The U.S. State Privacy Landscape

'Comprehensive' Laws

Keir Lamont
Future of Privacy Forum
Director, U.S. Legislation

Comprehensive Privacy Legislation –
a broad-based industry and technology neutral framework that governs the collection, use, and transfer of personal consumer data throughout the economy.

The Federal Privacy Landscape

- The United States is now the ***only*** G20 country without a comprehensive national law governing the collection, use, and transfer of personal information.
  - National laws largely informed by the European 'General Data Protection Regulation' (2018)

- Instead, the U.S. takes 'sectoral' approach
  - Laws protect sensitive categories and uses of personal information: health (HIPAA), financial (GLBA), children's (COPPA), and video rental records (VPPA)
  - Backstop enforcement by the Federal Trade Commission, Section 5 authority to deter 'unfair and deceptive' acts and practices
    - ANPR: "Commercial Surveillance and Data Security" (2022)

- American Data Privacy and Protection Act
  - 53-2 vote in House Energy & Commerce Committee (July, 2022)
  - Not (yet?) introduced this Congressional Session

- Senate efforts at children's online privacy and safety (KOSA & COPPA 2.0)

State Privacy Landscape: A Patchwork?

California Consumer Privacy Act (CCPA) of 2018

THE WALL STREET JOURNAL.

TECH

The Real-Estate Developer Who Took On the Tech Giants

After a disturbing cocktail party chat, Alastair Mactaggart bankrolled the push that led to California's landmark data-privacy bill

California state Sen. Bob Hertzberg (D., Van Nuys), left, and Assemblyman Ed Chau (D., Arcadia), right, celebrate with Alastair Mactaggart, center, after the Legislature approved their data-privacy bill on Thursday in Sacramento, Calif.

- 4th largest global economy; *de facto* U.S. law?
- "Bundle of rights": Access, Deletion, Do Not Sell My Data
- Enforced by the AG (w/limited PRA)

- Amended in Nov. 2020 by ballot initiative: **California Privacy Rights Act (CPRA)**
- Closes loopholes, new opt-out for "sensitive data"
- Creates new privacy agency
- New regulatory processes
- Applies to employee and b2b data

FORUM

A 'California Effect'? – Yes and No

No state has passed a comprehensive privacy law modeled on the CCPA – Why?

- CCPA Product of two distinct ballot initiatives
- Significant details left to ongoing regulatory processes (moving target)
- Terms and rights that are misaligned with emerging global norms

Instead, a 'Washington Privacy Act' – Template Emerged…

<u>California</u>

- New Enforcement Authority (CPPA)
- Sensitive Data 'Opt-Out'
- Broad rulemaking authority (AI, Risk Assessments, Data Minimization…)
- Applies to employee and b2b data
- Unique terms: "Business, service provider, contractor, third party…"
- Narrow private right of action (breaches)

<u>Washington Model</u>

- Enforcement by Attorneys General
- Sensitive Data 'Opt-In'
- No rulemaking authority (except Colorado)
- Only covers consumer data
- Familiar terms: "controller, processor"
- No private right of action

FUTURE OF PRIVACY FORUM

The "Washington Privacy Act" Model

Entering 2023

- Virginia (2021)
- Colorado (2021)
- Utah (2022)
- Connecticut (2022)

2023 (So far)

