Preparing Your Privacy Program for 2024 and Beyond

Association of Corporate Counsel Webinar

Presenters:

Gretchen A. Ramos | T: +1 415.655.1913 | RamosG@gtlaw.com

Darren J. Abernethy | T: +1 415.655.1261 | AbernethyD@gtlaw.com

NOVEMBER 16, 2023

FOR INFORMATION PURPOSES ONLY – NOT LEGAL ADVICE

www.gtlaw.com

Presenters

Gretchen A. Ramos
Global Co-Chair,
Data Privacy & Cybersecurity Group
Greenberg Traurig

Darren J. Abernethy
Shareholder,
Data Privacy & Cybersecurity Group
Greenberg Traurig

Today's Agenda

- ✓Background – Current Privacy Landscape
- ✓Privacy Program Considerations for 2024 and Beyond
- ✓Privacy Litigation Trends / Compliance
- ✓Global Goings-On
- ✓Questions

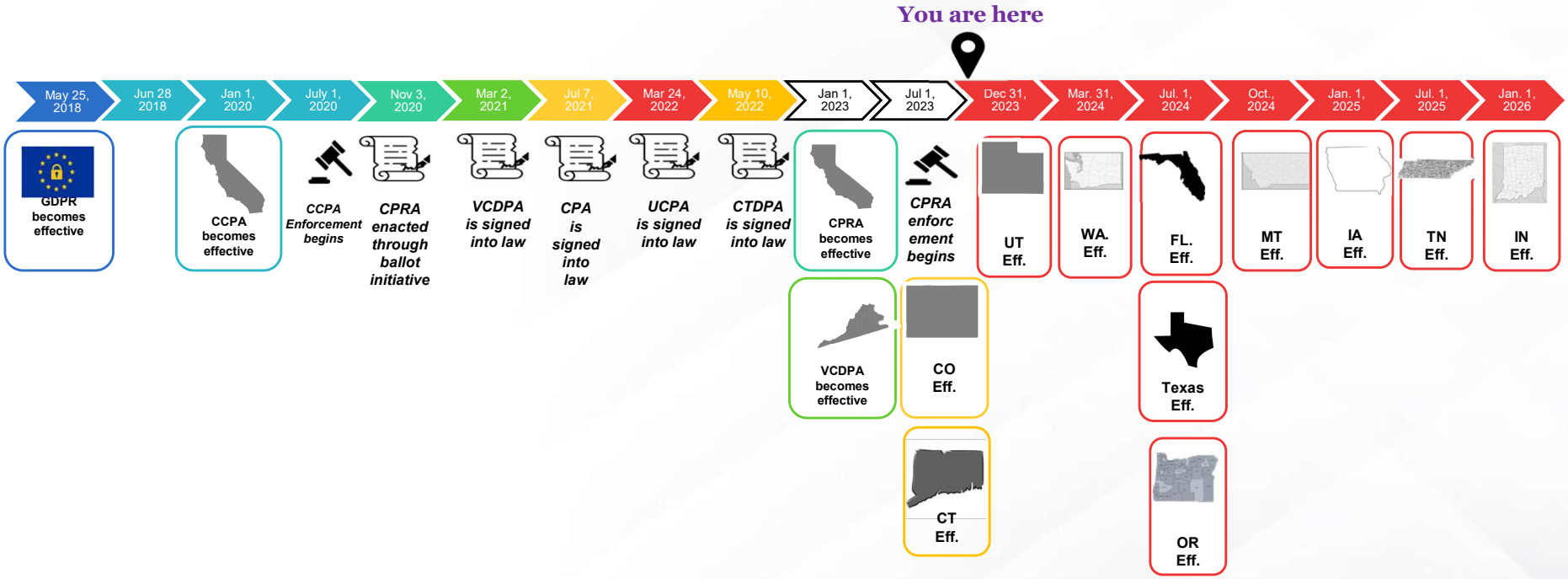
Background +
Current State Privacy Laws

The U.S. Approach to Privacy

- The United States has approximately 356 federal and state laws that impact data privacy and 232 federal and state laws that impact data security.
- On the ***federal*** level, however, there is no comprehensive privacy statute that contains all the same rights (unlike the EU's General Data Protection Regulation (GDPR)).
- To date, on the ***state*** level, so ~25% of the states (12 states) have enacted "comprehensive" consumer privacy legislation.

