California Consumer Privacy Act

New Consumer Rights – New Business Obligations

October 25, 2018

Presented by :

Deborah Thoren-Peden, Partner
Catherine Meyer, Senior Counsel
Pillsbury Winthrop Shaw Pittman LLP

Alma Angotti, Managing Director
Joseph Campbell, Director
Kathryn Rock, Director
Brian Segobiano, Associate Director
Navigant

NAVIGANT

Agenda

- Background
- Key Definitions
- New Consumer Rights
- New Business Obligations
- Exemptions
- Enforcement

NAVIGANT pillsbury

Key Definitions

- Consumer
  - Any natural person residing in California
  - No requirement for a business or transactional relationship
  - No limitation of coverage to personal, family or household purposes
  - “Resident” means every individual who is in the State for other than a temporary or transitory purpose, and every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents. 18 CA Code of Regulations 17014.

NAVIGANT pillsbury

Key Definitions

- Covered Business
  - Any for-profit legal entity that collects Consumers' Personal Information
  - Includes entity operated for the profit or financial benefit of its shareholders or other owners
  - Determines the purpose and means of processing Personal Information
  - Does business in California
  - Either has $25 million annual gross revenue, process personal information of at least 50,000 Consumers or derives 50% of its annual revenue from selling Consumer information.

NAVIGANT pillsbury

Key Definitions

- Personal Information
  - Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - Includes: real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers, commercial information, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies, biometric information, electronic network activity information, geolocation data, professional or employment-related information, and inferences drawn from any of the information identified in this subdivision to create a profile about a consumer.

NAVIGANT pillsbury

Key Definitions

- Collection of information
  - Buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means
  - Includes receipt from consumer directly or indirectly or by observation
- Sale of information
  - Any form of disclosure, in any format, to another covered business (or any other third party) in exchange for money or other valuable consideration
  - Excludes information provided to service providers who are not permitted to use information except to perform the contracted business service.

NAVIGANT pillsbury

New Consumer Rights

- Right to request information about the business's collection of the consumer's personal information and to receive a portable copy of such personal information
- Right to request information pertaining to the sale or disclosure of the consumer's personal information
- Right to request deletion of the consumer's personal information held by the business
- Right to opt out of the business's sale of the consumer's personal information
- Right not to be discriminated against because of choices regarding her/his personal information

NAVIGANT pillsbury

KEY CHALLENGES AND RECOMMENDATIONS

While organizations that have been focusing on General Data Protection Regulation (GDPR) compliance will be able to leverage some of that work for CCPA compliance efforts, there are still several actions required to comply with CCPA. The risk of non-compliance is significant and fines for each violation can be up to $7,500.

Establish Governance Structure and Develop Plan

Key Challenges

- **Resource Constraints**: Skillsets, availability
- **Data Requirements / Time Constraints:** 12 months' worth of data required on effective date of January 1, 2020; data needs to be retained beginning January 1, 2019

Key Activities

- **Create Governance Structure:** Update existing or establish new data privacy governance structure / committees to develop and implement strategy for compliance with CCPA, including potential inclusion of Chief Privacy Officer role
- **Determine Impacted Business Lines:** Identify all impacted business lines (e.g., Marketing, Sales, IT / MIS, Legal, Compliance)
- **Develop Plan:** Create high-level plan with milestones and timelines, including appropriate reporting mechanisms as well as reporting to management and the Board
- **Prepare Communication Plan:** Develop plan with endorsement from the C-suite on down throughout the company and to investors / shareholders. This will help set the "tone at the top / culture of compliance." This should also include a reporting mechanism for employees to identify and report potential violations with the company's CCPA program, either through supervisors or established company hotline / tip line

NAVIGANT pillsbury

KEY CHALLENGES AND RECOMMENDATIONS (*Cont.*)

In order to develop and implement policies and procedures to comply with CCPA requirements, businesses should assess the current state of its data privacy program, taking care to consider all sources of covered personal information, including potential physical data records.

Assess Current State

Key Challenges

- **Scope of Covered Data:** Identification of all personal data stored, sold, and shared publicly
- **Data / Systems Limitations:** Retention / archive capabilities, ability to identify / match consumer, ability to confirm consumer age

Key Activities

- **Assess Current State:** Identify and re-examine current data privacy policies and procedures (P&P):
  - Notifications and disclosures
  - Verifying requests
  - Responding to requests
    - Response time
    - Number of requests
  - Data deletion
  - Opt-outs and opt-ins
  - Prohibition of discrimination
- **Enhance Plan:** Considering the results of the current state assessment, adjust / modify plan to add more specificity to the required milestones and timelines

NAVIGANT pillsbury

KEY CHALLENGES AND RECOMMENDATIONS (*Cont.*)

When addressing laws that regulate how organizations collect and use personal data, it is critical to have an understanding of what information is collected and how that proliferates both within and outside of the organization.

