use adequacy mechanism for EEA, Swiss, or UK personal data	Almost always SCCs
Indemnity	**Controller:** For Security Incident, breach of laws, breach of DPA, all claims **Processor:** For direct damages arising from 3P claims related to Security Incidents due to breach of DPA.	Dependent on leverage
Limitation of Liability	**Controller:** No limit **Processor:** Subject to limits in main agreement (multiple of fees or amount of cyber/privacy insurance)	Consider number of records and sensitivity Most entities are limiting liability related to unauthorized disclosures or cyber events.

Questions?

California Privacy Rights Act of 2020 Series

LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

FRIDAY, APRIL 11, 2022

PERSPECTIVE

California Privacy Rights Act of 2020 brings U.S. closer to European standards

By Ron Raether, Kamran Salour, Sadia Mirza, Robyn W. Lin and Mary Kate Kamka

California was the first state to enact a comprehensive state privacy bill with the California Consumer Privacy Act of 2018 ("CCPA"). Although the CCPA went into effect on January 1, 2020, it was significantly overhauled during California's November 2020 General Election, when the California Privacy Rights Act of 2020 ("CPRA" or the "Act") was adopted.

The CPRA amends the CCPA in several ways, including modifying the thresholds for what qualifies as a regulated "business"; introducing new consumer rights and data processing obligations, and creating the first state agency dedicated to enforcing privacy laws – the California Privacy Protection Agency (the "Agency"). The CPRA also largely moves the California privacy law closer to the direction of the EU General Data Protection Regulation, which is a trend we see with the passage of new state privacy laws in Colorado, Virginia, and Utah. The full text of the CPRA is available here.

This five-part CPRA series is intended to provide a detailed overview of the Act, and how it compares to its predecessor – the CCPA. The series is divided into the following:

1. Introduction and Overview
2. Consumer Rights
3. Notice and Disclosure Obligations
4. Data Processing Obligations
5. Litigation and Enforcement

At the conclusion of the series, Troutman Pepper will host a webinar on the CPRA on Wednesday, May 11, 2022. Registration information will be circulated later.

A. Effective and Operative Dates

While the CPRA technically took effect December 15, 2020 – five days after the Secretary of State filed the statement of vote for the November 3, 2020 General Election – the majority of its provisions will not become operative until January 1, 2023.

B. Lookback Period

Once the CPRA is operative, it will only apply to personal information collected by a business on or after January 1, 2022. The only exception to this rule relates to the "Right to Access." On January 1, 2023, California residents who submit a request to access their personal information may be entitled to access all personal information a business has collected about them, regardless of when that information was collected, subject to the Act's many exemptions.

C. Enforcement Date

The CPRA will not be enforced immediately. Rather, enforcement is set to commence July 1, 2023, and will apply only to violations occurring on or after that date. Notably, the provisions of the CCPA amended or reenacted by the CPRA will remain in full force and effect and will continue to be enforceable until the same provisions of the CPRA become operative and enforceable. Practically, this means that we may continue to see CCPA enforcement initiatives by the California Attorney General up until the CPRA is ready to be enforced.

D. Implementing Regulations and Delayed Wait Times

The CPRA established the Agency and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." The Agency's responsibilities include appointing a "Chief Privacy Auditor" to conduct audits of businesses to ensure compliance with the CPRA and updating existing regulations and adopting new regulations.

Section 1798.185 of the CPRA, which is one of the few provisions that became operative on December 15, 2020, identifies twenty-two (22) areas for which the Agency is required to adopt regulations. This includes:

Right to Correct. Establishing how often, and under what circumstances, a consumer may request a correction under Section 1798.106, including: (i) standards governing how a business responds to a request for correction; (ii) exceptions for requests to which a response is impossible or would involve disproportionate efforts; and (iii) requests for correction of accurate information.

– Opt Out Requests and Processing of Sensitive Information. Establishing rules and procedures to facilitate and govern the submission of a consumer opt-out request of the sale or sharing of personal information under Section 1798.120, and to limit the use of a consumer's sensitive personal information under Section 1798.121.

– Cybersecurity Audits. Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent.

– Risk Assessments. Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to submit to the Agency on a regular basis a risk assessment, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

– Automated Decision-Making Technology. Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision- making processes, as well as a description of the likely outcome of the process with respect to the consumer.

– Agency's Audit Authority. Issuing regulations to define the scope and process for the exercise of the Agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

While the CPRA initially set the deadline for adopting final regulation as July 1, 2022, the Agency's Director, Ashkan Soltani, recently announced that the long-awaited regulations to the CPRA would be delayed. In a recent public meeting, he stated: "Formal proceedings, including public hearings, will continue into Q3 with rulemaking being completed in Q3 or Q4 of 2022. While this puts us somewhat past the July 1 rulemaking schedule in the statute, it allows us to balance staffing of the agency while undertaking substantial information gathering to support our rules."