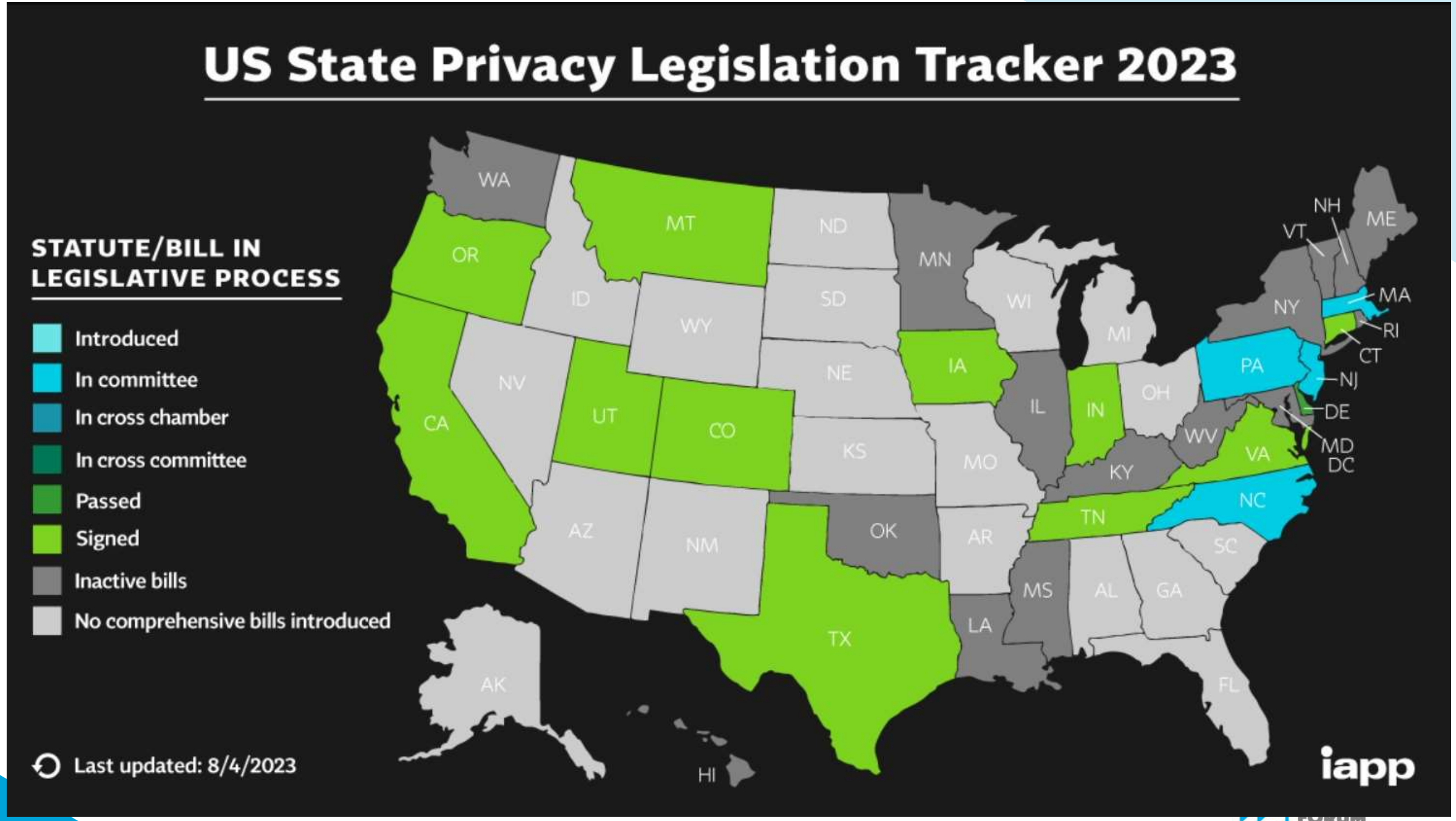
- Iowa (March)
- Indiana (May)
- Tennessee (May)
- Montana (May)
- Florida (?) (June)
- Texas (June)
- Oregon (July)
- Delaware (awaiting signature)

NOTE: *These laws share a key definitions and a common framework, but vary significantly in their scope of coverage, consumer rights, and business obligations.*

Depending on how you count, there are 12 'comprehensive' state privacy laws covering approximately a third of the U.S. population. However, these laws are just starting to take effect and become enforced.