Build / Develop Data Inventory / Registry

Key Challenges

- **Data Visibility**: Undocumented processes (Shadow IT) or unknown key processing attributes
- **Data Transfers**: Volume and speed at which data moves into, throughout, and externally from an organization

Key Activities

- **Develop a Data Inventory / Registry:** Data will likely be contained in multiple data sources (including hard copy documents), and an inventory / registry will allow for all sources to be available for requests. Inventory of processes and key attributes:
  - Business or legal purpose for the processing
  - Individuals impacted (customers, employees, vendors, etc.)
  - Whether individuals were notified or provided consent
  - Internal systems or third parties who supply, receive, or access the data (Data Mapping)
  - Secondary uses of the data
  - Data security measures
  - Retention period
- **Maintain the Data Inventory:** Deploy the inventory in a manner where it can continue to be updated and added to over time by the business owners. Options may include internal governance tools (e.g., SharePoint) or third party software tools

NAVIGANT pillsbury

KEY CHALLENGES AND RECOMMENDATIONS (*Cont.*)

In addition to implementing and executing new processes, businesses should also incorporate these new processes into its existing risk and controls framework and related assessments.

Develop / Update P&P and Develop / Implement Processes and Controls

Key Challenges

- **New Process Risks:** Updated processes may lead to unforeseen risks that require identification and new controls

Key Activities

- **Develop / Implement Processes / Controls:** Develop and implement processes, systems, and controls, including updating P&P, in all applicable business units
  - Response to verified consumer requests, including timeliness of responses
  - Data deletion
  - Number of verified consumer requests in 12-month period
  - Confirmation of consumer age
  - Length of opt-out period
- **Test Processes / Systems / Controls:** Identify risks and verify that newly implemented processes / systems / controls are functioning as expected and / or identify findings / recommendations, focusing on accuracy, completeness, and timeliness of responses to consumer requests
- **Conduct Ongoing Periodic Risk Assessment:** Establish ongoing mechanism to identify and manage risk and to test controls, including development of monitoring and reporting to identify instances of non-compliance

NAVIGANT pillsbury

KEY CHALLENGES AND RECOMMENDATIONS (*Cont.*)

As businesses fully implement these processes and train their staff, they should continue to track changes / updates to the regulation and incorporate into its change management process as required.

Training

Key Challenges

- **Identification of Appropriate Training Audience:** Requirements surrounding training are broad and require training for "all individuals responsible for handling consumer inquiries about the business's privacy practices"

Key Activities

- **Develop Training Program:** Create / update training programs for new processes, with a timeline for execution, including addition into annual or new employee curriculums
- **Identify Trainers:** Determine who will train impacted company personnel on the law and complying with it
- **Hold Training Sessions:** Hold workshops to train workforce on new privacy requirements, policies, procedures, processes, systems, and controls
- **Continual Refresh:** Monitor and disseminate updated trainings as required, as well as on a periodic basis, based on any changes to the regulations and / or P&P updates; also promotes culture of privacy compliance through periodic and consistent employee training
- **Enforce Standards through Disciplinary Guidelines:** Publicize and enforce disciplinary actions for any identified misconduct as dictated by communicated guidelines, which will further culture of compliance

NAVIGANT pillsbury

New Consumer Rights

- Right to request information about the business's collection of the consumer's personal information and to receive a portable copy of such personal information, including
  - The categories *and specific pieces* of the consumer's personal information that have been collected;
  - The categories of sources from which the personal information is collected;
  - The business purpose for collecting or selling the personal information; and
  - The categories of third parties with whom the business shares the information.

NAVIGANT pillsbury

KEY CONSIDERATIONS

Right to Request Information about Collection of Personal Information and Receive Portable Copy of Personal Information

12 months' worth of data required on effective date of January 1, 2020

Retention needs to begin by January 1, 2019

Data Requirements

Responses to Consumers

Process and controls should be put in place to ensure that responses to consumer requests occur within 45 days

Focus Areas

All data sources should be considered, including hard copy documents

Data Sources

Number of Consumer Requests

Processes and controls should be put in place to track the number of requests by consumer (only need to respond to 2 per consumer in 12 month period)

NAVIGANT pillsbury

New Consumer Rights

- Right to request information pertaining to the sale or disclosure of the consumer's personal information, including
  - The categories of personal information sold;
  - The categories of third parties that received the personal information; and
  - The categories of personal information that have been disclosed for a business purpose

NAVIGANT pillsbury

KEY CONSIDERATIONS

Right to Request Information Pertaining to Sale / Disclosure of Personal Information

12 months' worth of data required on effective date of January 1, 2020

Retention needs to begin by January 1, 2019

Data Requirements

Responses to Consumers

Process and controls should be put in place to ensure that responses to consumer requests occur within 45 days

