Reading the Tea Leaves - Privacy Compliance in 2025

Association of Corporate Counsel –SF Bay Area Webinar

Presenters:

Gretchen A. Ramos | T: +1 415.655.1913 | RamosG@gtlaw.com (bio) (LinkedIn)

Darren J. Abernethy | T: +1 415.655.1261 | AbernethyD@gtlaw.com (bio) (LinkedIn)

DECEMBER 10, 2024 **FOR INFORMATION PURPOSES ONLY – NOT LEGAL ADVICE**

Presenters

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

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

Sign up for updates at GT's Data Privacy Dish blog: https://www.gtlaw-dataprivacydish.com/

Today's Agenda

- ✓ New State Privacy Laws
- ✓ Evolving Digital Advertising Ecosystem
- ✓ Enforcement Priorities
- ✓ Litigation Trends
- ✓ Your Questions

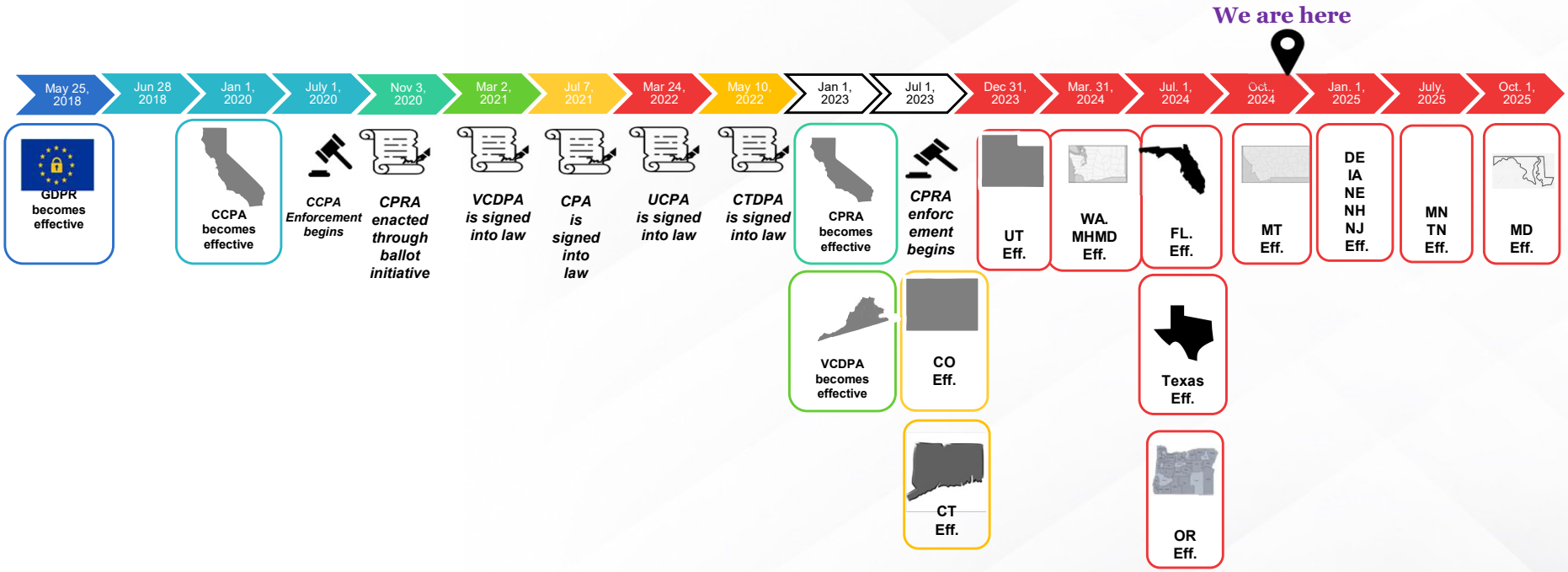
Background +
Current State Privacy Laws

The U.S. Approach to Privacy

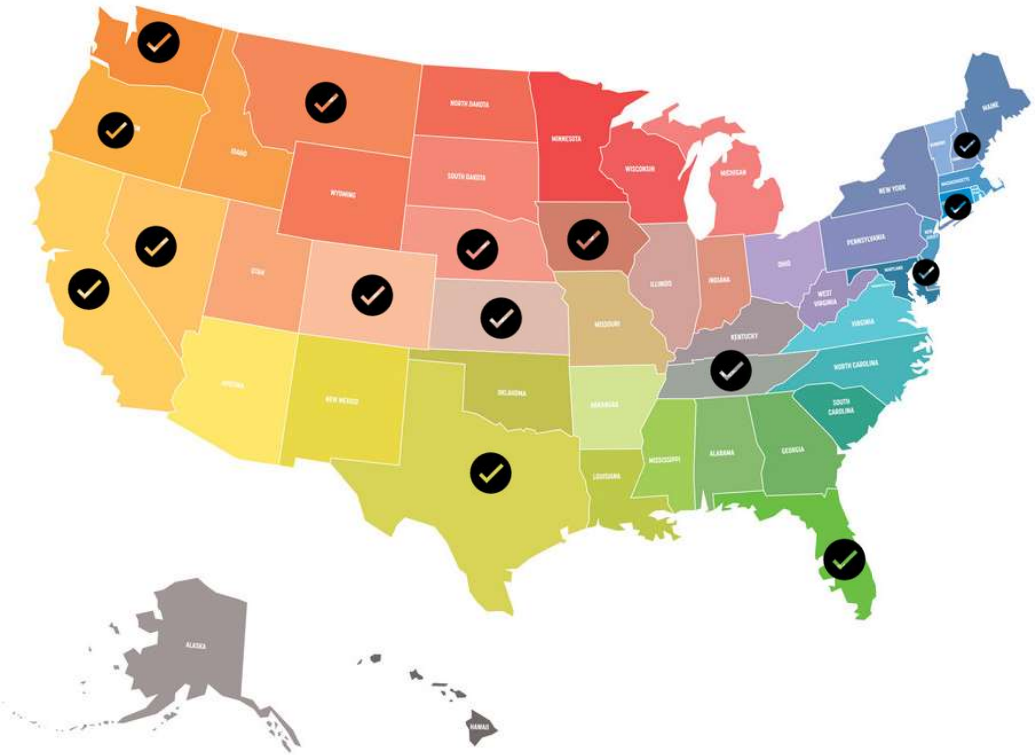
- The United States has approximately 356 federal and state laws that impact data privacy and 232 federal and state laws that impact data security.
- On the ***federal*** level, however, there is no comprehensive privacy statute that contains all the same rights (unlike the EU's General Data Protection Regulation (GDPR)).
- On the ***state*** level, 3 new state privacy laws took effect in 2024, and 8 will become effective in 2025. A total of 20 states--40% of U.S. states--have enacted "comprehensive" consumer privacy legislation.

GT GreenbergTraurig

Timeline



The State Privacy Law Landscape – Jan. 2025



- Delaware, Iowa, New Hampshire and Nebraska take effect on New Year's Day
- New Jersey takes effect on 1/15/2025
- Minnesota and Tennessee take effect in July 2025
- Maryland takes effect on 10/1/2025
- Indiana, Kentucky, Rhode Island as of 1/1/2026…and on

Commonalities Across State Privacy Laws

