US Consumer Privacy Program Workshop:

Lessons Learned and the Challenges Ahead to Address Evolving and Expanding Laws

Speakers

Alan Friel

Deputy Chair
Global Data Practice
Squire Patton Boggs

David Manek

Senior Managing Director, Data Privacy Practice Lead
Ankura Consulting

Linda Trickey

Assistant General Counsel, Privacy & Security
Cox Communications

US Consumer Privacy Program Workshop

Privacy+ Security Forum

1. Experiences and Lessons Learned 2018/19/20

2. Challenges of Evolving Interpretations of CCPA and CPRA / CDPA and other potential new laws

---------- Break ----------

3. CPRA/CDPA Readiness
   - Project plan and workstreams
   - Planning for the future
   - The retention challange

4. Case Studies and Questions

CCPA Experiences and Lessons Learned 2018/19/20

Privacy+ Security Forum

What worked?

- Stakeholder engagement
- Management support, including budget and regular meetings on progress
- Starting early
  - Educated “guesses” on interpretation of the law
  - Focus on baseline data mapping and inventory
  - Revisit as the regs evolved
- Formal project manager and workflows
  - With or without an outside consultant

What worked? (continued)

- Use of platforms and vendors
- Governance that includes stakeholder involvement in operationalizing
- Inside counsel on the front line with support from outside counsel
- Use of assessments and gap analysis to develop work plan and responsibilities, and regular tracking meetings

What was challenging or just didn't work

- Cutting corners on data mapping
- Creating an accessible and evolving inventory
  - Challenges to providing effective notices
    - pre-collection and off-line challenges
  - Challenges responding to requests
    - Data that is not useful or overly burdensome
  - Challenges to annual update
- Not having a vendor management system and thousands of processors
- Lack of PIAs throughout the year

What was challenging or just didn't work (continued)

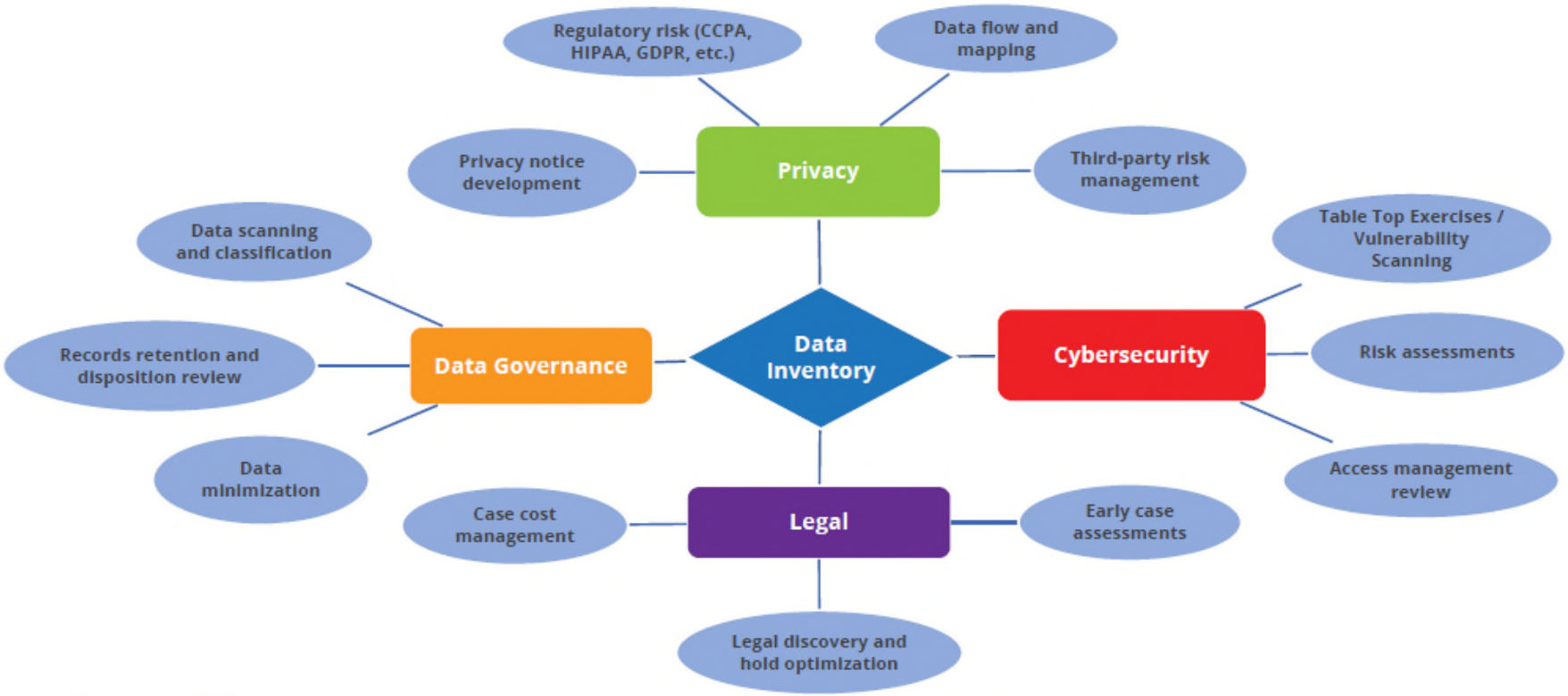
- Differing interpretations of the statute
- Split by adtech on what "sell" means and who is responsible for notice and opt-out (DAA vs. NAI)
- Moving target of the regulations
- Waiting too late to get started and throwing up "CCPA Lite"
- Ad hoc approach – not investing in foundational program and tools
- Static data map / no PIAs / Privacy by Design

What can we build off for future laws?