Focus Areas

All sources of potential sale or disclosure of personal information must be considered and tracked, including what information provided to each party

Sources of Data Sold / Disclosed

Number of Consumer Requests

Processes and controls should be put in place to track the number of requests by consumer (only need to respond to 2 per consumer in 12 month period)

NAVIGANT pillsbury

New Consumer Rights

- Right to request deletion of the consumer's personal information held by the business
- Exceptions:
  - Information to enable solely internal uses that are reasonably aligned with the expectations of the consumer;
  - To comply with a legal obligation;
  - Where retention is necessary to complete a transaction for the individual or reasonably anticipated in the context of a business's ongoing relationship with the consumer;
  - For security reasons such as to protect against fraudulent or illegal activity or to prosecute such activity

NAVIGANT pillsbury

KEY CONSIDERATIONS

Right to Request Deletion of Personal Information Held by Business

Personal information that is exempt from deletion requests should be clearly marked in data inventory / registry

Segregation of Information Exempt from Deletion

Oversight of Service Providers

Processes and controls need to be put in place to ensure service providers also delete requested information

Focus Areas

Data sources containing archived / historic information should be included in deletion requests, including those of service providers

Historic Information

Verification of Deletion

Processes and controls should be put in place to verify the appropriate deletion (and retention of exempt information) from both the business and its service providers

NAVIGANT pillsbury

New Consumer Rights

- Right to opt out of the business' sale of the consumer's personal information.
  - A business may not request that a consumer who has opted out re-authorize the sale of their personal information for at least 12 months after having opted out.

NAVIGANT pillsbury

KEY CONSIDERATIONS

Right to Opt Out of Sale of Personal Information

Processes and controls should be put in place to determine / confirm a consumer's age if a business does not already have this information

Consumer Age Verification

Exclusion of Information Exempt from Opt Out

Personal information that is exempt from opt out requests should be clearly marked in data inventory / registry

Focus Areas

Processes and controls should be put in place to confirm automatic opt-out of consumers under 16 and affirmative opt-ins

Affirmative Opt-In for Consumers Under 16

Honoring Opt Out Requests

Processes and controls should be put in place to process opt out requests, as well as to honor requests for at least 12 months before re-requesting sale / disclosure of personal information

