Navigating a Watershed Privacy Law: California Consumer Privacy Act

UNC Festival of Legal Learning
February 8, 2019

Corey Dennis, CIPP/US, CIPP/EU
Director of Privacy & Counsel
Pharmaceutical Product Development
corey.dennis@ppdi.com

Elizabeth Johnson
Partner
Wyrick Robbins
ejohnson@wyrick.com

PPD®

Wr
wyrickrobbins

[ELEMENTAL TO SUCCESS]

California Consumer Privacy Act of 2018

ORIGIN STORY

Origin Story

- Enacted June 2018
- Compromise bill to avoid ballot initiative (California Consumer Right to Privacy Act of 2018)
- Supported by $2.35M from real estate developer Alastair Mactaggart
- Opposed by Committee to Protect California Jobs with $200K donations from each of
  - Facebook
  - Google
  - Verizon
  - Comcast
  - AT&T

Future of U.S. privacy?

"I have been tracking ballots for 5 years . . .

Anytime there is a ballot measure in California, it is a bellwether for the nation."

- Josh Altic, Ballotpedia's project director for ballot measures project

PPD®

wyrickrobbins

Breach law trends

	2003: California	2018: 50 states + international + federal + local
Breach	Unauthorized acquisition	Unauthorized… • acquisition • access • use
Timing	"Without unreasonable delay"	• "without unreasonable delay" • "most expedient time possible" • "as expeditiously as practicable" • specific deadlines (10-60 days) (GDPR=72hrs)
Data	Name plus: • SSN • DL# • Financial account number	• Name not always required • SSN, DL#, state-issued ID, passport, military ID, TIN • Financial account info, credit/debit card number, checking account, savings account, any other info to access financial resources • Health info or health insurance info • Biometrics • Credentials for online account • Digital signature • Employee ID# • DOB • DNA • Parent's surname prior to marriage • Info collected by automated license plate recognition • Etc.…

California Consumer Privacy Act of 2018

KEY CONCEPTS

PPD®

wyrickrobbins

Territorial Reach

- Applies to for-profit entities that collect consumers' personal information and "alone or jointly with others determines the purposes and means of processing,"
- "Does business" in the State of California; and
- Satisfies any one of the following thresholds:
  - has more than $25M in annual gross revenues; or
  - annually receives, buys, or shares personal information of 50,000 or more "consumers, households or devices"; or
  - derives 50% or more of its annual revenues from selling consumers' personal information.

Other Businesses / Nonprofits

- Any entity that controls or is controlled by a business [covered by CCPA] and that shares common branding
- "Control" means
  - ownership of, or the power to vote, more than 50% of outstanding shares
  - control in any manner over the election of a majority of directors or similar function
  - power to exercise controlling influence
- "Common branding" means shared name, servicemark, or trademark

PPD®

wyrickrobbins

Application

- "Consumer" means a natural person who is a California resident
  - Employees are not exempted

- "Collect" means "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."

PPD®

wyrickrobbins

Personal Information

- real name
- alias
- postal address
- unique personal identifier
- online identifier
- Internet Protocol address
- email address
- account name
- social security number
- driver's license number
- passport number
- signature
- physical characteristics/description
- telephone number
- insurance policy number
- education status/history
- employment
- employment history
- bank account number
- credit card number
- debit card number
- financial information
- medical information
- health insurance information.
- protected classifications (race, ethnicity, sex, age, sexual orientation, etc.)
- commercial information
- personal property
- products or services (purchased or considered)
- other purchasing or consuming histories or tendencies
- biometric information
- Internet or other electronic network activity information
- browsing history
- search history
- interaction with an Internet Web site, application, or advertisement
- geolocation data
- audio, electronic, visual, thermal, olfactory, or similar information

