

## Balancing Innovation and Data Protection: Technology, Media and Privacy Considerations



Thomas Magnani, Jami Mills Vibbert, Nancy L. Perkins, Alex Altman

Monday, June 29, 2020

# Introductions



**Thomas A. Magnani**



**Jami Mills Vibbert**



**Nancy L. Perkins**



**Alex Altman**

# Agenda



- California Consumer Privacy Act (CCPA)
  - Overview and Tricky Issues
  - Liability and Reducing Risk
- Pending Legislation in Other States
- COVID-19 and Data Privacy
- Privacy and Security by Design
- Privacy and Security in Tech Transactions and Diligence

# CCPA Overview and Tricky Issues



# Timing



- Statute took effect January 1, 2020
- Limited private right of action available since January 1, 2020
- Final draft regulations have been submitted by the CA AG and *may* go into effect and become enforceable on July 1, 2020—otherwise October 1, 2020

# Scope: Who Is Regulated?



- **“Businesses”**
  - **Organizations operating in CA that:**
    - have annual gross revenues in excess of \$25 million;
    - annually buy, sell, receive, or share for commercial purposes personal information of 50,000 or more CA consumers or devices; *or*
    - derive 50 percent or more of annual revenues from selling CA consumers’ personal information
  - **Organizations that control or are controlled by a business as defined above**
- **Exempted entities**
  - Nonprofit companies
  - Businesses that have no physical presence or affiliates in CA *and* no commercial activity in CA



# Whose Privacy Is Protected?



- **“Consumers”**

- Any “natural person who is a California resident”
  - *E.g.*, individual customers, employees, website visitors
- Includes individuals domiciled in CA who are outside the state for a temporary or transitory purpose

- **Excludes**

- An individual who is in CA solely for a temporary or transitory purpose

# What Privacy Rights Are Provided?



- **With respect to information identifiable to the consumer, or that could “reasonably be linked” to the consumer or his/her household (with limited exemptions) [“Personal Information” definition #1]**
  - Right to notice of collection, use and disclosure
  - Right of access
  - Right to request deletion
  - Right to opt out of “sales”



# Privacy Requirement Exemptions



- “Protected health information” collected by a “covered entity” or “business associate” subject to the Health Insurance Portability and Accountability Act (HIPAA)
- Medical information under the California Confidentiality of Medical Information Act
- Information collected as part of a clinical trial subject to the Common Rule, clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the Food and Drug Administration
- Information subject to the federal Gramm-Leach-Bliley Act or California Financial Information Privacy Act
- Information that is “consumer report” information under the federal Fair Credit Reporting Act (FCRA) when used as permitted under FCRA
- Until Jan 1, 2021—Employee and job applicant information
  - BUT: privacy notice requirements already apply
- Until Jan 1, 2021—B2B contact information

# What Security Controls Are Required?



- **With respect to a more narrowly defined set of “personal information” [definition #2]**
  - An individual’s first name or first initial and his or her last name *in combination with* any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
    - Social Security number
    - Driver’s license number or California identification card number
    - Account number, credit or debit card number, *in combination with* any required security code, access code or password that would permit access to an individual’s financial account
    - Medical information
    - Health insurance information
- **Businesses must implement and maintain “reasonable security” procedures and practices**
  - Such procedures must prevent unauthorized access and exfiltration, theft, or disclosure of nonencrypted and nonredacted high-risk personal information

# Notice



- Notice must be given “at or before the point of collection”
- Notice must include:
  - List of categories of personal information to be collected
  - Statement of purposes for which the categories of personal information shall be used
  - If relevant, statement that personal information may be sold and the consumer can opt out of the sale; link to easy means to opt out labeled “Do Not Sell My Personal Information”
  - Link to privacy policy
  - If relevant, notice that the business offers a financial incentive or provides a price or service difference related to the collection, retention or sale of personal information

