November 10, 2023

# The Top Ways New State Privacy Laws Will Break Your Program, and How to Fix It

Privacy+ Security Forum

# Speakers

Privacy+ Security Forum

## Bret Cohen

Partner, Privacy & Cybersecurity
Hogan Lovells

## Annie Bai

Associate General Counsel
Socure

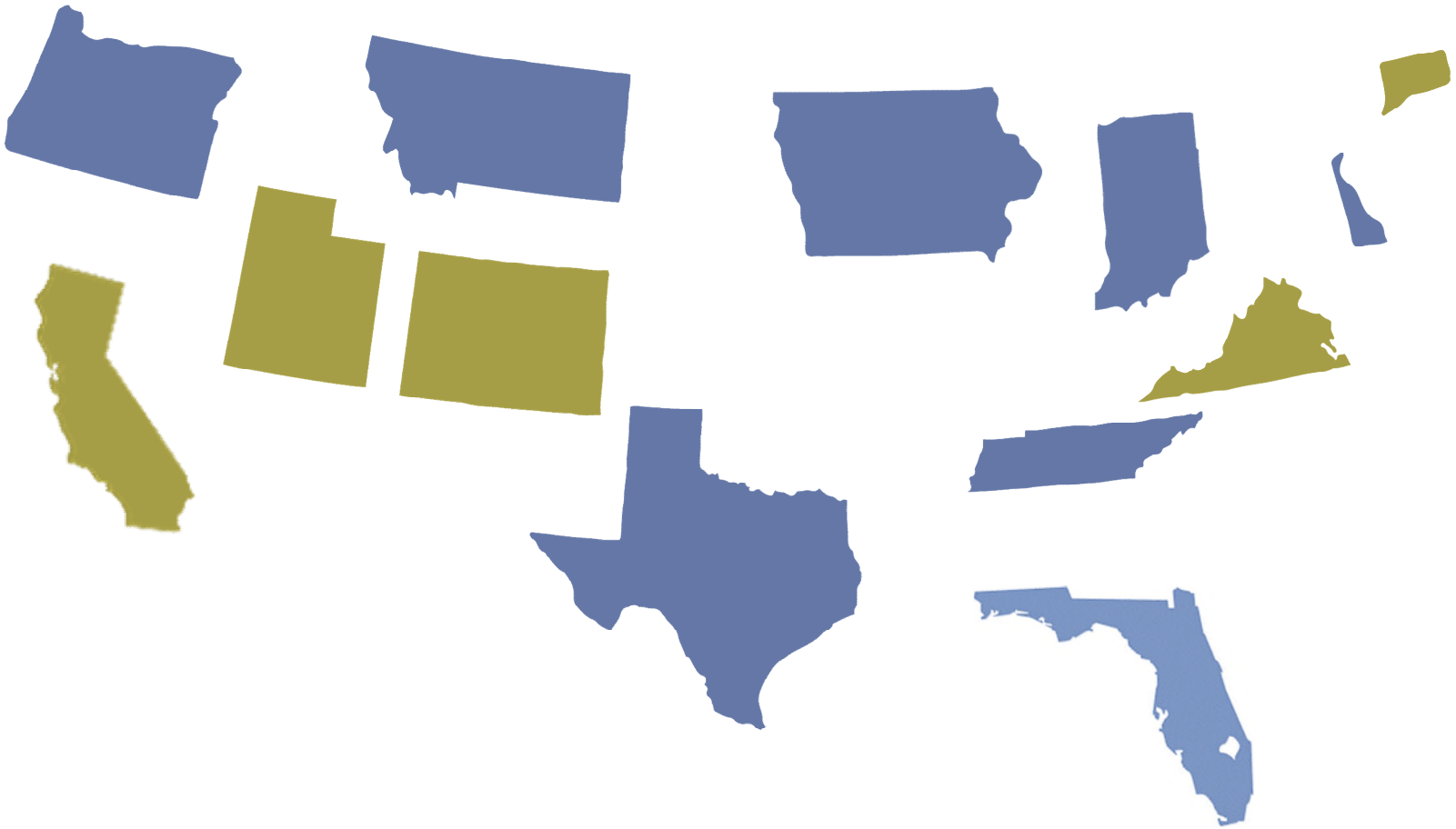
## Charlie Wood

Vice President, Legal & Compliance
The Carlyle Group

## Warren Allen

VP & Associate General Counsel
Diligent Corporation

# A progression of state privacy laws



# Privacy Policies

# Expanded Privacy Policy Requirements

Privacy+ Security Forum

| | All 13 states | CA | CO | CT | DE | FL | IA | IN | MT | OR | TN | TX | UT | VA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| • Categories PI collected<br>• Purposes for PI collection/use<br>• Description of consumer's rights, and how to exercise<br>• Categories of PI disclosed to third parties<br>• Categories of third parties to whom the controller discloses PI | ✓ | | | | | | | | | | | | | |
| • Separate notice at collection,<br>• Length of time to retain each category of PI (including sensitive PI)<br>• Categories of PI sold, shared, disclosed for business purposes in the preceding 12 months and for each the categories of third parties; must state if no selling, sharing, or disclosure for a business purpose<br>• Whether the business has actual knowledge it shares PI of consumers under 16<br>• Metrics on receipt and response to verified consumer rights requests<br>• For rights requests: verification mechanisms, authorized agent procedures | | ✓ | | | | | | | | | | | | |
| • Specific disclosure in the event sensitive or biometric personal data is sold | | | | | | ✓ | | | | | | ✓ | | |
| • How consumers may appeal a controller's actions regarding a consumer's rights request | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| • Contact information or other online contact mechanism | | ✓ | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | | | ✓ |

"NOTICE: We may sell your sensitive personal data."
"NOTICE: We may sell your biometric personal data."