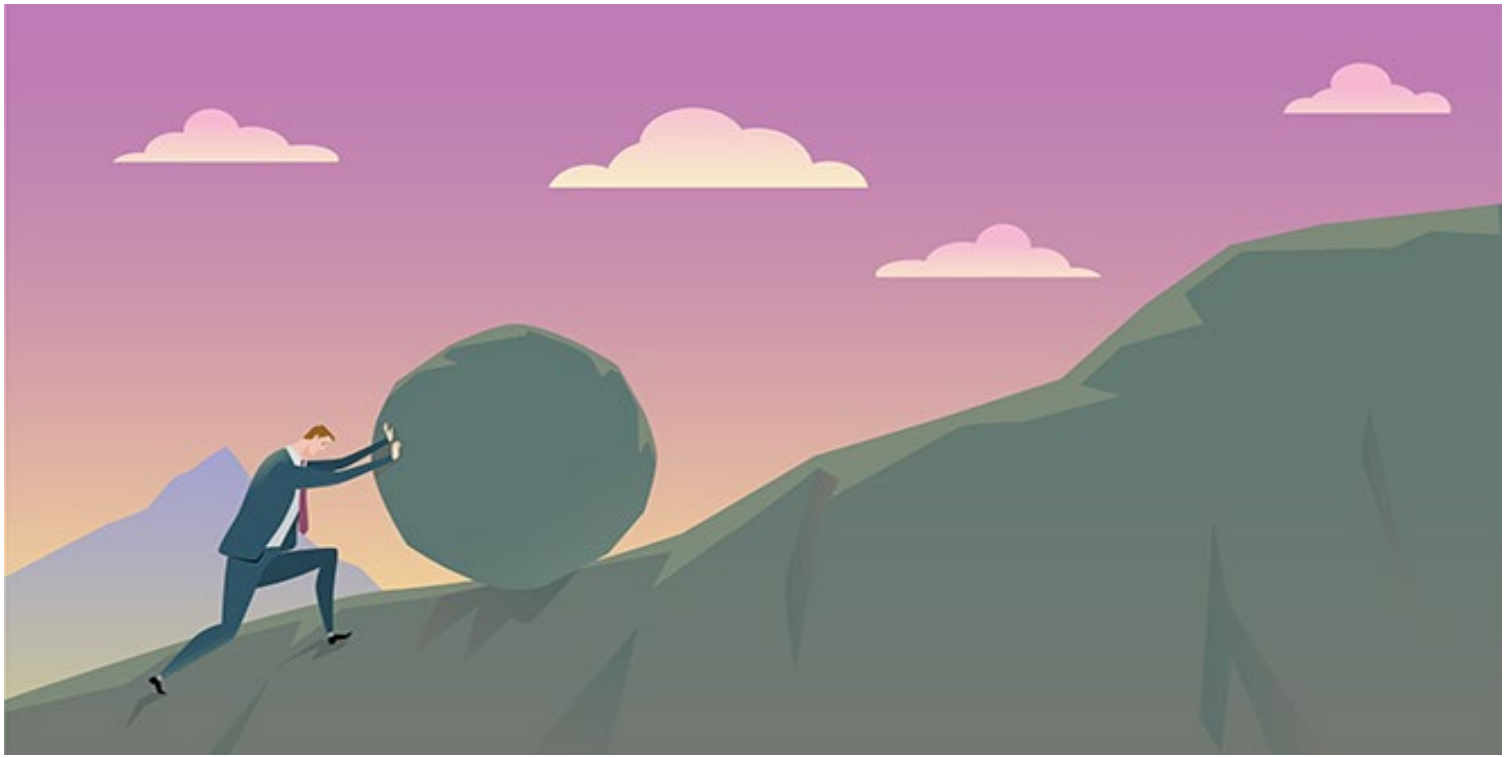
…and inferences drawn to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

PPD®

wyrickrobbins

De-Identified Information

- De-identified means “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer”
- Business is required to:
  - Implement technical safeguards that prohibit re-identification of the consumer to whom information pertains
  - Implement business processes that specifically prohibit reidentification of de-identified information
  - Implement business processes to prevent inadvertent release of de-identified information
  - Make no attempt to re-identify information