FUTURE OF PRIVACY FORUM

US State Privacy Legislation Tracker 2023



Building Blocks - Scope

Covered Entities

- "Persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state"
- Exceptions:
  - Small Businesses (process data of fewer than 100,000 residents)
  - Businesses / data subject to existing federal privacy laws
  - Government entities; Nonprofits

Covered Data

- "Any information that is linked or reasonably linkable to an identified or identifiable individual."
- Exceptions:
  - Publicly available information
  - De-identified data
  - Pseudonymous data

Exceptions

- Broad carve-outs for businesses activities such as complying with legal obligations or law enforcement requests; providing a requested product or service; preventing security threats or illegal activity; public interest research

Building Blocks – Individual Rights

Consumer Controls:

- Confirm whether processing is taking place
- Access (and receive data in a portable format)
- Deletion
- Correct inaccurate data

Consumer Choice

- Opt-in for processing sensitive personal data
  - SPI: reveals an individuals racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, physical or mental health diagnosis or condition, genetic or biometric data, precise geolocation information, status as transgender or nonbinary, status as victim of a crime.
- Opt-out of processing for:
  - Targeted advertising
  - Sale of personal data (monetary or other valuable consideration)
  - Solely automated profiling that reaches decisions with with "legal or similarly significant effects"
- Authorized agents and Universal Opt-Out Mechanisms

FUTURE OF PRIVACY FORUM

Building Blocks – Business Obligations

- **Transparency:** Disclose data collection and processing activities
- **Data Minimization:** Don't process data for undisclosed purposes without obtaining consent
- **Service providers:** Ensure that any downstream processing is carried out pursuant to a binding contract
- **Data Security:** Maintain "reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data"
- **Non-discrimination:** Don't process data in violation of laws that prohibit unlawful discrimination
- **Non-retaliation:** Don't change costs or degrade services because of the exercise of a consumer right
- **Risk Assessments:** Document benefits of processing, risks, and mitigation measures

New Wrinkles in 2023

Ease of Compliance

- Access to a "representative summary" of personal data (Indiana)
- Affirmative defense when a business "reasonably conforms" with NIST or other privacy framework (Tennessee)
- Exceptions for complying with a UOOM signal (technical ability) (Texas)

Consumer Protections:

- Certain obligations apply to small businesses (Texas and Connecticut)
- Lowered thresholds for small business carveouts (Montana, Delaware)
- Expanded protections for adolescent data (Oregon, Delaware)
- Right to know specific third parties to whom personal data has been disclosed (Oregon)

Questions?

klamont@fpf.org

in/keirlamont

HUSCH BLACKWELL

Other Types of State Privacy Bills and Laws

David M. Stauss, Partner, CIPP/US/E, CIPT, FIP, PLS

Overview

1. Health data privacy
2. Children's data privacy
3. Biometric privacy
4. Data broker
5. Automated employment decision tools
6. Algorithmic discrimination

HUSCH BLACKWELL

Health Data Privacy

States that Passed Bills in 2023

Washington My Health My Data (HB 1155)

Connecticut (SB 3)

- Amended Connecticut Data Privacy Act
- Added consumer health data to definition of sensitive data
- Added geofence restrictions

Nevada (SB 370)

- More business-friendly version of Washington bill

HUSCH BLACKWELL

Washington My Health My Data

Enforcement

- Private right of action and Attorney General
- No statutory damages

Applicability

- Broad applicability (applies to small businesses)

Consumer Health Data

- Broad definition
- Could include ordinary products and services

HUSCH BLACKWELL

Washington My Health My Data

Collection / Sharing of Consumer Health Data

- Requires consent or necessary to provide product or service

Selling Consumer Health Data

- Requires “valid authorization”

Privacy Policy

- Must maintain privacy policy (unclear if it can be combined with other disclosures)

Rights

- Confirm processing
- Obtain list of third parties and affiliates with whom data is shared or sold and email addresses
- Revoke consent
- Deletion