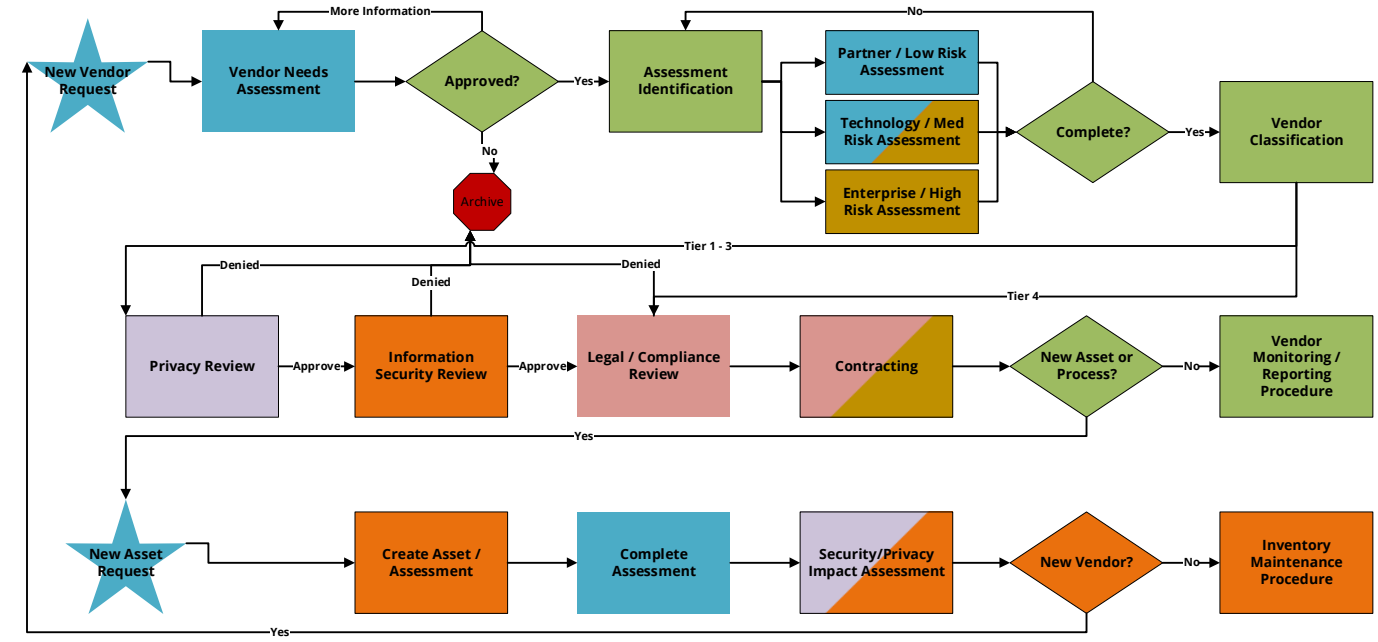
- Governance structure
- CRR procedures and platform
- Existing training and awareness
- Cookie consent platform
- Privacy-by-design
- Good notices
- FAQs – consumer education
- Retention programs and schedules
- Vendor management
  - DPAs
  - Assessments
  - Monitoring
- Data inventory

Get More Out of Your Data Inventory

Privacy+ Security Forum



Target Operating Model To Integrate Privacy, Vendor Risk Management, Security and Legal Functions



Part 2:

Challenges of Evolving Interpretations of CCPA and CPRA / CDPA and other potential new laws

Privacy+ Security Forum

CCPA 1.0 – What is a "sale"

Privacy+ Security Forum

1. "Sell" means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, or 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 consideration."
2. "Personal Information" includes IP address, unique ID and associated usage activities and inferences.
3. If "sell" then "opt-out"
4. Who collects and from whom?
   i. The DAA theory
   ii. Not our problem, but…
5. Exception from "sale" -- "service providers"
   i. IAB, Google, Facebook
6. Exception from sale – direction of the user

Additional CCPA 1.0 Limitations + Repercussions

Privacy+ Security Forum

Limits on differential treatment and universal opt-out

1. **Limits on discrimination and financial incentives**
   - Must be reasonably related to the value of the consumer data
   - Opt-in, with ability to withdraw
   - Advance notice requirements, including valuation statement
2. **"Global Privacy Control"**
   - Act grants authority to develop regs to "facilitate and govern" opt-outs
   - Regs require "user enabled privacy controls" to be a valid opt-out if:
     - clearly communicate intent to opt-out;
     - if conflicts with opt-ins, including financial incentive programs, must notify and give choice
   - AG endorses new browser controls
3. **Enforcement**
   - Over 200 pending actions, including as to IBA cookies and "do not sell"
   - 30 day cure (for now)
   - Civil penalties, but no consumer lawsuits

California Privacy Rights Act ("CPRA")

Privacy+ Security Forum

Limits on differential treatment and universal opt-out

- Amends certain provisions of the CCPA
- Timeline
  - Became effective on December 16, 2020
  - Most provisions are not operative until January 1, 2023
  - Enforcement of the CPRA-amended title begins on July 1, 2023
- Data Covered
  - The scope of "personal information" remains broad but is amended in a number of ways
- Creates new data protection authority ("Agency")

New U.S. Consumer Privacy Rights

CA and VA pass EU-inspired legislation

Consumer Right	CCPA	CPRA	VCDPA	GDPR
Right to access	✓	✓	✓	✓
Right to confirm personal data is being processed	Implied	Implied	✓	✓
Right to data portability	✓	✓	✓	✓
Right to delete	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	×	✓	✓	✓
Right to opt-out of sales	✓	✓	✓	✓*
Right to opt-out of targeted advertising/cross-context advertising	×**	✓	✓	✓
Right to object to or opt-out of automated decision-making	×	✓	✓	✓
Opt-in or opt-out for processing of "sensitive" personal data?	×	Opt-out†	Opt-in	Opt-in††
Right to object to/restrict processing generally	×	×	×	✓
Right to non-discrimination	✓	✓	✓	Implied

*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.

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

†Under the CPRA, consumers' opt out rights do not apply to processing sensitive personal information for certain limited purposes.

††Under the GDPR, processing sensitive personal information is allowed with explicit consumer consent or where it is otherwise justified under another recognized lawful basis.

TL(2

"Sell" vs. "Share" and scope of "Business"

Privacy+ Security Forum

Resolving the consideration controversy…, but not all issues…

Sell	Share
"…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**."	"…**sharing**, 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 a third party **for cross-context behavioral advertising**, **whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged**."

Slide 17

TL(2 Alan, what is definition of "share" under CPRA?
Trickey, Linda (CCI-Atlanta-LD), 5/11/2021

Cross-Context Behavioral Advertising

The targeting of advertising to a consumer based on the consumer's personal information ***obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services,*** *other than* ***the*** *business, distinctly-branded website, application, or service with which the consumer intentionally interacts.*

Exceptions to Sale/Sharing

- CPRA makes opt-in to digital advertising more viable
- Service providers: permissible purposes for SP (and new “contractor” party) processing subject to change in the regs
- Opt-out Preference Signal

TL(5

Downstream Deletion "Clawback"

- CPRA amends CCPA to add that a business is required to notify "all third parties to whom the business has sold or shared … personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort."