# Privacy Policy



- Privacy Policy must include disclosure of:
  - Categories of personal information about consumers that the business has, in the past 12 months:
    - Collected about consumers
    - Sold or disclosed to third parties for a business purpose
  - Categories of third parties to whom personal information has been sold or disclosed
  - Consumer's right to know and submit requests for:
    - List of categories of personal information collected, disclosed or sold
    - Specific pieces of personal information collected
  - Consumer's right to request deletion of personal information
  - Business's obligation not to discriminate against a consumer for the exercise of CCPA rights

# Consumer Requests



## Know Categories

Of PI collected, sold, disclosed  
Of sources  
Of third parties

Verifiability to a “**reasonable** degree of certainty”  
(2 data points)

Two methods to submit, unless business is online only

## Know Specific

Pieces of personal information collected

Verifiability to a “**reasonably high** degree of certainty”  
(3 data points plus sworn declaration)

Two methods to submit, unless business is online only

## Deletion

Pieces of personal information collected

Verifiability “to a **reasonable degree or a reasonably high degree of certainty** depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion”

Two methods to submit, including toll free number for all businesses

May use a two-step verification method

## Sale Opt Out

Optional for adults (may opt in by default)  
Default opt out for all children 16 and under  
13–16 may opt in  
Under 13, parent may opt in

Two or more methods, including “Do Not Sell My Personal Information” link

User-enabled global privacy controls, such as a browser plugin or privacy setting

Offline method for substantially offline businesses

# “Household” Requests



May be made through password-protected account

If no such account, business must:

- Have all consumers in household jointly request to know/delete
- Verify all members of household per verification requirements
- Verify each member is a member of the household



If request is to know specific information or to delete and household has child under 13, business must obtain verifiable parental consent



# Additional Request Considerations



- Authorized agents
  - Requests to know, delete and opt out may be made by an “authorized agent” of the consumer
  - Business responding to such request may require consumer to:
    - Provide proof of consumer’s signed permission for agent to make requests
    - Verify their own identity
    - Directly confirm with the business that they provided the authorized agent permission to submit the request
  - Alternately, authorized agent may act under power of attorney
- Fees
  - Information must be provided or deleted free of charge unless requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, in which case a business may charge a reasonable fee or deny the request
- Service Providers
  - May act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider

# CCPA Liability and Reducing Risk



# CA Attorney General Enforcement



- For failure to provide privacy-related protections (required notices, timely access to personal information (definition #1)) upon consumer request, etc.)
- Injunctive relief
- Civil penalties for enforcement by CA Attorney General
  - Up to \$2,500 per violation
  - Up to \$7,500 for each intentional violation

# Private Right of Action



- Only available for:
  - Unauthorized access and exfiltration, theft or disclosure of “high-risk” personal information *as a result of*:
    - The business’s violation of the duty to implement and maintain reasonable security procedures and practices
- May be brought as a class action
- Injunctive relief, actual damages, statutory damages
- Statutory damages capped at \$750 per consumer per incident
- 30-day notice and cure period before seeking statutory damages

# Exemptions from Private Right of Action



- Exemptions for breaches involving:
  - “Protected health information” collected by a “covered entity” or “business associate” subject to the Health Insurance Portability and Accountability Act (HIPAA)
  - Medical information under the California Confidentiality of Medical Information Act
  - Information collected as part of a clinical trial subject to the Common Rule, clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the Food and Drug Administration

# Reducing Risk of a Claim Under the PROA



- Do a risk assessment to lower risk of being subject to a data breach under California law
- Monitor security practices
- If and when a breach occurs, be able to show that reasonable security was in place



# Reasonable Security—What Is It?



- The CCPA does not define what constitutes “reasonable security procedures and practices”
- No standard definition of reasonable security, but guidance may be taken from various sources. For example:
  - Former California AG Kamala Harris: “The failure to implement all the [CIS] Controls that apply to an organization’s environment constitutes a lack of reasonable security.”
  - Case law, agency guidance, regulatory enforcement, self-regulatory standard-setting bodies, and industry best practices