GT GreenbergTraurig

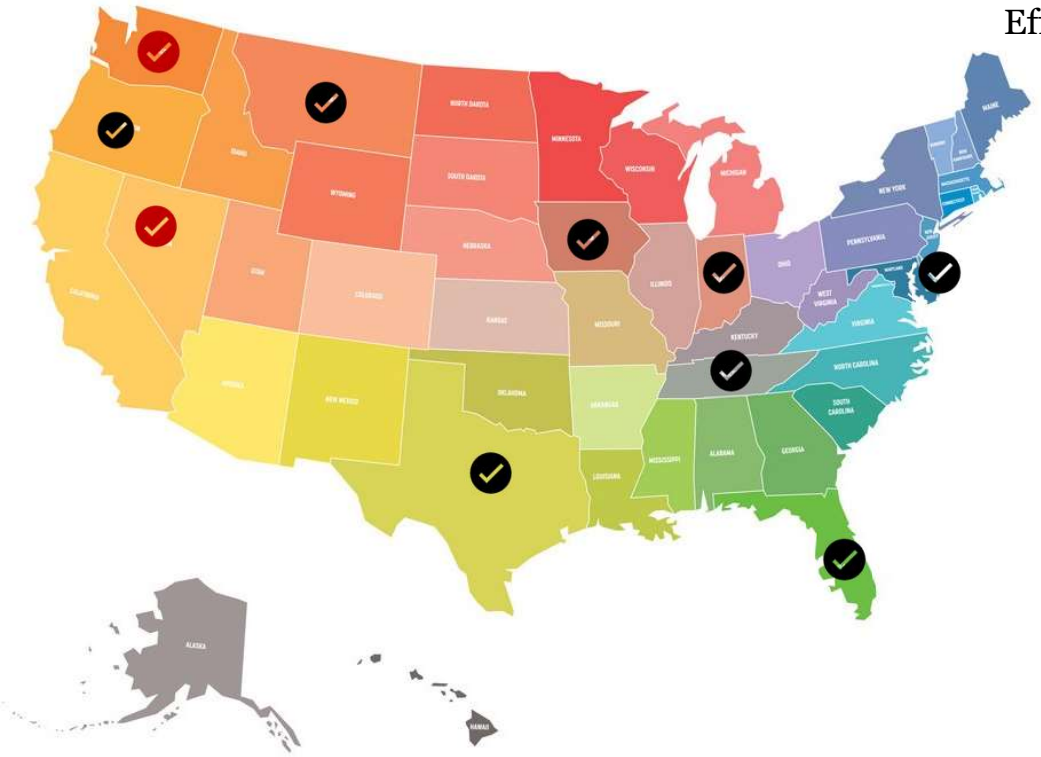
Timeline



State Privacy Laws – eff. 2023

- **California Consumer Privacy Act,** *as amended by the California Privacy Rights Act* (CCPA), eff. 1.1.23, enforced 7.1.23
- **Connecticut Data Privacy Rights Act** (CTDPA), eff. 7.1.23
- **Colorado Privacy Act** (CPA), eff. 7.1.23
- **Utah Consumer Privacy Act** (UCPA), eff. 12.31.23
- **Virginia Consumer Data Protection Act** (VCDPA), eff. 1.1.23

Privacy Legislation – Enacted 2023



Effective 2024+

- **Washington My Health My Data**, eff. 3.31.24
- **Nevada Consumer Health Data Law**, eff. 3.31.24
- **Florida Digital Bill of Rights**, eff. 7.1.2024
- **Oregon Privacy Act**, eff. 7.1.24
- **Texas Data Privacy and Security Act**, eff. 7.1.24
- **Montana Consumer Data Privacy Act**, eff. 10.1.24
- **Iowa Consumer Data Protection Act**, eff. 1.1.25
- **Delaware Personal Data Privacy Act**, eff. 1.1.25
- **Tennessee Information Protection Act**, eff. 7.1.25
- **Indiana Consumer Data Protection Act**, eff. 1.1.26

Organizational Privacy Programs – Key Considerations for 2024 and Beyond

GT GreenbergTraurig

Setting Up or Iterating a Privacy Program

- As noted, there are hundreds of privacy- and security-related laws in the U.S. and around the world
- So, how to comply without "reinventing the wheel" with each new law that's passed?
- By setting up a privacy program organized around ***common controls*** that can be adjusted as needed for the jurisdiction and scalability, in coordination with the right people, process and technology