- SP / Cs now must comply with deletion instructions and ensure their subcontractors do the same.

- There is no explicit obligation for third parties to delete information upon notice from the business or pass on deletion requests to their service providers, contractors, or third parties (i.e., downstream).

Slide 20

TL(5 Trickey, Linda (CCI-Atlanta-LD), 5/11/2021

Virginia's Consumer Data Protection Act ("CDPA")

- CCPA/CPRA and GDPR inspired, but material differences
- Timeline
  - Passed March 2, 2021
  - Findings of "working group" due November 1, 2021
  - Effective January 1, 2023
- Data Covered
  - The scope of "personal data" is more narrow than the CPRA
- No private right of action
  - Enforced only by the Attorney General

CDPA

- More limited definition of “sale”
- “Targeted Advertising” opt-out
  - definition tracks IBA – activity across time and online services
- “Sensitive data” opt-in
  - no processing without consent
- “profiling” opt-out
- Only certain rights apply to “pseudonymous data”
  - Rights: Opt-out (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
  - Does it exclude the right to obtain opt-in consent for processing of pseudonymous data that constitutes sensitive data?

Sensitive Information: California & Virginia

- What Constitutes Sensitive Personal Information?
  - CDPA
  - CPRA
- Challenges under CDPA and CPRA
  - CDPA requires consent in order to process;
  - CPRA does not require consent, but consumers can "opt out" of any use beyond a defined set of purposes (that expressly exclude online advertising);
- Note: CPRA provides an exemption for sensitive personal information that is processed for purposes other than inferring characteristics about a consumer- in the context of online advertising, would it ever be available?

Sensitive Information: California & Virginia

"Sensitive Personal Information" and Online Advertising: Some Examples

- Health condition/Pharma
- Affinity groups
- Language-based
- Location-based
- Household-level

Profiling: CPRA and CDPA and Advertising

- The CPRA requires that regulations be adopted "governing access and opt-out rights with respect to a business's use of automated decision-making technology, including profiling…."
  - "Profiling" is defined, while "automated decision-making technology" is not.
  - Without a definition of "automated decision-making technology," it is difficult to say what impact these rights will have on online advertising.
- Rights under the CDPA to opt out of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer" should not apply to online advertising.

New Laws Stricter on Vendors and Disclosures

- Under the CCPA, there are limited exceptions set forth in the Regs that are more restrictive as to what constitutes permitted Service Provider purposes that will not constitute a CCPA sale.
- The CPRA is even more restrictive than the CCPA, as is CDPA with processors.
- We will have to watch the rulemaking to learn what service providers will be permitted to do that is not necessary to provide service to the business supplying the data.
- CPRA has more definitive requirements for contracting with vendors and third parties, as does CDPA.
- CPRA adds downstream deletion claw-back.

Vendor Contracts

Privacy+ Security Forum

CCPA/CPRA TP

NOTE: Any organization that is not a SP or CT is a TP under CCPA/CPRA

A. REQUIRED IN ALL CONTRACTS in order to qualify as a TP

No required language to designate a data recipient as a third party, however, CPRA requires contracts in place with all data recipients, including with TPs.

B. Required under CPRA if B is SELLING/SHARING PI with a TP SUCH AS FOR CCBA (but would not disqualify B from being a TP if absent) (*see CPRA §.100(d)*)

(1) Specify PI is sold/disclosed for only limited and specific purposes.

(2) Requires TP to comply with CPRA and provide same level of privacy protection as required by CPRA.

(3) Grants B rights to take reasonable and appropriate steps to help ensure TP uses PI in a manner consistent with B's obligations under CPRA

(4) Requires TP to notify B if it determines it can no longer comply with its obligations.

(5) Grants B the right to upon notice (including notice under 4 above) take "reasonable and appropriate" steps to "stop and remediate" unauthorized use of PI.

CCPA/CPRA SP

A. REQUIRED IN ALL CONTRACTS to qualify as a SP (*see CPRA §.140 (ag)(1)*):
(1) process PI on behalf of B and receive PI "from or on behalf" of the B and
(2) enter into written contract with B which must prohibit:

- Selling or sharing PI**
- Retaining, using, or disclosing PI for any purpose other than for the B purposes specified in the contract, or as otherwise permitted by the CCPA/CPRA
- Retaining, using, or disclosing PI outside of the direct relationship with the B**
- Combining PI process on behalf of B with PI received from other person(s)/other interactions with the consumer (except as allowed by CCPA Regs)**

B. REQUIRED UNDER CPRA (but would not disqualify org from being deemed a SP):

- Specify PI is disclosed only for limited and specified B purposes.
- Include same requirements as those in CPRA TP list under B (2)-(5)

C. NOT REQUIRED IN CONTRACT WITH VENDOR BUT TYPICALLY INCLUDED:

(1) Grant the B rights to monitor compliance through measures such as manual reviews, automated scans, regular assessments and audits (permitted but not required under CPRA §.140(ag)(1)(D))

(2) Notify the B of subcontractors, enter into a written contract with them and ensure subcontractors are subject to the prohibitions in A.2. above (this is an obligation for SPs under CPRA §.140(ag)(2) –and for CTs under .140(j)(2) -whether it's included in the contract or not)

(3) Specifically allow SPs to (*see CCPA Regs. 999.314(c)*):

- Process PI on behalf of the B in compliance with CCPA & share with subcontractors that comply with CCPA
- Use PI for its limited internal uses to build or improve the quality of its services, subject to certain limitations set forth in the CCPA Regs.
- Use PI to detect data security incidents or protect against fraudulent or illegal activities
- Use PI to comply with law, regulatory inquiries/investigations, cooperate with law enforcement, and exercise or defend legal claims.

(4) Require SP to reasonably assist the B in responding to consumer requests and notify its own SPs or CTs to do so as well (*see CCPA Regs. 999.314(e) and CPRA §.105(c)(3)*)

CPRA Contractor

NOTE: A CT is processing PI of the B in order to provide services to an entity other than the B or the B's SPs/subcontractors to B's SPs.