# Personalization

# Opt Outs From Personalization?

- Opt-outs of "profiling" for automated decision-making (CA, CO, CT, DE, FL, IN, MT, OR, TN, TX, VA)
  - "Profiling" includes evaluating personal aspects to predict "personal preferences" and "interests"
  - Existing state rules limit the opt-out to that which "produces legal or similarly significant effects concerning the consumer"
- CA rulemaking preview recommendations:

A business shall provide consumers with the right to [access information about/opt-out of] the business's use of Automated Decisionmaking Technology if the business:

1) Uses Automated Decisionmaking Technology in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities;
2) Uses Automated Decisionmaking Technology to monitor or surveil employees, independent contractors, job applicants, or students;
3) Uses Automated Decisionmaking Technology to track the behavior, location, movements, or actions of consumers in publicly accessible places;
4) Processes the personal information of consumers that the business has actual knowledge are less than 16 years of age in the business's use of Automated Decisionmaking Technology; or
5) Processes the personal information of consumers to train Automated Decisionmaking Technology.

# “Sensitive” Information

Privacy+ Security Forum

# Sensitive Information & Sensitive Data

Privacy+ Security Forum

## Broadened Definitions

1. Precise Geolocation
2. Children – personal data (DE, OR); collected from a child (FL)
3. Mental or physical (health) condition or diagnosis (DE, OR, WA)
4. Status as transgender/nonbinary (DE, OR)
5. Status as a victim of a crime (OR)
6. Genetic/biometric data (FL, OR, VA)
7. Inferences with regards to sensitive status (CO & regs)

## Greater Obligations

- Notice (IA, UT)
- Opt in (VA)
- Opt out (CA); or Ability to withdraw consent (DE, MT, OR)
  - Consent revocation must be honored within 15 days
- Deletion of inferences within 24 hours (exemption)

## Operational Impacts

- Update **privacy notices** (additional biometrics one?)
- Build opt/consent* mechanisms
- Update **data governance** labels
- Consult **stakeholders** on need
- Spotlight on **marketing**
- Check on processor activities (as controller or processor needing to be included in the **consent**)
- Protect trade secrets

## Open Issues

- What are inferences anyway?
- What about photos?

# Precise Geolocation

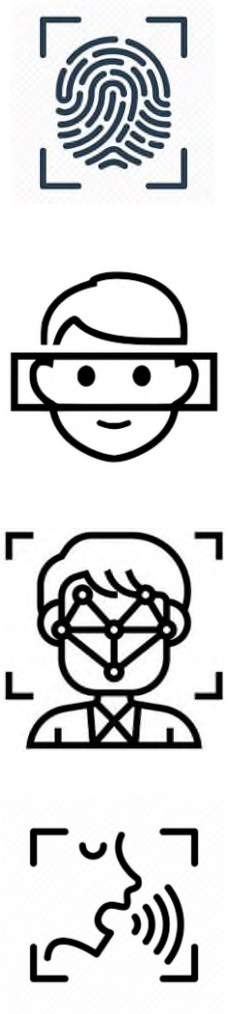
Privacy+ Security Forum

| Jurisdiction | Definition specifies radius of 1750' | Notice | Consent | Data Assessment | Right to Limit |
|---|---|---|---|---|---|
| California Consumer Privacy Act (CCPA) | 1,850 feet | ✓ including purpose/retention | | | ✓ with explicit consent required |
| Connecticut Data Privacy Act (CDPA) | ✓ | | ✓ | ✓ | |
| Florida Digital Bill of Rights (FDBR) | ✓ | | | | |
| Indiana Data Privacy Law (IDPL) | ✓ | | ✓ | ✓ | |
| Montana Consumer Data Privacy Act (MCDPA) | ✓ | | ✓ | ✓ | |
| Oregon Consumer Privacy Act (OCPA) | ✓ | ✓ Privacy Notice | ✓ | ✓ | |
| Tennessee Information Privacy Act (TIPA) | ✓ | | ✓ | ✓ | |
| Texas Data Privacy and Security Act (TDPSA) | ✓ | ✓ Privacy Notice | ✓ and specifically Small Businesses | ✓ | |
| Utah Consumer Privacy Act (UCPA) | ✓ | ✓ Allow opt out | | | |
| Virginia Consumer Data Protection Act (VCDPA) | ✓ | ✓ in consent | ✓ | ✓ | |