In remarks with the California Lawyers Association in October 2021, the Agency's Board Chair, Jennifer Urban, spoke on her own behalf and addressed the many logistical and legal impediments in getting the new administrative agency up and running in time to develop and adopt regulations by the deadline. The many challenges include hiring, rulemaking under

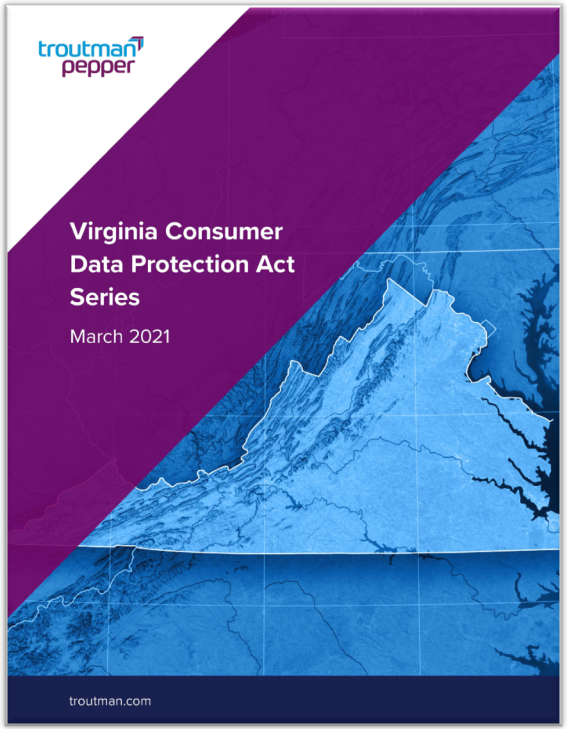
California was the first state to enact a comprehensive state privacy bill with the California Consumer Privacy Act of 2018 (CCPA). Although the CCPA went into effect on January 1, 2020, it was significantly overhauled during California's November 2020 General Election, when the California Privacy Rights Act of 2020 (CPRA or the Act) was adopted.

This five-part CPRA series published in the *Daily Journal* is intended to provide a detailed overview of the Act, and how it compares to its predecessor — the CCPA.

To access the series, please visit: https://www.troutman.com/insights/california-privacy-rights-act-series.html

troutman pepper

Virginia Consumer Data Protection Act Series



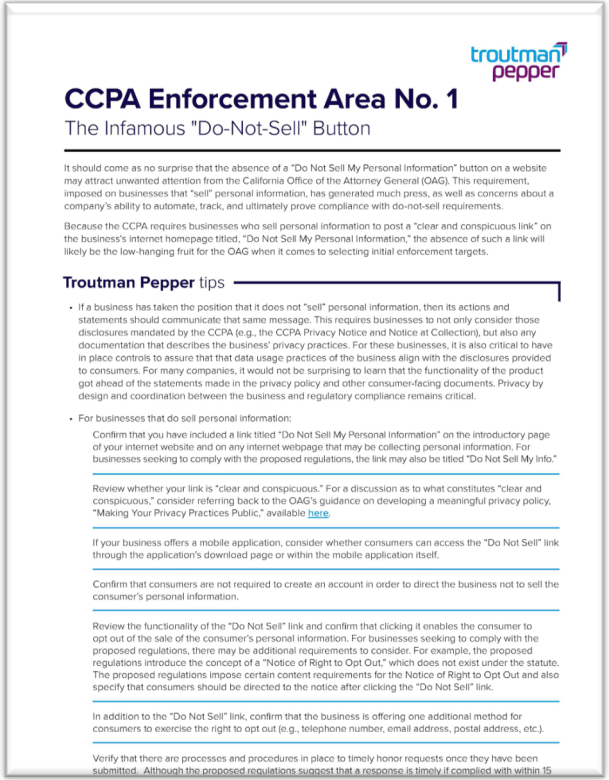
We have long predicted that just as other states followed California in passing breach notification laws, states would follow in California's footsteps in regulating information privacy practices with the California Consumer Privacy Act of 2018 (CCPA), which was later amended by the California Privacy Rights Act of 2020 (CPRA).

Our team has produced a five-part series on Virginia's CDPA. It provides a detailed overview of the act and how it compares to California's approach to privacy under the CCPA and CPRA. To access the entire series, please visit: https://www.troutman.com/insights/virginia-consumer-data-protection-act-series.html

troutman pepper

California Consumer Privacy Act Enforcement Series

Our six-part *California Consumer Privacy Act Enforcement Series* focuses on six areas of enforcement likely to catch the California Office of the Attorney General's attention. Our privacy compliance team discusses discrete strategies to minimize enforcement risk and bolster compliance efforts. To access the entire series, please visit: https://www.troutman.com/insights/california-consumer-privacy-act-enforcement-series-oags-reaction-to-cpra-referendum.html



troutman pepper

CCPA Enforcement Area No. 1

The Infamous "Do-Not-Sell" Button

It should come as no surprise that the absence of a "Do Not Sell My Personal Information" button on a website may attract unwanted attention from the California Office of the Attorney General (OAG). This requirement, imposed on businesses that "sell" personal information, has generated much press, as well as concerns about a company's ability to automate, track, and ultimately prove compliance with do-not-sell requirements.