A. REQUIRED IN ALL CONTRACTS in order to qualify as a CT (see CPRA § *.140(j)(1))(A)*:

(1) Enter into a contract with the organization to which the CT is providing services that includes all of the prohibitions listed in the CCPA/CPRA SP list of requirements under A.(2)

(2) Include a certification issued to the B that CT understands the prohibitions in (1) above and will comply with them (*see .140(j)(1)(B)*)

(2) Grant the B rights to monitor compliance through measures such as manual reviews, automated scans, regular assessments and audits. (permitted but not required under CPRA §.140(j)(C))

B. REQUIRED UNDER CPRA (but would not disqualify org from being deemed a CT):

Same as SPs except that rights to monitor are mandatory for CTs to qualify as such

C. NOT REQUIRED BUT TYPICALLY INCLUDED IN CONTRACTS

Same as that listed as C.(2) under CCPA/CPRA SP column. Likely would not include purposes listed in C.(3) under CCPA/CPRA SP column in CT contracts.

*CCPA = California Consumer Privacy Act; CPRA = California Privacy Rights Act; SP = Service Provider; CT = Contractor; TP = Third Party; B = Business; PI = personal information under CPRA/CDPA; CCBA = Cross-Context Behavioral Advertising; Red text = CPRA requirements beyond what CCPA currently requires; **Although not expressly required under the title of the CCPA to qualify as a SP, CCPA Regs. 999.314 arguably does require this to qualify as a SP.

Vendor Contracts

Privacy+ Security Forum

Virginia CDPA Processor

A. REQUIRED IN ALL CONTRACTS: in order to qualify as a P

NONE

B. Required under CDPA but would not disqualify org. from being a P if absent) (see 59.1-575.B.)):

(1) Clearly set forth in the contract:
- instructions for processing data;
- the nature and purpose of processing;
- the type of data subject to processing;
- the duration of processing; and
- the rights and obligations of both parties.

(2) Stipulate that P must:
- Provide necessary information to enable C to conduct and document data protection assessments;
- Ensure each person processing PD is subject to a duty of confidentiality with respect to the PD;
- At C's direction, delete or return all PD to the C as requested at the end of the provision of services, unless retention of the PD is required by law;
- Upon the reasonable request of C, make available to C all information in its possession necessary to demonstrate the P's compliance with CDPA obligations;
- Allow, and cooperate with, reasonable assessments by C or C's designated assessor; alternatively, P may arrange for a qualified, independent assessor to conduct an assessment of the P's policies and technical and organizational measures in support of its CDPA obligations using an appropriate and accepted control standard or framework and assessment procedure for such assessments;
- Provide a report of such assessment to C upon request; and
- Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of P with respect to the PD.

GDPR Processor

A. REQUIRED IN ALL CONTRACTS: in order to qualify as a P

NONE

B. Required under GDPR but would not disqualify org. from being a P if absent) (see Art. 28)):

(1) Cs must only engage Ps providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet GDPR requirements.

(2) Enter into a written contract or other legal act under EU or MS law, that is binding on P

(3) Set fort in the contract
- the subject-matter and duration of the processing,
- the nature and purpose of the processing,
- the type of PD and categories of DSs + the obligations and rights of the C

(4) Stipulate in contract that P must (see Art. 28(3)):
- processes PD only on documented instructions from C, including with re/ cross-border transfers, unless required to do so by EU or MS law to which P is subject (in such a case, P shall inform C of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest);
- ensure that persons authorised to process PD have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all security measures required pursuant to Art. 32
- taking into account the nature of the processing, assists C by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of C's obligation to DS requests
- assists C in ensuring compliance with security, breach notification, DPIAs and prior consultation obligations under Art. 32-36;
- at the choice of C, delete or return all PD to C after the end of the provision of services, and deletes existing copies unless Union or Member State law requires storage of PD;
- makes available to C all information necessary to demonstrate compliance with the obligations that apply to Ps and allow for and contribute to audits, including inspections, conducted by the C or another auditor mandated by C
- Immediately inform C if, in its opinion, an instruction infringes GDPR or other Union or Member State data protection provisions. .

(4) In re subcontractors Ps must (Art. 28 (2) & (4)):
- Obtain general or specific written authorization from C before engaging them (if general, then P must C of changes/additions/replacements and give C the opportunity to object)
- Impose on sub-processors same data protection obligations by way of a written contract providing sufficient guarantees to implement appropriate technical and organizational measures.
- If subcontractor fails to fulfil its data protection obligations, P shall remain fully liable to the C for the performance of subcontractor.

* CDPA = Virginia's Consumer Data Protection Act; GDPR = General Data Protection Regulation; P = Processor; C= Controller; DS = data subject; PD = personal data; MS = EU Member State

TL(20
SPB4

Part 3:

CPRA / CDPA Readiness

How to scope and manage a project plan to assess both current compliance and 2023 readiness, and develop workstreams to ensure remediation of current state before the end of 2021 and future state before the end of 2022.

Privacy+ Security Forum

Slide 29

TL(20 Alan to add truncated version of workstreams here
Trickey, Linda (CCI-Atlanta-LD), 5/11/2021

SPB4 What is going on here Dave with your text?
Squire Patton Boggs, 5/14/2021

TL(20
SPB4

Part 3 (a):

Project plan and workstreams

Privacy+ Security Forum

Slide 30

TL(20 Alan to add truncated version of workstreams here
Trickey, Linda (CCI-Atlanta-LD), 5/11/2021

SPB4 What is going on here Dave with your text?
Squire Patton Boggs, 5/14/2021

Things to think about

Privacy+ Security Forum

1. Segregate rights or highest requirements for all?
    - Global, regional, hybrid
        - Traveling consumers
        - 2nd class customers
2. Key issues
        - Vendors
        - Sale/share
        - Sensitive
        - AI / profiling
3. Who is responsible and accountable?
4. How do you get buy-in and participation from all stakeholders

The path forward…

- 2021 program audit and assessment;
- combined with CPRA / CDPA gap assessment;
- to scope and manage a project plan to assess both current compliance and 2023 readiness and develop workstreams to ensure remediation of current state before the end of 2021 and implementation of future state before the end of 2022.
- Assess whether you have adequate internal resources and funding or whether you need external help in order to meet the deadlines

WORKSTREAM #1: Preliminary Scoping and Information Gathering

- Task: Assess whether and to what extent the CPRA and CDPA applies to each of the entities within the organization and determine their respective classification (*e.g.*, business/controller, service provider/processor, contractor, etc.).