# Biometrics & Health Data

## Biometrics

- Broad definition (OR) – includes data that "allow or confirm the unique identification of the consumer" vs other laws limited to data that is "used to identify a specific individual."
- Even broader definition (WA MHMDA) – includes behavioral characteristics, e.g. keystrokes



## Geofencing as Health Data

- CT – No geofencing (1,750 feet or less) of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data.
- WA – No geofence (2000' or less) around a facility that provides health care services. Specifically prohibited for: 1) identifying or tracking consumers seeking health care services, 2) collecting consumer health data from consumers, or 3) sending notifications, messages, or advertisements to consumers related to their consumer health data or health care services

# Contracts

Privacy+ Security Forum

# Requirements

- For processors: increasing GDPR-alignment
  - Common GDPR provisions like Confidentiality, Audit/Information Rights, Subprocessor Contracts, Details of Processing, Deletion/Return of Data
  - CA is similar but not identical to this
  - Some trend towards objection rights for Subprocessors too (CO, CT, DE)
- Also continued contract commitments around **keeping** deidentified data from being reidentified whenever disclosed to a third party (started in CA, now prolific)

# Operational Impact

- Local: Who doesn't enjoy updating DPA templates every few months?
- Global: the growing patchwork pushes us away from narrowly scoped DPAs
- US states may be better than the global picture if they keep close to GDPR
- Worth worrying about co-controller equivalents?
- Hope for consistency but prepare for creativity

# Access Rights

Privacy+ Security Forum

# Requirements

- Some right to access in all 12 comprehensive state laws
- Response times: seemingly unifying around 45 day expectation; CA 10 business days to confirm receipt, then respond in 45 days
- OR requirement to disclose **specific third parties** (other than natural persons) who have received data
- TBD how trade secret exemptions from access will play out (most laws have explicit exemptions, but not VA and exemption limited in CO to portability)

# Operational Impact

- Do unified global access right procedures work best?
- Is state by state realistic/desirable?
- Trade secret exemptions so far:
  - CO AG regulations call out that the controller has to find a way to give the data subject access **even if** the request involves portable data that could threaten a trade secret: such as providing a non-portable option
  - CA AG opinion: no generic denials, despite what inferences could reveal

# PIAs

Privacy+ Security Forum

# Get Ready for a Flood of PIAs

Privacy+ Security Forum

## Requirements

- Required where there is risk of consumer harm (CA, CO, CT, IN, MT, TN, VA)
- Changes to come:
  - **When** must a business conduct an impact assessment
  - **What** must be included in an impact assessment
  - **When** must an impact assessment be shared externally
  - **How long** must impact assessments be retained
  - New requirements related to **children's data**

## Operational Impact

- Retroactive PIAs for current processing activities
- Potential exposure of confidential info in externally disclosed PIAs
- PIAs for positive data processing (e.g., bonus systems)?
- How to simplify/streamline?
- How to keep PIAs evergreen?
- How to address multi-jurisdictional requirements?
- Embedding PIAs in product and process design
- Consider automated tools
- PIAs as standard of care in class action suits
- PIAs for AI

# NIST Privacy Framework as an affirmative defence

Privacy+ Security Forum

# Tennessee's Affirmative Defense

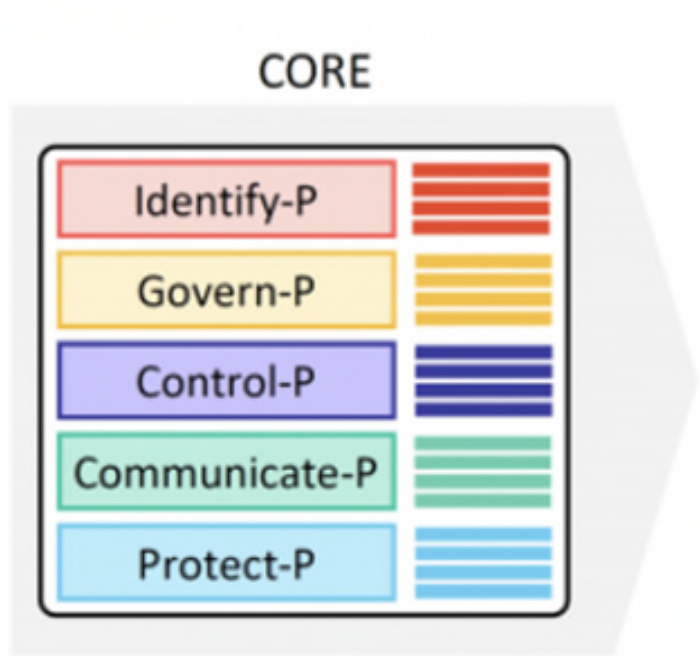
Privacy+ Security Forum

## NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

Tennessee: A controller or processor has an affirmative defense to a cause of action for a violation of this part if the controller or processor creates, maintains, and complies with a written privacy program that:

(1) (A) Reasonably conforms to the [NIST Privacy Framework] Version 1.0." or other documented policies, standards, and procedures designed to safeguard consumer privacy; and (B) Is updated to reasonably conform with a subsequent revision to the NIST or comparable privacy framework within two (2) years ...; and

(2) Provides a person with the substantive rights required by this part.



# Questions & Contacts