California Consumer Privacy Act of 2018

MAJOR REQUIREMENTS

PPD®

wyrickrobbins

Just-in-Time Notice

- At or before collection ("collect" includes "access")
- Categories of personal info collected, disclosed or sold in prior 12 months
  - Categories must align to statutory definition of PI, and must be distinct (no "lumping" of collect/disclose/sell activities)
  - "Sale" means to sell, rent, release, disclose, making available, etc. "for monetary or other valuable consideration"
- Purposes of collection
- Must disclose a consumer's rights (e.g., access, deletion) and designated request methods
- Must update every 12 months

PPD®

wyrickrobbins

Notice on Demand

- Applies to businesses that collect data
- ALSO applies to businesses that disclose or sell data
- Consumer may request the following information at any time (regarding activity in prior 12 months):
  - Categories of PI collected and categories of sources
  - Categories of PI disclosed or sold to third parties (must be separate lists)
  - Business and commercial purposes for collecting or selling PI
  - Whether or not any PI has been disclosed or sold (i.e., affirmative denial)
  - Categories of third parties to which PI was disclosed or sold (identifying categories of PI sold to each recipient)

PPD®

wyrickrobbins

Right of Access and Portability

- Consumer may request to know categories and specific pieces of PI collected in prior 12 months
- Request may be made at any time, but response required only twice in 12 months
- May supply data by mail or electronically
- If electronic, must be “portable”
- Free of charge

Right to Erasure
(aka "Right to Be Forgotten")

- Consumer may request deletion of PI
- Business also must direct "service providers" to delete PI
- Example exceptions (PI must be **NECESSARY** to these purposes):
  - Complete the transaction *for which PI was collected*
  - Provide goods or services *requested by consumer*
  - Perform contract *with the consumer*
  - Research (later slide)
  - Comply with legal obligation

PPD®

wyrickrobbins

More Right to Erasure Exceptions

- Enable solely “internal uses” “reasonably aligned” with consumer expectations based on relationship with business
- Otherwise use information “internally” “compatible with the context” in which consumer provided the information
- Debug or identify and repair errors that impair existing intended functionality
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible…

Image Source Credit: Michelle Lee

Restriction on Sale / Opt-Out Rights

- Reminder: “Sale” means to sell, rent, release, disclose, make available “for monetary or other valuable consideration”
  - Not a sale: necessary disclosures to service providers; acting at consumer’s specific, deliberate direction
- Consumers may at any time request to opt out of sale
- Consumers age 13-16 must affirmatively authorize sale
- Consumers < 13: Parents must affirmatively authorize sale
- Prior express authorization required to resume sales after an opt out; may not request authorization for 12 months
- Must train employees who handle customer inquiries

Restriction on Sale / Opt-Out Rights

- Opt-out notice must be "reasonably accessible":
  - Clear and conspicuous link on homepage
  - "Do Not Sell My Personal Information"
- Webpage must enable opt out
- May not require account creation
- Include separate description in privacy notice, again with "Do Not Sell My Personal Information" link
- Option to have California-only homepage with link
- Secondary sale prohibited unless explicit notice and opt out are provided (i.e., may not rely on initial seller's notice and opt out)

Important Exclusion

- "Third party" excludes business that collected the PI
- Also excludes recipients of PI if contract with business:
  - Prohibits selling the PI
  - Prohibits retaining, using, or disclosing PI for any purpose other than performing the services specified in the contract
  - Prohibits retaining, using, or disclosing PI outside the direct business relationship with the business
  - Includes a "certification" that they understand restrictions above and will comply

Ready to rebuild your website?