- Task: Gather existing privacy compliance materials developed for CCPA compliance (*e.g.*, data maps, internal policies, external privacy policy, rights requests procedures, contracts, training, etc.). Identify the gaps between any existing CCPA program and requirements of the CPRA or CDPA to inform the workstreams below.

Workstream 1 cont.

- Task: Confirm that you have a reasonable, documented basis for concluding that processing of PI is "reasonably necessary and proportionate" to achieve the purposes for which the PI is collected or processed. This data minimization principle is a requirement under the CPRA and the CDPA.

- Task (Optional): Develop a detailed work plan listing all required/optional tasks to allocate roles and responsibilities.

WORKSTREAM #2: Data Mapping

Task: Update/develop data map(s) to identify how the following categories of PI are collected, used, transferred or disclosed and for what purposes:

- *Sensitive PI*- this is a new category of PI under the CPRA and is also found in the CDPA;
- *B2B Contact PI*- the exemption under CCPA for this type of PI will expire on January 1, 2023; this type of PI is not subject to the CDPA; and
- *Employee/Contractor PI*- the exemption under the CCPA for this type of PI will expire on January 1, 2023; this type of PI is not subject to the CDPA.

Workstream 2, cont…

- Task: Determine which entities within the organization, if any, qualify for the entity-level exemptions in the CDPA for financial institutions subject to Title V of the federal Gramm-Leach-Bliley Act or for covered entities or business associates governed by the Health Insurance Portability and Accountability Act.

- Task: Identify categories of PI that may be totally or partially exempt from the CPRA or CDPA, such as PI regulated by the FCRA, GLBA and HIPAA and certain educational data.

- Task: Determine the reasonably necessary retention period, and the processing purposes, for all PI.

- Task (Optional): Conduct "training" sessions to guide internal personnel assisting with data gathering/mapping how to conduct exercise and/or prepare written guidance. If not already using a data mapping and management platform, consider doing so as part of the data mapping update.

WORKSTREAM #3: Privacy Policy (External-Facing)

Task: Update the organization's CCPA-compliant privacy policy to include certain new disclosures required by the CPRA and CDPA.

WORKSTREAM #4: Consumer Rights

- Task: Modify processes for responding to requests to exercise existing CCPA consumer rights to address new CPRA and CDPA requirements; *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 B2B contact PI and employee/contractor PI for rights requests from California residents.

- Task: Develop substantive processes to honor new consumer rights provided by the CPRA and CDPA- the rights to correct PI, to opt-out of "sharing" or "targeted advertising", to limit the use and disclosure of "sensitive" PI and to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

- Task: Develop substantive processes to comply with new CPRA regulations (once issued) granting rights to access and opt-out of automated decision-making.

WORKSTREAM #5: Privacy Impact Assessments and Cybersecurity Audits

Privacy+ Security Forum

- Task: **CPRA** requires businesses that engage in **high-risk processing activities** to perform privacy impact assessments that must be filed with the California Privacy Protection Agency. The specific requirements, including what constitutes high-risk processing activities, are to be developed through rulemaking. Similarly, the **CDPA** requires a controller to conduct a data protection assessment of **certain processing activities**, including targeted advertising, the sale of PI, the processing of sensitive PI and any other processing activities that present a **heightened risk of harm** to consumers. The Virginia Attorney General may request such assessments, but controllers are not required to submit them to the Attorney General absent a request.

- Task: CPRA requires businesses that engage in **high-risk processing** activities to perform cybersecurity audits, with the specifics to be developed through rulemaking.

- Task: Assess data security and remediate vulnerabilities. If this is done at direction of outside counsel there is a basis for taking the position that the work and work product are privileged.

- Task (Optional): **Consider a privacy impact assessment program for all PI processing**, to help meet purpose, proportionality, data minimization and other requirements and reduce risks.

WORKSTREAM #6: Vendor/Supplier Contracts

- Task: Review and, as necessary, amend/execute (upstream and downstream) contracts to ensure compliance with the CPRA and CDPA (mainly prohibiting secondary uses, allowing for audits and requiring assistance honoring consumer rights) and to avoid transfers of PI being considered a "sale" under the CPRA and to address expanded deletion requirements.

- Task: Identify any (upstream and downstream) contracts that involve the processing of "de-identified" data to include new contract terms required by the CPRA and CDPA.

- Task: Prepare/update template agreements with appropriate CPRA and CDPA language.

- Task (Optional): Prepare/update any contracting "playbooks" with key provisions, fallback language, and explanations reflecting new CPRA and CDPA requirements.

WORKSTREAM #7: Review/Develop/Update Policies (Internal-Facing)

- Task: Update/develop policies to support CPRA and CDPA compliance, including privacy policy, consumer rights procedures, privacy impact assessments, audit functions, data retention policy and schedules, routine updates (to data map, privacy policy, etc.), retention limitations, and training and record keeping requirements and best practices.

- Task (Optional): Review Written Information Security Program plan, including incident response plan.

WORKSTREAM #8: Training

- Task: Update training materials for employees with specific responsibilities for handling consumer requests or compliance to reflect new CPRA and CDPA requirements. Consider broader training, especially regarding privacy impact assessments and privacy-by-design.

- Task (Optional): Update any explanatory business guidance documents on critical aspects of the CPRA or CDPA (*e.g.*, definition of "sensitive" PI, what constitutes a "sale/share," activities that may be impermissible "discrimination," service providers/processors vs. contractors vs. third parties, de-identification requirements, comparisons to CCPA, etc.).

WORKSTREAM #9: Other Security and Compliance (Optional but recommended)

- Task (Optional): Review and update Written Information Security Program plan, including incident response plan, acceptable use plan, and vendor management program.

- Task (Optional): Review and update security safeguards to meet California's "reasonableness" standard (which will avoid statutory damage claims for a data breach).