# Reasonable Security—Some Practices to Consider



**Governance**

**Risk  
Assessment and  
Management**

**Access Controls**

**Cryptography**

**Vulnerability  
Management**

**Business  
Continuity and  
Disaster  
Recovery**

**Vendor  
Management**

**Security Incident  
Response  
Planning**

# Reducing Risk of AG Enforcement

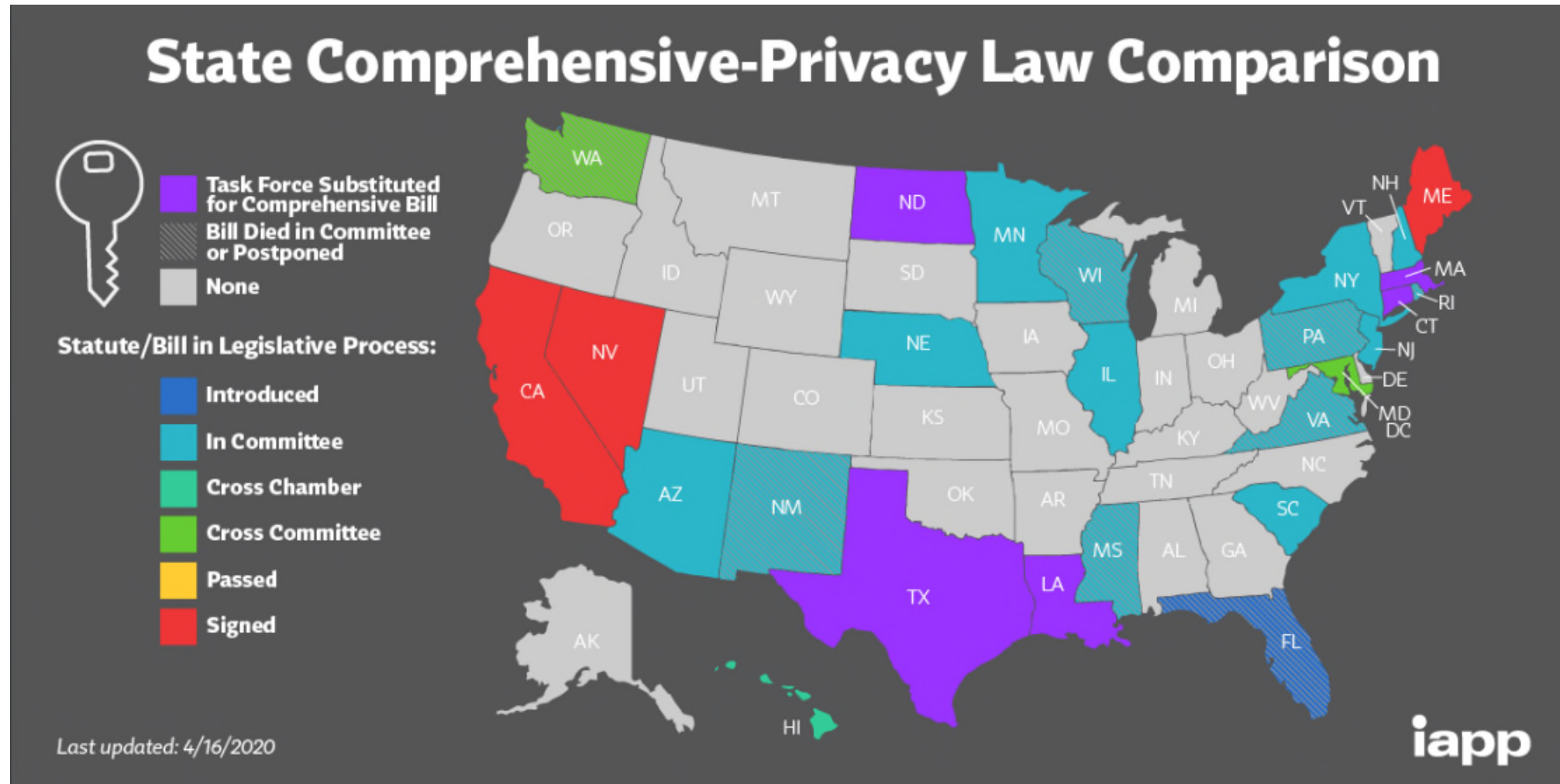


- Assess data and risk
- Assign responsibility
- Create processes and procedures
- Document position