Because the CCPA requires businesses who sell personal information to post a "clear and conspicuous link" on the business's internet homepage titled, "Do Not Sell My Personal Information," the absence of such a link will likely be the low-hanging fruit for the OAG when it comes to selecting initial enforcement targets.

Troutman Pepper tips

- If a business has taken the position that it does not "sell" personal information, then its actions and statements should communicate that same message. This requires businesses to not only consider those disclosures mandated by the CCPA (e.g., the CCPA Privacy Notice and Notice at Collection), but also any documentation that describes the business' privacy practices. For these businesses, it is also critical to have in place controls to assure that that data usage practices of the business align with the disclosures provided to consumers. For many companies, it would not be surprising to learn that the functionality of the product got ahead of the statements made in the privacy policy and other consumer-facing documents. Privacy by design and coordination between the business and regulatory compliance remains critical.
- For businesses that do sell personal information:

  Confirm that you have included a link titled "Do Not Sell My Personal Information" on the introductory page of your internet website and on any internet webpage that may be collecting personal information. For businesses seeking to comply with the proposed regulations, the link may also be titled "Do Not Sell My Info."

  Review whether your link is "clear and conspicuous." For a discussion as to what constitutes "clear and conspicuous," consider referring back to the OAG's guidance on developing a meaningful privacy policy, "Making Your Privacy Practices Public," available here.

  If your business offers a mobile application, consider whether consumers can access the "Do Not Sell" link through the application's download page or within the mobile application itself.

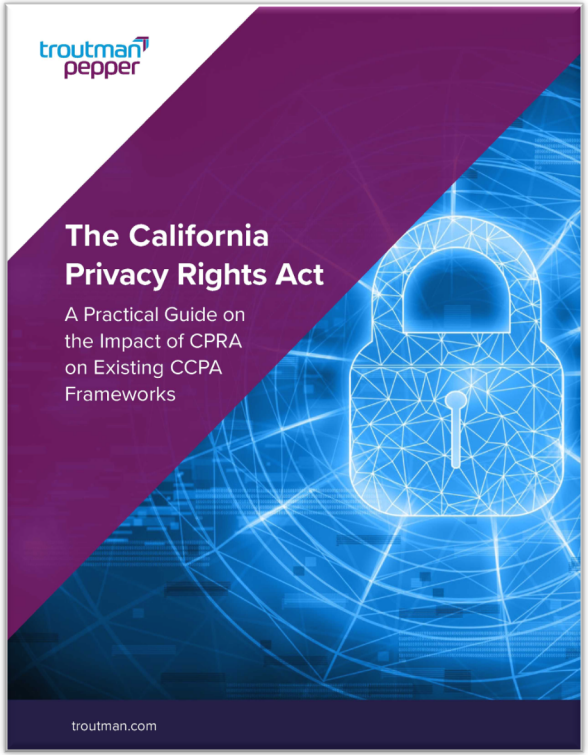
  Confirm that consumers are not required to create an account in order to direct the business not to sell the consumer's personal information.

  Review the functionality of the "Do Not Sell" link and confirm that clicking it enables the consumer to opt out of the sale of the consumer's personal information. For businesses seeking to comply with the proposed regulations, there may be additional requirements to consider. For example, the proposed regulations introduce the concept of a "Notice of Right to Opt Out," which does not exist under the statute. The proposed regulations impose certain content requirements for the Notice of Right to Opt Out and also specify that consumers should be directed to the notice after clicking the "Do Not Sell" link.

  In addition to the "Do Not Sell" link, confirm that the business is offering one additional method for consumers to exercise the right to opt out (e.g., telephone number, email address, postal address, etc.).

  Verify that there are processes and procedures in place to timely honor requests once they have been submitted. Although the proposed regulations suggest that a response is timely if complied with within 15

The California Privacy Rights Act: A Practical Guide on the Impact of CPRA and Existing CCPA Frameworks



We have compiled a compendium entitled, “The California Privacy Rights Act: A Practical Guide on the Impact of CPRA and Existing CCPA Frameworks,” which provides an overview of the operational impact of the CPRA on existing CCPA compliance frameworks. It focuses on issues such as notable updates to existing definitions, the addition of new consumer rights, modifications to existing CCPA rights, and newly introduced concepts (at least for the CCPA) such as data minimization and limitations on the use of “sensitive personal information.”

More Privacy, Please

The *More Privacy, Please* monthly newsletter recaps significant industry and legal developments, as well as trends in the areas of cybersecurity, information governance, and privacy. To access the latest installment, please visit https://www.troutman.com/insights/more-privacy-please.html

To subscribe to our mailing list, please visit https://www.troutman.com/signup-page.html

troutman pepper

Thank you!

Jim Koenig
Partner
New York
Troutman Pepper
jim.koenig@troutman.com

Brandon Woods
Partner
Charlotte
Troutman Pepper
brandon.woods@troutman.com

Manny Clark
Counsel
Charlotte
Troutman Pepper
manny.clark@troutman.com

Lissette Payne
Associate
Charlotte
Troutman Pepper
lissette.payne@troutman.com