PPD®

wyrickrobbins

Handling Requests
("Notice on Demand," Access, Deletion)

- Two or more designated request methods required
  - Toll free number required
  - Website must be an option if one is maintained
- Response should be given in writing
  - Recall obligation for portability re: access requests
  - Must deliver through consumer's account, if they have one
  - Otherwise postal mail or electronic, at consumer's option
- Response due in 45 days, with 45-day extension when reasonably necessary

Verifying Requests

- Need sufficient information to:
  - identify the consumer and
  - "associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected"
- Engaging in verification does not extend time to respond
- May come from someone acting on consumer's behalf
- May not require account creation
- Business may only respond to verified requests
- Not required to respond if cannot verify

PPD®

wyrickrobbins

Verification Tips

- Confirming residency is not “verification”; denying request based on failure to confirm residency is not supportable (yet)
- Do not collect so much PI that you create a security risk or privacy snafu
- Do use “invisible” methods (e.g., device IDs)
- Do not fail to verify and cause security breach when disclosing
- Do develop graduated methods based on sensitivity of data
- Do watch this space for:
  - AG rules and guidance
  - Technology/vendor solutions
  - Lawsuits
  - Fraudsters and troublemakers

PPD®

wyrickrobbins

Reminder: Notice

Consumers must be advised of all of these rights, and the methods to effectuate them, via a privacy notice

PPD®

wyrickrobbins

Quiz

Commercial conduct is not restricted by CCPA if it takes place "wholly outside of" CA, which means:

1. Info was collected while consumer was outside CA
2. No part of sale of PI occurs in CA
3. No PI collected while consumer was in CA is sold

Are 1 and 3:

- *Redundant?*
- *Contradictory?*
- *Complimentary?*

California Consumer Privacy Act of 2018

SIGNIFICANT EXCEPTIONS

PPD®

wyrickrobbins

HIPAA Exception

- CCPA does not apply to HIPAA covered entities, or PHI "collected by" a covered entity or business associate
- Incomplete as to:
  - Employee data
  - Non-covered functions
    - Education
    - Research (but see clinical trial exception)
    - Website functions and marketing activities
    - Fundraising (but see nonprofit issue)
  - Non-standard transactions (e.g., cash pay)
  - Entities not covered by HIPAA (e.g., wearables, PHRs, fitness apps)
  - Benefits that are not part of group health plan

GLBA Exception

- CCPA does not apply to “personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act”
- Note: Not “in compliance with” or “consistent with”
- “Financial institution” has a specific meaning and scope under GLBA
- Regulatory obligations arise based on relationship with the individual

Clinical Trial Data Exemption

- Information collected as part of clinical trial:
  - subject to the Common Rule,
  - pursuant to good clinical practice guidelines issued by the International Council for Harmonisation, or
  - pursuant to human subject protection requirements of the FDA
- May not cover recruitment data
- Will not cover data regarding clinicians or other practitioners

Research Exception

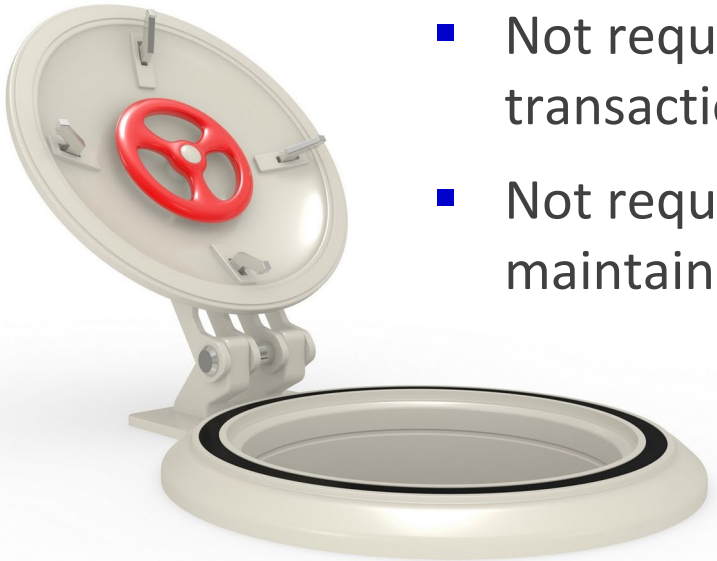
- PI not subject to deletion request if:
  - NECESSARY to engage in "public or peer-reviewed scientific, historical, or statistical research in the public interest"
  - Research "adheres to all other applicable ethics and privacy laws"
  - Deletion is "likely to render impossible or seriously impair the achievement of such research" **AND**
  - Consumer provided informed consent
- *("Informed" of what? That PI might not be deleted on request?)*