Common Themes in U.S. Privacy Law

- Notice / transparency re: personal information collection, use and sharing
- Choice / opt-outs
- Consent
- Individual rights / access
- Security
- Proper contractual protections (and vendor management)
- Children's privacy
- Avoiding deceptive statements and practices in relation to all of the above

Initial Privacy Program Action Items

- Determine if your company is even in-scope of some or all U.S. state privacy laws
- Either way, ***inventory/map*** the data your company collects or receives about customers, consumers, employees, vendors, business partners and others
- Compare your inventory against the applicable definitions of "personal information" or "personal data"
- Determine if any exceptions/exemptions exist, or if special protections may be triggered
- Make privacy program decisions based on all of the above (e.g., do we need to collect that PI? Should we share it with others? What could we do differently?)

State Privacy Law Eligibility, Exemptions and Covered Data

GT GreenbergTraurig

Eligibility – Are You Covered?

- Applicability varies across the 12 laws but with common themes
- Usually applies to for-profit entities (***but not CO, DE, OR***) that act as controllers (and/or processors) of PI, while meeting one or more other criteria involving consumer thresholds, gross annual revenue or revenue derived from selling PI
- Beware of "common branding" for California purposes
- Florida is an outlier – must make in excess of $1 bn, and Texas defines eligibility in part as *not* "small businesses" by the SBA's definitions

Exemptions / Out of Scope

- General exceptions relating to GLBA, FCRA, HIPAA, higher education institutions and a few other federal laws and medical research purposes.
  - However, exemptions are ***not always at the entity level***...sometimes just the PI covered by those laws is exempt.
- CA, unlike the other states, covers B2B PI and employee PI as "consumer" PI.

PI *Before* U.S. State Privacy Laws

- Many U.S. federal laws, such as HIPAA and COPPA, address the processing of "personally identifiable information" (PII)
- However, then the EU GDPR, followed by the California Consumer Privacy Act came along to ***vastly expand the definition*** of "personal data" or "personal information" (together, "PI") – collected online OR offline
- CCPA uses a broad and prescriptive definition, but other states like CO, CT, UT, MT, DE, IA define PI as information that is linked or reasonably linkable to an identified individual

PI *After* State Privacy Laws

- **Identifiers** such as 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
- **Signatures**
- **Physical characteristics or descriptions**
- **Telephone numbers**
- **Characteristics** of protected classifications under California or federal law
- **Insurance policy numbers**
- **Medical information** or **health insurance information**
- Bank account numbers, credit card numbers, debit card numbers, or **any other financial information**
- **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
- **Biometric information**
- **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement
- **Geolocation data**
- **Audio, electronic, visual, thermal, olfactory, or similar information**
- **Professional or employment-related information**
- **Education information**
- **Inferences** drawn from any personal information to create a consumer profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Sensitive Personal Information

- Depending on the law, may be broader than you think!
- Opt-in consent vs. contours of a ***right to limit*** the use of SPI
- California, for example:

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

SPI – Different State Approaches

- There are effectively three different regimes for processing sensitive data under the applicable state privacy laws (listed from most restrictive to least restrictive):

- 1. **CO, CT, FL, IN, MT, TN, TX, and VA Approach** - Opt-in Consent - though be mindful of the additional requirements in CT re: CHD and FL and TX requirements re: selling SPI;

- 2. **IA and UT Approach** - Clear notice and right to opt-out; and

- 3. **CA Approach -** Right to limit the use of SPI; however, given CA's broader definition of SPI, these requirements extend to a greater amount of PI.

Other Key Features of U.S. State Privacy Laws + Privacy Program Considerations

Operational Action Items

- Evaluate your program's methods for verifying and honoring privacy requests
- Establish or update your contact templates for use with vendors, customers or recipients of "***sold***" or "***shared***" PI
- Take action if children's PI may be collected, and be aware of age-appropriate design codes (<18 y.o.)
- Scan websites and mobile apps to understand whether your company may be "selling" or "sharing" PI to any third parties, or else solidify contractual grounds for "service provider" or "processor" relationships
  - If so, understand the different types of opt-outs that are possible or may be required (e.g., GPC in CA)

Common Consumer Privacy Rights

- Right to access
- Right to delete
- Right to correction
- Right to non-discrimination
- Rights in relation to sensitive PI
- Right to opt-out of automated decision-making technology
- Right to opt out of selling/sharing/targeted advertising
- Right to know – privacy policy and just-in-time notice transparency

Contracts and Data Processing Addenda

- The state privacy laws require controllers/businesses to enter into contracts limiting service providers/processors/contractors in their ability to retain, use and disclose PI
- Also require the latter group to support the controllers in honoring consumer requests and other controller obligations
- Where do state privacy law contracts fit in w/r/t to GDPR Art. 28 DPAs and other global data processing agreement / SCC requirements?
- Should you use a global privacy addendum, a U.S. specific, or state-specific DPA?