# Pending Privacy Legislation in Other States



# Pending Privacy Legislation



# COVID-19 and Privacy

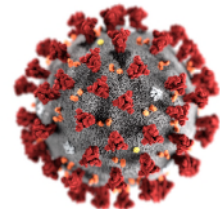
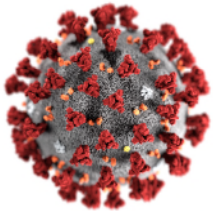
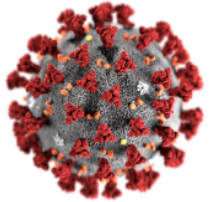
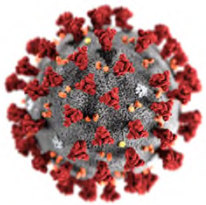




# Contact Tracing Tech and Privacy Concerns



- Most privacy regimes rely on notice and consent to some degree. What if users do not consent to all uses of their data?
  - Fewer consenting users means less effective tracing
  - Rely on applicable exceptions
    - CCPA—Businesses need not honor deletion requests in cases of “public or peer-reviewed scientific, historical, or statistical research”
    - GDPR—Consent not needed if “processing is necessary for the performance of a task carried out in the public interest”
    - HIPAA—Disclosure without authorization allowed for “public health activities and purposes”
- Limiting data collection by design
  - Limit/eliminate geolocation data collection
  - Anonymize/pseudonymize records as much as possible