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

Part 3(b):
Planning for the future – consider using the NIST Privacy Framework

Privacy+ Security Forum

Leveraging the NIST Privacy Framework to Mature Your Privacy Program

Privacy+ Security Forum

Sample of 10 NIST Subcategories Mapped to GDPR, HIPAA, CCPA and other pending State Laws
ID.IM-P1: Systems/products/services that process data are inventoried.
ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
CT.DM-P2: Data elements can be accessed for transmission or disclosure.
CT.DM-P4: Data elements can be accessed for deletion.
CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
PR.DS-P2: Data-in-transit are protected.
PR.DS-P5: Protections against data leaks are implemented.

State Level Mapping to NIST Privacy Framework

M = Subcategory can be mapped to the law						S = Subcategory cannot be directly mapped to a law and is a noted as a supporting activity				
GDPR	**HIPAA**	**CA**	**WA**	**MS**	**NH**	**IL**	**MD**	**MS**	**NY**	**VA**
M	M	S	M	S	S	M	S	S	S	M
M	M	M	M	M	M	M	M	M	M	M
S	S	S	S	S	S	S	S	S	S	S
M	M	M	S	M	M	S	M	M	M	S
M	M	S	M	S	S	M	S	S	S	M
M	M	M	M	M	M	M	M	M	M	M
M	S	M	M	M	M	M	M	M	M	M
M	S	S	M	S	S	M	S	S	S	M
M	M	M	M	M	M	M	M	M	M	M
M	S	M	M	M	M	M	M	M	M	M

Leveraging the NIST Privacy Framework to Mature Your Privacy Program

Privacy+ Security Forum

- Start project with assessment using NIST Privacy Framework as baseline
- Divide and conquer - Assign functional area owner to each subcategory control:

- Document current state, proposed future state, and in the future, document the then current state

TL(22

Part 3(c):
Retention -- Building an Operating Model for Defensible Disposition

Slide 47

TL(22 moving some of David's slides to Part 3

Trickey, Linda (CCI-Atlanta-LD), 5/11/2021

Data Retention Text Similarities – GDPR v CPRA

GDPR Article 13: the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: 1) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;…

GDPR Article 30: "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility…That record shall contain all of the following information: 1) where possible, the envisaged time limits for erasure of the different categories of data"

CPRA: 1798.100 "A business that controls the collection of consumer's personal information shall, at or before the point of collection, inform consumers as to: the length of time the business intends to retain each category of personal Information, including sensitive personal Information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal Information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

Records Retention and Defensible Data Disposition

Workstream	Key Activities				
Data Inventory	Review existing artifacts and conduct discovery interviews with key functional leads	Design and configure technology in coordination with other workstreams	Conduct Pilot data mapping interviews	Conduct Data mapping surveys and risk analysis	Maintain and refresh the Data Inventory
File Analysis	Install and configure file analytics solution	Pilot file analytics on a subset of unstructured content	Identify data risks and provide recommendations for remediation	Transition file analytics to operations at scale	Support operations and maintenance of file analytics platform
Records Retention	Develop or enhance records management policy	Link data inventory to records retention schedules	Develop change management collateral including training materials	Deliver records management training to functional areas	Engage with functional areas on a rolling basis to troubleshoot and assess compliance
Data Disposition	Develop target operating model for defensible data disposition	Implement control documentation to support defensible disposition	Pilot target operating model for three applications	Refine target operating model based on pilots	Scale defensible disposition operating model

Purpose and Proportionality Limitations

- **CPRA introduces purpose limitation provisions**
  - Prohibit collecting additional categories of PI or using PI collected for additional purposes *that are incompatible with disclosed purpose for which the PI was collected*
  - Collection, use, retention, and sharing of PI must be reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed, or for another disclosed purpose that is compatible with context in which PI was collected

- **Implications**
  - Limits a business' ability to make new use cases of PI and retain PI longer than necessary for express collection purpose
  - Practically requires PIAs, good data inventories, robust records retention program, and defensible destruction protocol

Potential Disclosure Format of Privacy Notice with Retention Periods

Company X California Privacy Notice

….

a) Collection, Purpose, Retention and Sharing

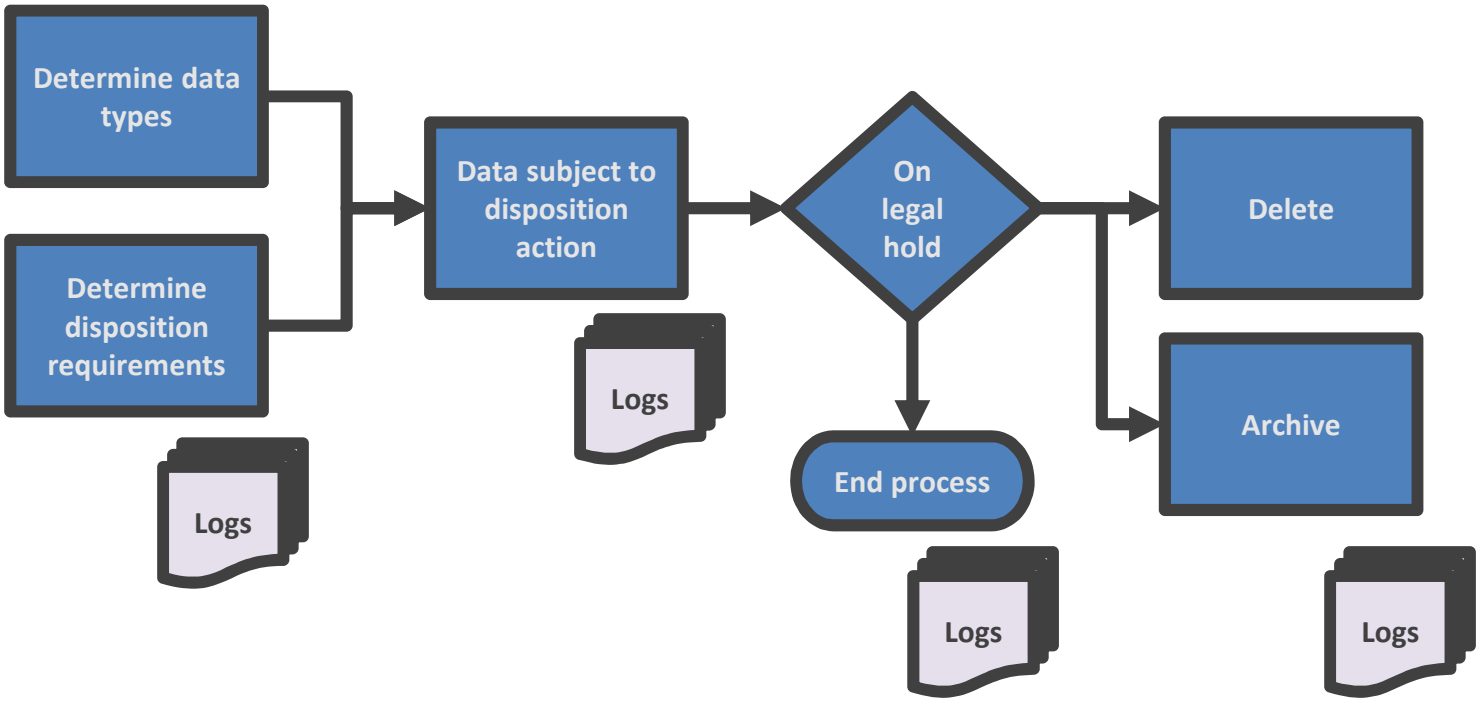
Category of PI	Purposes	Retention Period
Identifiers - Name, postal address, Internet Protocol address and email address.	1. Performing Services 2. Short-term Transient Use (e.g., to serve contextual ads)	1. For as long as services are performed, thereafter 4 years for records keeping or as otherwise required by law or legal process 2. Only as needed to complete the transient use, typically less than a day
Geolocation Data - Approximate physical location	?	?
Sensory Data - Audio recordings of customer support calls.	?	?