Other Exceptions

- Health care provider or medical info governed by CA's Confidentiality of Medical Information Act
- Personal information processed pursuant to CA's Financial Information Privacy Act
- Personal information processed pursuant to the DPPA
- Sale of information to a consumer reporting information if the data is included in a consumer report subject to the FCRA

Escape Hatches

- CCPA may not restrict ability to comply with law, cooperate with law enforcement, exercise or defend legal claims, or respond to legal inquiries (e.g., regulators, subpoena)
- Does not restrict commercial conduct “wholly outside CA” (see quiz slide)
- Not required to retain PI collected for a one-time transaction
- Not required to re-identify or link data not maintained in a manner that would be PI



PPD®

wyrickrobbins

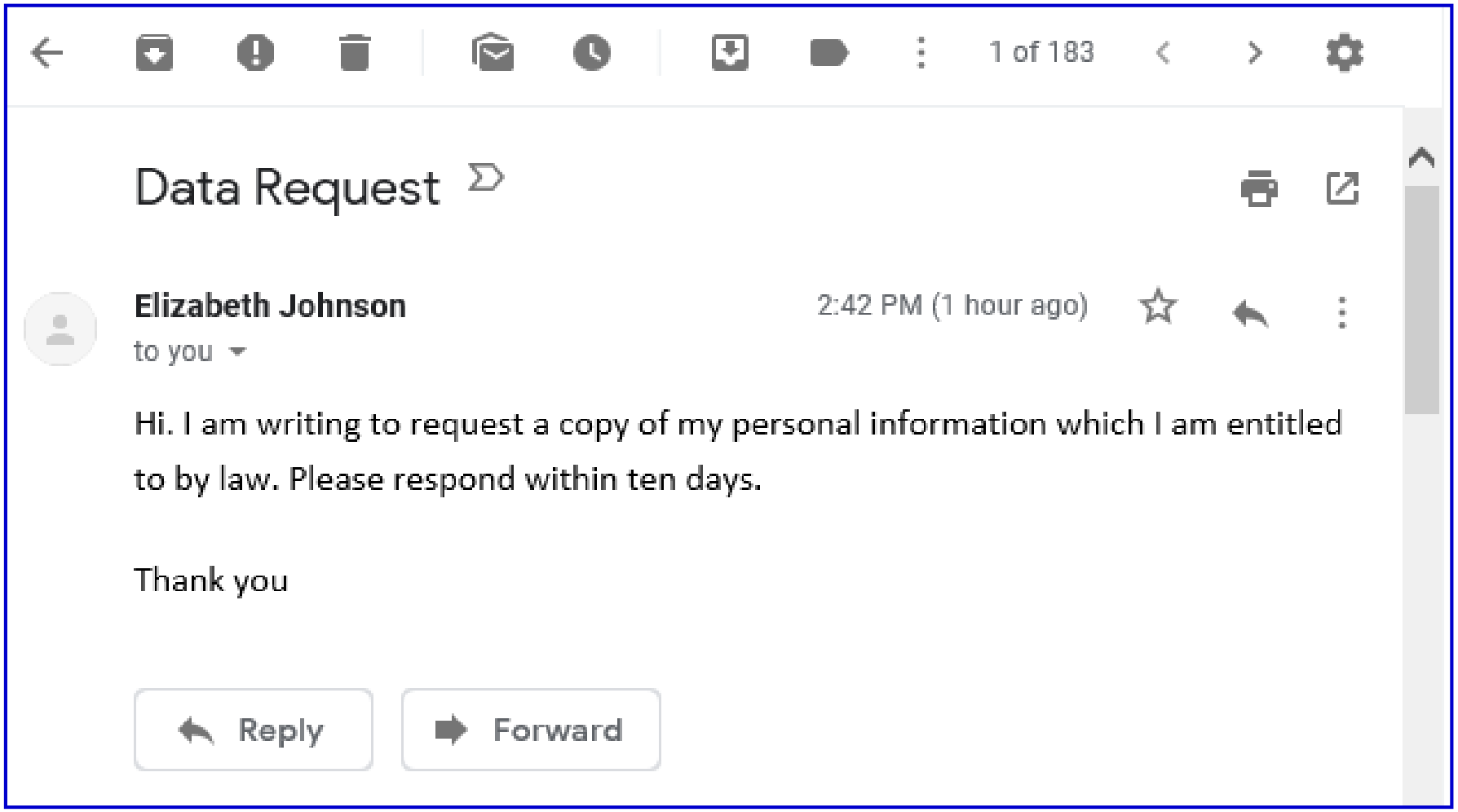
CCPA in Action

USE CASES

PPD®

wyrickrobbins

Use Case #1: You've Got Mail



Use Case #2

- You are a fintech company offering investment services to individuals via a mobile app
- You partner with an FDIC-insured bank to offer a deposit account as part of the overall service model
- You operate a general information website to advertise and provide information about the app
- Does CCPA attach to all aspects of this business model? How do you decide?

PPD®

wyrickrobbins

Use Case #3

- You sell consumer goods through an ecommerce site
- You engage a third party to evaluate transactions for fraud, including by engaging in device fingerprinting
- How do you prepare for CCPA's impact on this one element of your operation?
- What questions do you have for the third party regarding their CCPA readiness?

PPD®

wyrickrobbins

California Consumer Privacy Act of 2018

RULE MAKING AND ENFORCEMENT

PPD®

wyrickrobbins

Important Dates and Rulemaking