HUSCH BLACKWELL

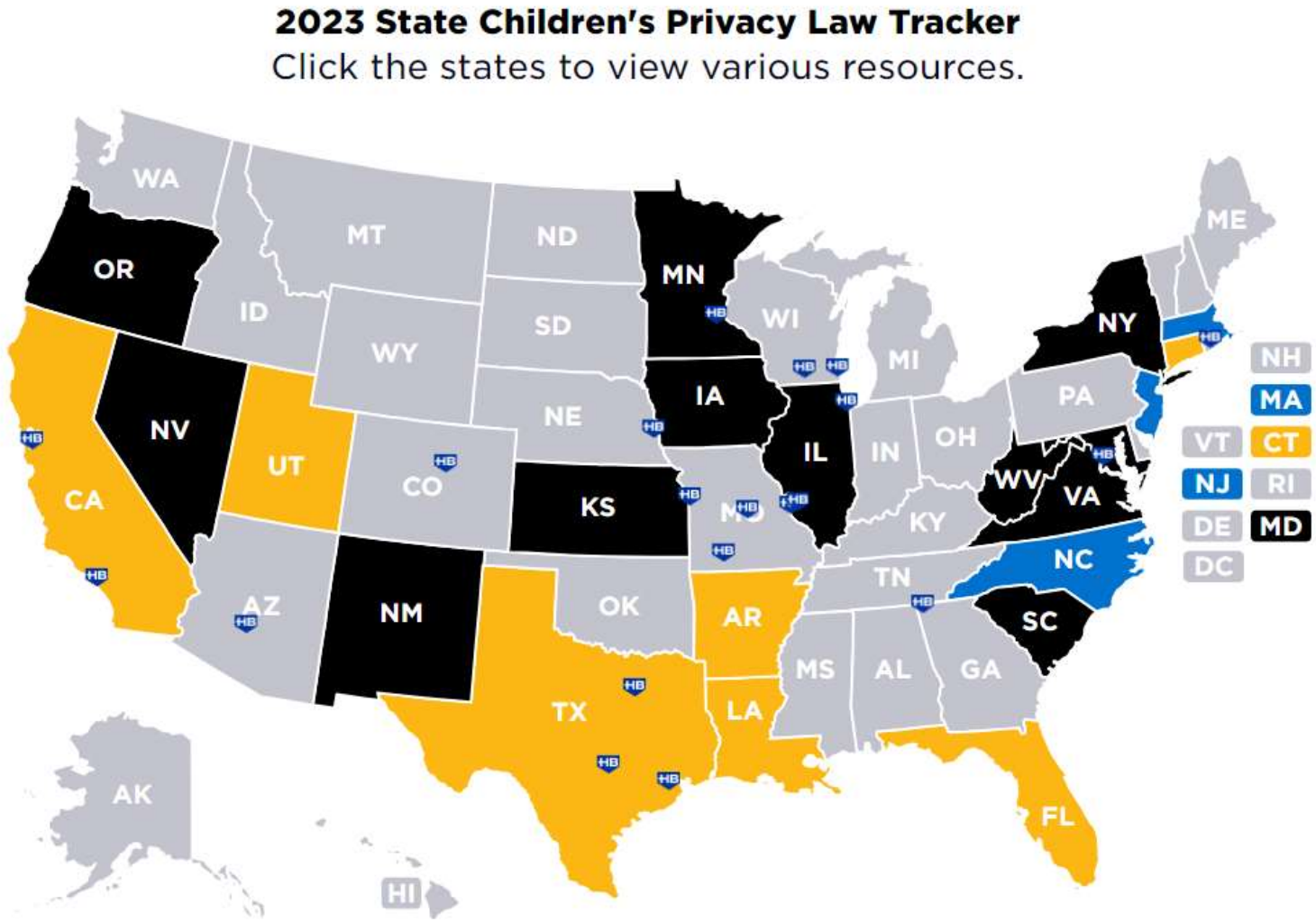
Washington My Health My Data

- Geofence restrictions
- Data processing agreements
- Access restrictions
- Technical and organizational measures