NAVIGANT pillsbury

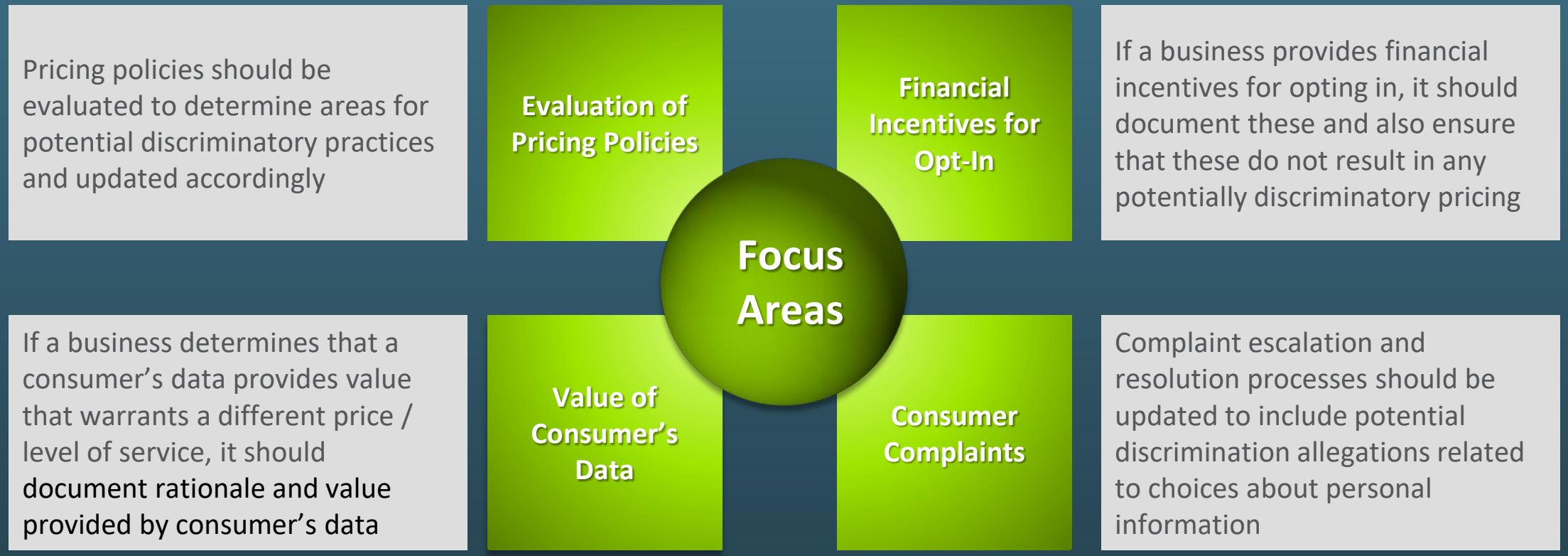
New Consumer Rights

- Right not to be discriminated against because of choices regarding her/his personal information, including:
  - Denying goods or services to such consumers;
  - Charging different prices or rates for goods or services (including through the use of discounts or other benefits or penalties) to such consumers as compared to consumers who have not exercised their rights; or
  - Providing a different level or quality of goods or services to such consumers as compared to consumers who have not exercised their rights.

NAVIGANT pillsbury

KEY CONSIDERATIONS

Right Not to be Discriminated Against Due to Choices About Personal Information



NAVIGANT pillsbury

New Business Obligations

New disclosures at point of collection or in the privacy policy

- Provide at least two methods for submitting requests for disclosure (toll free phone number and website address)
- Privacy policy disclosures
  - Categories of personal information being collected, sold or disclosed during the prior 12 months,
  - Sources from which the information is collected,
  - Categories of third parties with whom the information is shared,
  - All purposes for which the information is used or a statement that personal information has not been sold or disclosed during the prior 12 months. (Additional notice is required before using for new purpose.)
  - Description of opt-out rights
  - Update privacy policy annually
- Include website home page link: “Do Not Sell My Personal Information” linking to a page enabling an opt-out.

NAVIGANT pillsbury

New Business Obligations

On-demand Obligations

- Must provide 2 channels for making requests for disclosure (Toll-free telephone and webpage)
- Must respond within 45 days (can be extended for 45 more days)
- Must verify identity of requesting consumer
- Consumers may only make requests twice a year

NAVIGANT pillsbury

New Business Obligations

On-Demand Obligations include responding to

- Request for disclosure of personal information collected
- Request for deletion of personal information
- Request to opt-out of sale of personal information

NAVIGANT pillsbury

Practical Implications

- Review and update privacy policy
- Implement procedures for verifying requesting consumers
- Implement operations to be able to identify and locate consumer information so that disclosures can be made within 45 days
- Develop means to provide specific information disclosures electronically
- Implement Do-Not-Sell protocols for opting out (or opting-in for 13-16 year olds)

NAVIGANT pillsbury

Exemptions

- Health information collected under and protected by California's Confidentiality of Medical Information Act or HIPAA,
- Sale of information to or from a consumer reporting agency as permitted by the Fair Credit Reporting Act as amended,
- Information collected through activities taking place wholly outside of California,
- Information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act**, or
- Information collected, processed, sold or disclosed pursuant to the Drivers Privacy Protection Act of 1994 (18 U.S.C. § 2721)**

**Exemption does not apply to private right of action for unauthorized access resulting from failure to comply with statutory duty to protect personal information.

NAVIGANT pillsbury

Regulations and Enforcement

- Attorney General is required to promulgate regulations no later than July 1, 2020. (per 9/7/18 Amendment)
- Consumer rights cannot be waived.
- Violation occurs if business fails, within 30 days after being notified of noncompliance, to cure the noncompliance.

NAVIGANT pillsbury

Regulations and Enforcement

- Limited private right of action for security breaches
  - May sue to recover damages between $100 and $750 or actual damages, injunctive and declaratory relief
  - Limited to actions arising from unauthorized access to unencrypted or unredacted personal information resulting from the business' violation of its statutory duty to implement and maintain reasonable security measures to protect personal information
  - Currently required to notify AG within 30 days of filing
- General enforcement only by Attorney General
  - AG can bring enforcement actions starting 6 months after regulations are promulgated.
  - Penalties of $2500 per violation, up to $7500 for intentional violations.

NAVIGANT pillsbury

For those attorneys participating, please note the following code on our attendance sheet:

CLE VERIFICATION CODE:

2018-089

NAVIGANT pillsbury

Questions?

NAVIGANT pillsbury

Presented by

pillsbury & NAVIGANT

CATHERINE MEYER
Senior Counsel
213-488-7362
Catherine.meyer@pillsburylaw.com

ALMA ANGOTTI
Managing Director
(202) 481-8398
alma.angotti@navigant.com

KATHRYN ROCK
Director
(202) 973-6541
krock@navigant.com

DEBORAH THOREN-PEDEN
Partner
213-488-7320
deborah.thorenpeden@pillsburylaw.com

JOSEPH CAMPBELL
Director
(202) 973-4595
joseph.campbell@navigant.com

BRIAN SEGOBIANO
Associate Director
(312) 583-2749
brian.segobiano@navigant.com

NAVIGANT pillsbury