- January 1, 2020: Effective date
- July 1, 2020
  - Rules due from AG
  - Enforcement date

- CA AG public fora
  - February 13, California State Bldg, Fresno
  - March 5, Stanford Law School, Stanford
- CA AG requests comments by email by March 8, 2019

More information: https://oag.ca.gov/privacy/ccpa

PPD®

wyrickrobbins

Riddle

Consumers are entitled to receive information regarding disclosures of their PI over prior 12 months

Effective date of the CCPA is January 1, 2020

A consumer sends you a verified request regarding disclosures of his/her PI on January 2, 2020

When do you need to start logging disclosures in order to comply?

PPD®

wyrickrobbins

Enforcement

- Fines by CA AG up to $7,500/violation
- Private right of action
  - unencrypted or unredacted personal information exposed due to failure to maintain appropriate security
  - statutory damages $150-$750

PPD®

wyrickrobbins

Organization Name	Date(s) of Breach	Reported Date
Centerstone Insurance and Financial Services d/b/a BenefitMall	06/13/2018, 10/11/2018	01/03/2019
Humana Inc	05/30/2018	01/03/2019
OXO International, Ltd.	07/01/2018	01/03/2019
Aimbridge Hospitality Holdings, LLC	06/07/2018, 09/24/2018	01/02/2019
Hammer Nutrition	01/01/2018	01/02/2019
Wolverine Solutions Group	09/23/2018	12/28/2018
MJ Insurance, Inc	09/26/2018	12/27/2018
BEL USA, LLC ("BEL") through its website DiscountMugs.com	08/05/2018	12/26/2018
San Jose State University	12/10/2018	12/26/2018
JAND Inc. d/b/a Warby Parker	09/25/2018, 11/30/2018	12/21/2018
Michael Koch, dba Lockhart, Britton & Koch	11/25/2018	12/20/2018
Beverages & More, Inc. dba BevMo!	08/02/2018, 09/26/2018	12/14/2018

Use Case #4

- You identify a data incident that qualifies as a "breach" under CA law and report it
- An affected person files suit
- What records maintained by your business might be discoverable?