HUSCH BLACKWELL

Children's Data Privacy

State Children's Data Privacy Bills



HUSCH BLACKWELL

Different Types of Children's Privacy Bills

Age-Appropriate Design Code Act Bills

- California, Florida, Oregon, Nevada, New Mexico, Minnesota, New Jersey, and New York

Social Media Privacy Bills

- Utah, Texas, Kansas, Louisiana, Arkansas, Iowa, Illinois, North Carolina, and South Carolina

Amendment to Existing State Privacy Law

- Connecticut

Other

- Illinois, Massachusetts, Florida, West Virginia, and Virginia

HUSCH BLACKWELL

California Age-Appropriate Design Code Act (AB 2273)

Enacted

- September 15, 2022

Effective

- July 1, 2024

Applies to

- Businesses that provide online services, products or features that are "likely to be accessed by children"
- Children – Under 18 years of age

Data Protection Impact Assessment

Must be performed before offering any new online services, products or features to the public

Must consider 8 factors

"Whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service, or feature."

Document "any risk of material detriment to children that arises from the data management practices" and "create a timed plan to mitigate or eliminate the risk"

HUSCH BLACKWELL

Additional Relevant Provisions

Age Estimation

- Estimate age of child users with a reasonable level of certainty appropriate to risks that arise from data management practices of business or apply privacy and data protections afforded to children to all consumers

Default Privacy Settings

- Configure all default privacy settings provided to children by online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children

Age-Appropriate Disclosures

- Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature

HUSCH BLACKWELL

NetChoice v. Rob Bonta

Lawsuit

- NetChoice filed a lawsuit claiming that the California Age-Appropriate Design Code Act is unconstitutional

First Amendment

- Primary argument is that law violates First Amendment

Current Status

- Expect ruling on motion for preliminary injunction in coming months

HUSCH BLACKWELL

Connecticut Approach

Standard of Care

- "Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature."

Opt In

- Absent consent, cannot sell personal information of minors (i.e., children under 18), engage in targeted advertising, or profile

Data Protection Impact Assessments

- Controllers must conduct data protection impact assessments to avoid heightened risk of harm to minors

Utah Social Media Company Bills (SB 152)

- Prohibit minors (defined as individuals under 18) from holding or opening an account on a social media platform without parental consent
- Social media companies must verify the age of an existing or new Utah account holder based on rules promulgated by the Division of Consumer Protection ("Division")
- Parents must be given access to the account to view their child's posts and messages
- Prohibit certain activities such as allowing direct messaging between the account and any other user that is not linked to the account through friending and the display of advertising in the account
- Restrict a minor's access to their account from the hours of 10:30 p.m. to 6:30 a.m. unless a parent changes or eliminates that restriction
- Enforceable by the Division and a private right of action

Utah Social Media Company Bills (HB 311)

Addiction Prohibition

- Prohibits a social media company from using a practice, design, or feature on the company's social media platform that the social media company knows, or which by the exercise of reasonable care should know, causes a Utah minor account holder to have an addiction to the social media platform.

Private Right of Action

- Creates a private right of action for a Utah minor account holder for any addiction, financial, physical, or emotional harm suffered as a consequence of using or having an account on the social media company's social media platform.