# Contact-Tracing Privacy Legislation

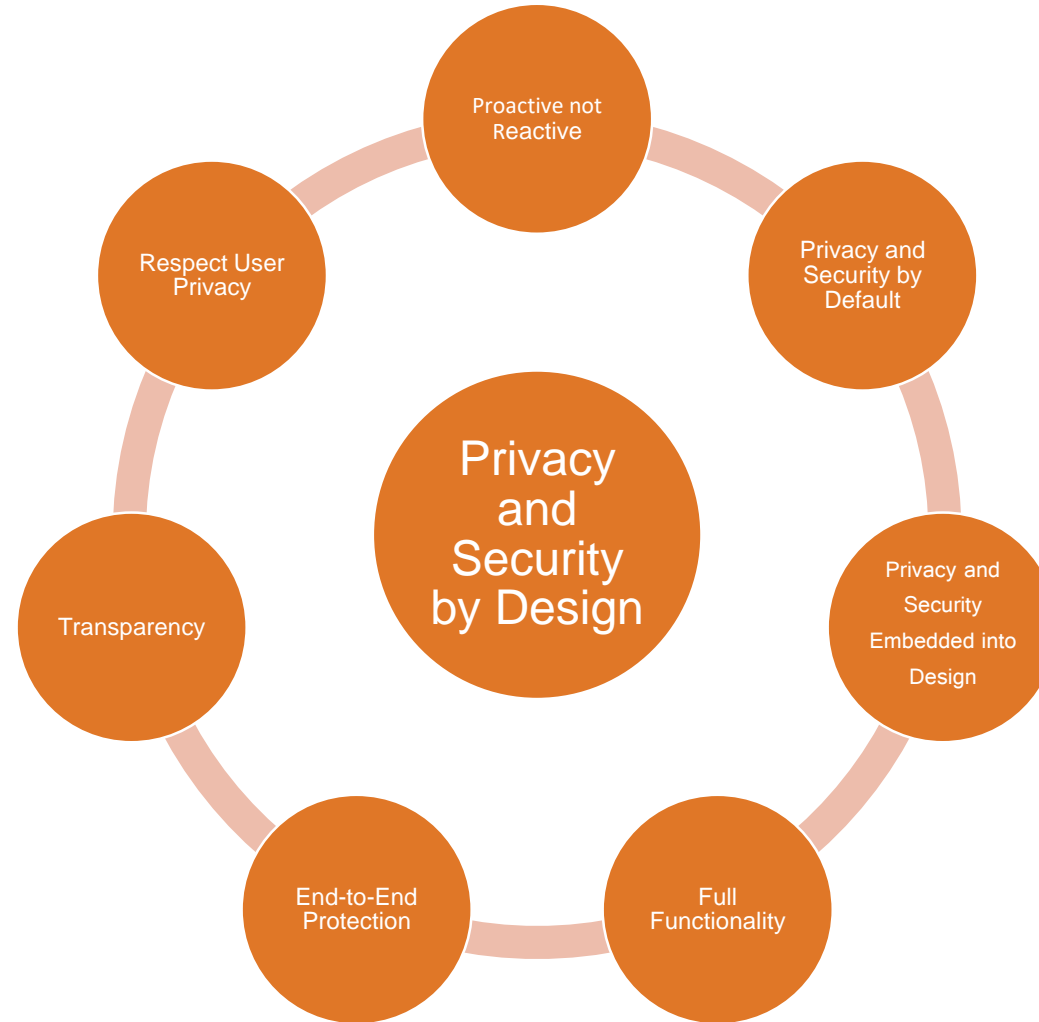


- Three federal bills pending in Congress:
  - [COVID-19 Consumer Data Protection Act of 2020 \(S. 3663\)](#), sponsored by Senator Roger Wicker (R-MS) and several other Republican senators
  - [Public Health Emergency Privacy Act \(S. 3749\)](#), sponsored by Senators Richard Blumenthal (D-CT) and Mark Warner (D-VA) and Representative Anna Eshoo (D-CA)
  - [Exposure Notification Privacy Act \(S.3861\)](#), sponsored by Senators Maria Cantwell (D-WA), Bill Cassidy (R-LA) and Amy Klobuchar (D-MN)
- Bills pending in several states, including CA, MN, NY

# Privacy and Security by Design



# Privacy and Security by Design Principles



# Privacy and Security by Design Implementation



Process



Governance



Culture

# Operationalizing Privacy and Security by Design



- Think about privacy and data security in all stages of development
- Change the way you collect and process data
- Document your data protection
- Demonstrate compliance
- Ensure that the entire organization is thinking about privacy and data security



# Privacy and Security in Tech Transactions and Diligence



# Tech Transactions—What to Look For?



- Data Provisions
  - Confidential data v. personal data v. customer data
- Data Ownership and Rights to Data
- Appropriate Data Uses and Services to be Provided
  - Segregate data types carefully and future proof for data uses not yet contemplated

# Tech Transactions—Provisions







- CCPA, BAA, GDPR
  - All require a determination as to company/service provider or covered entity/business associate or controller/processor
- Compliance with laws
- Breach notification
  - Timing
  - Who controls response
  - What cooperation looks like
- Indemnification and Liability

# Dangers of Acquiring Privacy/Security Risk



Even the most appealing target may come with outsized privacy/security risks:

-  Immature compliance programs
-  Unprotected legacy systems
-  Nonexistent governance
-  Cultural indifference

# Managing Risk in M&A: Pre-Close



## Do your due diligence!

- Draft default questionnaire/checklist for target to complete and document request
  - Lets target know you take privacy and security seriously
- Perform a preliminary risk assessment to understand risks
  - E.g., if the target does not operate in the EU, GDPR risk may be minimal or nonexistent
- Work closely with IT, InfoSec, Legal, Compliance, and HR to align goals and streamline inquiries
- Interview with relevant individuals
- Full risk assessment, if needed



# Managing Risk in M&A: The Agreement



Factor latent risk into the terms

- Use reps and warranties
- Indemnification and liability caps
- Price risk into the final consideration
  - Ultimately, the deal may not be worth the risk!



# Managing Risk in M&A: Integration



- Segregate inherited systems until full integration possible
- Train new employees and employee notices
- Revise policies and procedures
- Risk assessment

# Questions?



**Thomas A. Magnani**

Partner, San Francisco, CA  
tom.magnani@arnoldporter.com  
+1 415.471.3162



**Jami Mills Vibbert**

Partner, New York  
jami.vibbert@arnoldporter.com+  
+1 212.836.7950



**Nancy L. Perkins**

Counsel, Washington, DC  
nancy.perkins@arnoldporter.com  
+1 202.942.5065



**Alex Altman**

Senior Associate, New York  
alexander.altman@arnoldporter.com  
+1 212.836.7960