Vision for a Defensible Disposition Operating Model

Policy-driven, repeatable approach – designed by humans, assisted by technology

- Disposition is an “if then” activity when done correctly – repeatable and predictable
- Disposition is a process in support of a policy – any exceptions should be handled at the policy level (i.e., as a deviation from corporate policy), not at the process level (i.e., as an approval to proceed)
- The goal is zero human decision-making when executing disposition actions – all meaningful decisions should have already been made when the process was defined, not at run time
- Defensible does not mean perfect – it means consistent, documented, and repeatable

Defensible Disposition Top-level Process



Determine Data Types

1. Determine what kind of data the application holds
    - Data Classification – public, internal, confidential, highly confidential
    - Record types
    - Personal Information – consumer/employee data
2. Leverage existing information
    - Enterprise data map
    - CMDB
    - Application inventory
    - Records retention schedule
    - Information Security risk assessment, audit, etc.
    - Privacy Impact Assessment, audit, etc.
3. Conduct interviews/surveys to close gaps in existing information
4. Utilize data analytics tool(s) to interrogate the data to help determine what kind of data the application holds
5. Complete **System-level Data Type Catalog**

Determine Disposition Requirements

1. Determine the compliance obligations in force on the application
    - Regulations (e.g., CCPA, GDPR, GLBA)
    - Standards (e.g., NIST, ISO)
    - Audit
    - Contractual/Third-party
2. Leverage existing information about what disposition requirements are needed to meet the compliance obligations
    - Records retention schedule
    - Information Security risk assessment, audit, etc.
    - Privacy Impact Assessment, audit, etc.
    - Regulatory crosswalk
3. Conduct interviews/surveys to close gaps in existing information
4. Complete **Disposition Requirements Documentation**

Data Subject to Disposition Action

1. Cross reference **System-level Data Type Catalog** and **Disposition Requirements Documentation** to generate a list of data types subject to disposition action (delete or archive)
2. Develop a report of all data for each data type subject to disposition action
3. Leverage one or more of the following as needed
    - Native application functionality
    - Third-party data management tools
    - Ad hoc methods (e.g., scripts, queries, etc.)
4. Document all assumptions, search criteria, rules/logic, etc. as well as results
5. Complete **Data Subject to Disposition Action List**

On Legal Hold

1. Cross reference **Data Subject to Disposition Action List** with information about active legal holds to determine data eligible for disposition action (i.e., what data subject to disposition action is not subject to legal hold)
2. Some considerations
   - •Does Legal use software to manage holds?
   - •Are legal holds placed and released systematically?
   - •Does Legal hold in place or by collection?
   - •Are legal holds applied by system/repository, custodian, or keyword (or some combination)?
3. Complete **Data Eligible for Disposition Action List**

Delete or Archive (1 of 2)

1. Execute the actions included in the **Data Eligible for Disposition Action List**
2. Leverage one or more of the following as needed for disposition
    - Native application “hard delete” functionality
    - Third-party forensic deletion tools (e.g., SDelete, Eraser)
    - Third-party data management tools (e.g., Informatica)
    - Third-party archiving/migration tools
    - Third-party archive platforms
    - Ad hoc methods (e.g., scripts, queries, etc.)

Delete or Archive (2 of 2)

3. Some considerations
    - Application level and enterprise “recycle bin” usage – need to account for when data is emptied from these
    - Enterprise archiving and business continuity and disaster recovery (BC/DR) practices – need to account for how application data is replicated for both archiving and BC/DR
    - Ensure that the integrity of metadata is maintained during and after the archiving process
4. Complete the **Disposition Action Results Report**

Part 4:

Use Cases and Discussion

Privacy+ Security Forum

Agent Requests, Due Diligence, CA AG Notice Letters and Class Actions

Privacy+ Security Forum

Large Number of Autogenerated Consumer Requests

Hello [ ],

My name is [ ], and I hereby request to erase all personal data that you hold about me.

Please send me an email confirmation of the complete and permanent erasure of the personal data once you have completed the erasure process.

My personal details are:

* Name: [ ]
* Email: [ ]

As evidence of my interaction with your company, I received an email on [ ] that indicates that you are holding personal data about me.
Companies: For additional context to complete this DSR, visit the secured Mine portal.

Thanks,
[ ]

Powered by Mine®

Mine Case: [ ]

Due Diligence – Debt Refinancing and/or Seed Stage Financing

- **Lender and Venture Funding Due Diligence is highly focused on data privacy compliance.**
- **Real-world example questions from lender:**

1. Provide an **overview** of the company's privacy compliance program
2. Provide approved and actual **privacy program budgets** for last three years
3. For the data entered into the Company's products by customers does the Company have visibility and **access** to this data?
4. Identify the extent to which the Company hosts customer data, whether on its **cloud instance or on local servers**.
5. Please describe the steps the Company has taken to ensure compliance with applicable marketing laws (e.g. **TCPA, CAN-SPAM**).