Children's Privacy

- General rule across all states that processing <13 y.o. children's PI (including selling, profiling for targeted ads) must be done in line with COPPA and verifiable parental consent requirements
- State laws also may use a tiered system of requirements for children aged 13-16 in relation to opt-in consent for selling PI, targeting ads, or creating a consumer profile
  - CT even requires opt-in consent in order for a child to use any system designed to "significantly increase, sustain, or extend" any minor's use of such online service, product, or feature
- Status of ***California's Age-Appropriate Design Code Act*** – preliminary injunction

Enforcement

- Some states offer a “cure period,” i.e., time to fix an alleged violation after being notified of it
- Usually no private right of action
- AGs, CPPA or district attorneys
- Varying financial penalties (e.g., $7,500 per violation) and possible statutory damages
- Add-on regulations (CA, CO…)

Opt-Out of Sharing & Selling

- All current state privacy laws provide consumers with right to opt-out of selling and sharing:
  - **Selling** – disclosing PI to a third-party for money or other valuable consideration.
  - **Sharing** – sharing PI for targeted advertising purposes. **CA** is the only state that refers to it as "sharing for purposes of cross-context behavioral advertising" (and ***no consideration is required***)
- Big implications for the use of third-party trackers on websites or third-party SDKs/integrations on mobile
- If consent obtained from the consumer to share or sell PI, then it is not considered selling or sharing under these laws

Sharing/Selling Opt-outs – Website Compliance

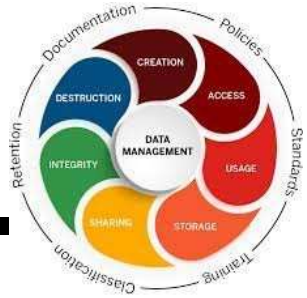
CALIFORNIA

- Websites currently required to honor opt-out preference signal (Global Privacy Control) for CA residents. *See* **https://globalprivacycontrol.org/implementation.**
- Businesses must provide 2 or more designated methods for submitting requests to opt-out.
    - Applies to collection of PI to sell or share over the phone, in a retail store, or elsewhere, thus businesses must provide notice orally or through other means to opt-out.
- Instead of posting the "Do Not Sell or Share My Personal Information" link in the footer, a business may provide the Alternative Opt-out Link in accordance with § 7015 (post "Your Privacy Rights") **OR** process opt-out preference signals in a frictionless manner in accordance with § 7025(f)-(g).

OTHER STATES

- Laws require honoring opt-out preference signals, but enforcement of the requirement delayed until 2024, and beyond.

Privacy Program Decisions to Make



- Limit consumer rights on a state-by-state basis vs. apply to everyone?
- Do any of the consumer right exceptions apply? Rights aren't absolute.
- IT updates needed for "reasonable security measures"?
- Data minimization and retention periods
- Technology to help scale the privacy program (DSARs, cookie banners/opt-outs, ***training*** for employees)

What Else Is on the Horizon?

- California CCPA regulations taking effect 3/29/2024– after judicial stay
- New CA rulemakings on cybersecurity audits, PIAs and ADM
- Federal privacy legislation?
- Regulatory emphasis on dark patterns
- New rules for data brokers (CA, OR, TX)
- More legal challenges to privacy-related laws? (social media, children's privacy, etc.)