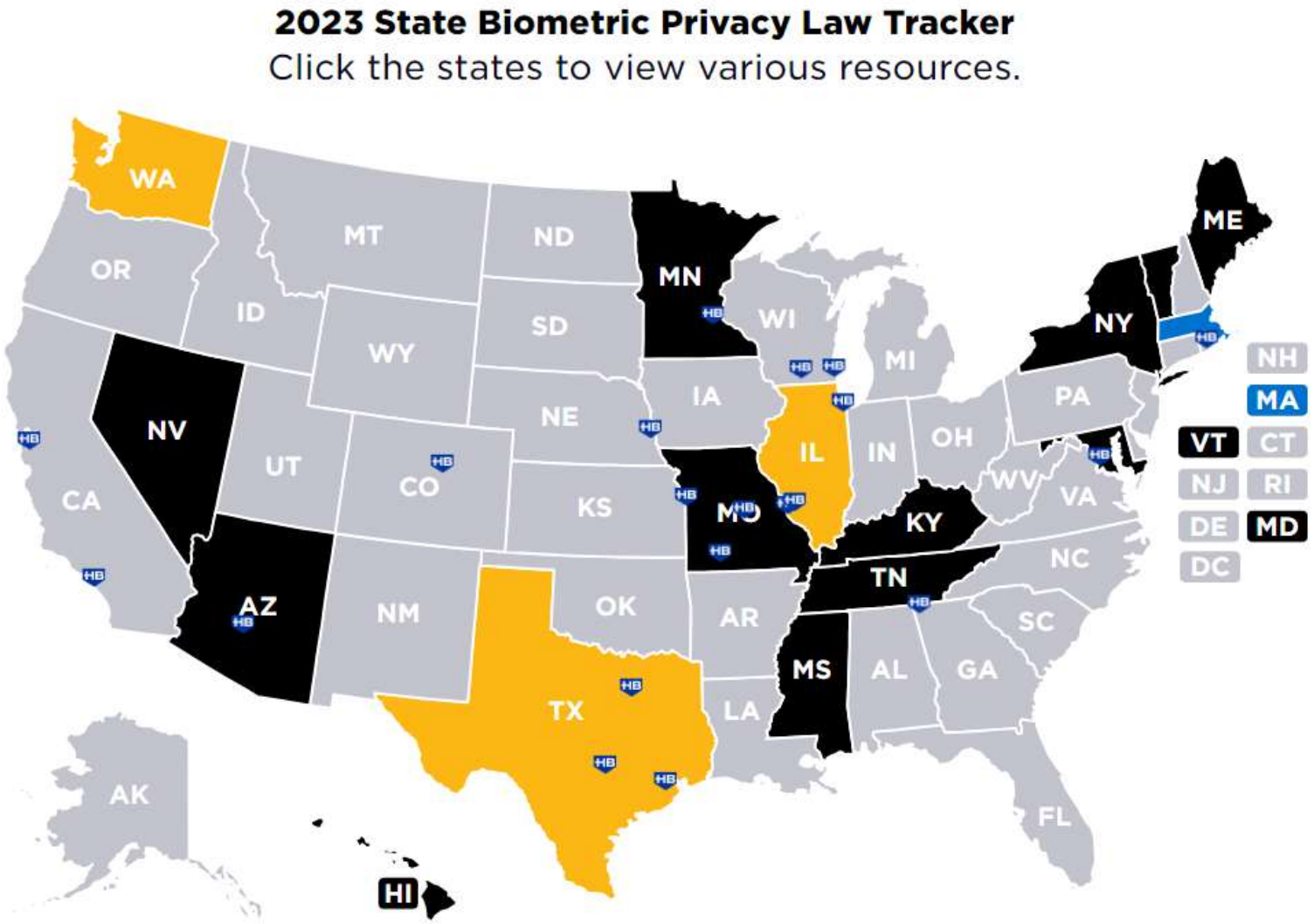
Rebuttable Presumption

- If the account holder is under the age of 16, there is a rebuttal presumption that the harm actually occurred and that the harm was caused as a consequence of using or having an account on the social media company's social media platform.

HUSCH BLACKWELL

Biometric Privacy

State Biometric Privacy Bills



HUSCH BLACKWELL

Other Types of Bills

Other Types of Bills

Data Brokers

- Passed - Oregon and Texas

Automated Employment Decision Tools Bills

- Proposed (Did Not Pass) - New Jersey, New York, and Vermont

Algorithmic Discrimination Bills

- Proposed (Did Not Pass) - California, Minnesota, Washington, D.C.

HUSCH BLACKWELL

Subscribe to our blog…

www.bytebacklaw.com

HUSCH BLACKWELL