Due Diligence – Debt Refinancing and/or Seed Stage Financing

- **Real-world example questions from lender (continued):**

  6. Please describe the steps taken by the Company following **Brexit**

  7. Please provide copies of all internal policies that are relevant to its data protection compliance program, including any employee privacy policy, **record of processing**, **retention and deletion polices**, information security policy, complaint response policy, policy for responding to data subject requests, data protection impact assessments,…

  9. Provide details of the **diligenc**e that the Company carries out **on third party service providers**…and confirm whether the Company's data processor agreements include the GDPR-mandated **contractual provisions under Article 28 GDPR** (if applicable).

Lessons Learned from AG's CCPA Notice of Noncompliance Letters

- Several hundred letters have been sent?

    1. Very Specific
    2. Chart or No Chart?
    3. GDPR compliant notice <> CCPA compliant notice
    4. Response letter
    5. "Do not sell"
    6. Loyalty programs / financial incentives

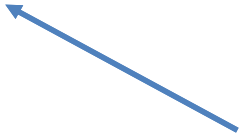
- Tip: Need to be mindful or incremental state requirements such as Virginia assuming the Virginia AG follows a similar approach and ensure privacy notices are updated accordingly.

Top 10 industries targeted by plaintiffs for CCPA violations

Privacy+ Security Forum

Based upon a review of federal class actions filed in 2020 that referenced either "CCPA" or "California Consumer Privacy Act," the following are the top industries that attracted CCPA-related class action filings:

Industry	Percentage of Class Actions
Health care & Health Services	18.92%
Financial Services	10.81%
Technology – Communication	9.46%
Technology – Software	9.46%
Hospitality	8.11%
Restaurants, Food & Beverage	5.41%
Retail	5.41%
Debt Collection	4.05%
Insurance	4.05%
Consumer Goods	2.70%



What about the HIPAA and GLBA exemption?

Source: Lexology.com. David Zetoony. May 6, 2021

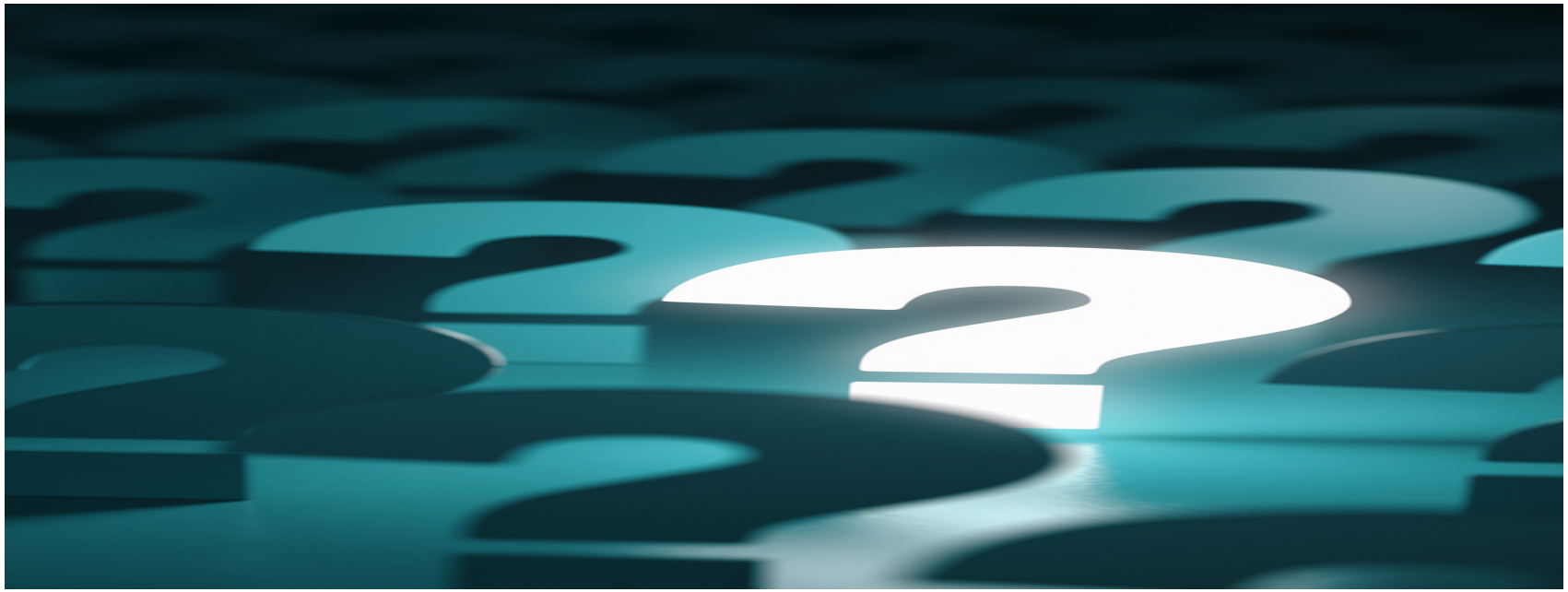
Litigation Regarding a Defendant's Failure to Maintain Reasonable Security

- CCPA's private right of action in a nutshell.
    - California residents can file suit for "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of ***the duty to implement and maintain reasonable security procedures*** and practices appropriate to the nature of the information to protect the personal information."
- Statutory liquidated damages ranging from $100-$750 per consumer, per incident.
- The **CPRA:**
    - includes an explicit requirement for businesses that collect consumers' personal information to implement reasonable security procedures and practices;
    - Clarifies that you can't "cure" and avoid statutory damages by fixing an unreasonable inadequacy post-breach.

What is reasonable security?

- Term not defined by statute.
- 2016 California Data Breach Report (published by former California AG and current VP Kamala Harris).
  - CIS Top 20
    - Categorical
    - Many more subcategories

Questions?



Questions + Contact

Alan Friel
Deputy Chair
Global Data Practice
Squire Patton Boggs
T +1 213 689 6518
alan.friel@squirepb.com

David Manek
Senior Managing Director
Ankura Consulting
T +1 312 583 6841
david.manek@ankura.com

Linda Trickey
Assistant General Counsel,
Privacy & Security
Cox Communications
linda.trickey@cox.com