Brief Overview of New Consumer Health Laws

GT GreenbergTraurig

Non-PHI Consumer Health Data

- In 2023, we saw new state laws spring up addressing the gap between HIPAA PHI and other health-related data not covered by HIPAA
- Washington's My Health My Data (MHMD) is chief amongst them
  - Nevada passed a similar law (minus a private right of action)
  - Connecticut amended its privacy law to add CHD as a type of sensitive data
- Also, enforcement by FTC of the Health Breach Notification Rule and use of FTC Act Section 5 in consumer health data enforcement

WA MHMD Act Overview

- Consumer health data definition
- Applicability + extraterritorial scope
  - fitness services, health tracking wearables and apps, online marketplaces selling health-related supplements, and services related to assessing, measuring or improving physical and mental health are likely captured
- "Physical and mental health status" includes what?
- Effective date for regulated entities as of March 31, 2024 (with small businesses by June 30)

WA MHMD Main Features

• Detailed consumer health data privacy policies	• Prohibitions on certain geofencing practices
• Opt-<u>in</u> consent for "collecting" or "sharing" CHD unless <u>necessary</u> for requested product/service;	• CHD "Need to know" data access restrictions;
• Signed consumer authorization for "selling" CHD;	• Contractual requirements for CHD processors;
• Consumer CHD access & deletion privacy rights;	• Applies to sharing CHD among company affiliates.

Privacy Litigation / Enforcement Trends

GT GreenbergTraurig

Risk Mitigation Action Items

- Review your website, mobile app, and consumer UX for potential "***dark patterns***"
- Understand all ***tracking technologies*** used on your digital properties, and evaluate what events are set, what PI is captured (including sensitive PI, health info, tax/fin.-related, video titles, etc.), and whether proactive ***notice*** is provided
- Understand state wiretapping laws and potentially make technical updates based on communications to, or recordings of, individuals in ***"all-party" consent*** states
- Explore a 2-3 year roadmap to understand your organization's goals in order to stay current on the regulatory environment and advise on risk
- Helping educate senior management on new regulatory emphases on openness re: data breaches and cybersecurity (and possible personal liability if not)

Enforcement of Dark Patterns

- The use of subtly deceptive practices in marketing, consent and user interfaces has seen greatly increased attention
- Accounted for in state privacy laws in relation to obtaining consent
- Federal Trade Commission and state AGs have begun enforcing here
- Work with Marketing and Web Ops teams on consumer touchpoints, UX and wording

AdTech/Wiretapping Litigation

- Wiretapping theory of liability: Recording or monitoring the contents of a communication without the required consent (laws like ***CIPA in California***)
- Why? Availability of statutory damages up to **$5,000 per violation**
- ~12 states require a form of *two-party consent* for wiretapping / invasion of privacy acts

California	Connecticut	Delaware
Florida	Illinois	Maryland
Massachusetts	Michigan	Montana
Nevada	New Hampshire	Oregon
Pennsylvania	Vermont	Washington

AdTech/Wiretapping Litigation

- **Over 600** website-based wiretapping suits filed nationwide, predominantly in California, Pennsylvania, and Maryland
  - Wiretapping-based suits, increasingly encompassing broader range of torts (invasion of privacy, conversion, trespass to chattels)
- Initially focused on ***session replay*** – with recent focus on ***chatbots*** and website ***pixels***
- Effort to apply online video titles transferred via pixels to the Video Privacy Protection Act
- Don't overlook HIPAA and the FTC Health Breach Notification Rule

SEC Imposing Liability on CISOs

- On Oct. 30th, the SEC announced charges against a publicly traded company's CISO for allegedly:
  - Making material false misstatements regarding the company's cybersecurity practices;
  - The description of a large-scale breach; and
  - Not having reasonable internal controls to safeguard important systems and IT assets
- ***C-suite is on notice*** to not mislead, indicate compliance with external standards that the company is not actually aligned with (NIST), or be aware of insufficient cybersecurity practices while doing nothing to fix them and publicly stating to the contrary
- Have a strong cybersecurity culture…or it might show up otherwise during discovery with internal IMs, emails and more

Trends: Where We Are Going

- Rise of ***mass*** arbitration
- Expansion to not only litigation re: pixels, but also analytics, fraud prevention software
  - Continued battle over the scope of data that can give rise to a wiretapping claim
- Call recording suits & AI – *again*?
- Deceptive cookie banners, biometric privacy class actions, and more

Brief Look at Global Goings-On

GT GreenbergTraurig

What Else Is Happening in 2024?

- Artificial intelligence focus, e.g., EU AI Act, implementation of GPTs, etc.
- Privacy law updates in Canada, India, Australia, Saudi Arabia and elsewhere
- Chinese data protection law updates, contracts and cybersecurity
- Challenge to the EU-U.S. Data Privacy Framework
- Google Chrome deprecation of support for most 3P cross-site cookies? 4Q24??
- Regulatory guidance focus on employee workplace monitoring
- And what else…??

Questions?

Thank You!