PPD®

wyrickrobbins

PROSPECTS FOR PREEMPTION

PPD®

wyrickrobbins

Federal Bills Proposed

- Wyden: Consumer Data Protection Act
  - Requires annual privacy report to FTC, signed by CEOs
  - Up to 20 years in prison if they lie
  - "Do No Track" website to opt out of data sharing online
  - FTC enforcement
- Schatz: Data Care Act
  - Requires companies to safeguard data
  - Prohibits use of data in ways that harm consumers
  - FTC enforcement
- Rubio: American Data Dissemination Act
  - Tasks FTC to ID laws and suggest updates to Congress

PPD®

wyrickrobbins

Follow-up questions

Corey Dennis

PPD

corey.dennis@ppdi.com

910.558.6500

Elizabeth Johnson

Wyrick Robbins

ejohnson@Wyrick.com

919.228.2902

2018: Privacy and Data Security

OTHER LEGAL DEVELOPMENTS

GDPR Now Effective

- Notice/consent
- Data processing reviews and data protection impact assessments
- Individual rights (access, portability, deletion)
- Data breach reporting
- Security
- Vendor management
- Data transfer restriction
- Data protection officer/representative
- Fines of up to 20M€ or 4% global revenue

PPD®

wyrickrobbins

Data Breach Notification 2018

- Alabama and South Dakota became 49th and 50th states to enact data breach notification statutes
- Complex overall picture:
  - PCI DSS
  - Federal: HIPAA, financial federal functional regulators (GLBA/NPI), FTC (vendors of PHR), FCC (CPNI)
  - Territories etc.: Puerto Rico, Guam, Virgin Islands, District of Columbia
  - Local: See e.g., CT insurance regs, Chicago
  - International: EU (GDPR), Canada, etc.

Trends in State Data Breach Laws

- Slight majority of laws amended/enacted in 2018 added ***regulator reporting requirement***
- Substantial majority of laws amended/enacted in 2018 added ***reporting deadline***
- Substantial majority of laws amended/enacted in 2018 ***expanded coverage of personal information***
  - Biometric data
  - Login credentials
  - Health care and/or health insurance
  - Passport number
  - Tax ID Number (TIN)

PPD®

wyrickrobbins

Other Trends

- Mandatory consumer protections
- Broadening definition of breach (ransomware)
- Web portal reporting to regulators
- Regulators cataloging reports and root causes

Proposed Changes to NC Breach Law

- 15-day reporting requirement
- Expanded concept of PII
- Lower harm threshold
- Access added as breach concept
- Data security obligation
- Possible safe harbor
- Submission of material to AG

Ohio: Data Security Safe Harbor

- Affirmative defense for tort claims based on OH law or brought in OH court
- Security program must:
  - Include admin, physical, technical controls
  - Address risk/anticipated threats
  - Conform to: NIST CSF, NIST 800-171, NIST 800-53, FedRAMP, CIS Critical Security Controls, ISO 27000, HIPAA/HITECH, GLBA, FISMA, PCI DSS
- North Carolina considered similar measures in 2018
- ***Possible trend***: Safe harbors are bipartisan, pro-security, and business-friendly

PPD®

wyrickrobbins

Colorado: Data Security

- Requires "reasonable security procedures and practices" appropriate to data and business nature/size
- Requires contract with vendors that specifies security, unless they work under customer's security program
- See also:
  - Specific: Massachusetts, Oregon, Nevada
  - Vendors: California, Florida, Maryland, Nebraska, North Carolina, Rhode Island
  - General: Additional 10-12 states
- ***Trend***: Adding proactive data security mandates when breach laws are amended

PPD®

wyrickrobbins

Follow-up questions

Corey Dennis

PPD

corey.dennis@ppdi.com

910.558.6500

Elizabeth Johnson

Wyrick Robbins

ejohnson@Wyrick.com

919.228.2902