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

State Privacy Laws

Baseline Approach	⇒	Virginia, Indiana, Kentucky, Tennessee, Florida, Texas, Nebraska, Rhode Island
Fewer Obligations	⇒	Utah, Iowa, Nevada
More Obligations	⇒	Colorado, Connecticut, New Hampshire, New Jersey, Montana, Delaware, Oregon
Outlier States	⇒	California, Maryland, Minnesota, and Washington & Nevada consumer health data laws

Differences - Eligibility Thresholds

- Revenue requirement: Utah and Florida
- Controlling or processing PI of certain number of consumers (varies by state)
- “Selling” or “sharing” (as defined in the CPRA) 100K CA consumers’ PI
- Derive a certain percentage of revenue from the sale of PI (varies by state)
- Texas is an outlier – applies to entities that Are are not considered small businesses as defined by the U.S. Small Business Administration (SBA)

Differences - Exemptions / Out of Scope

- General exceptions relating to GLBA, FCRA, FERPA, and HIPAA 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.

Unique Compliance Requirements

- *Strict Minimization Standard*: **Maryland** requires controllers to limit their collection of PI to what is necessary and proportionate to provide or maintain specific product or service. No selling sensitive personal information.

- *Profiling*. **Minnesota** provides a right for consumers to question the result of profiling in furtherance of decisions that produce legal or similarly significant effects, to be informed of reason profiling resulted in the decision, to review PI used in profiling and to correct PI and have profiling decision reevaluated if inaccurate PI used.

- *Third Parties List*. **Oregon** and **Minnesota** provide consumers the right to obtain a list of specific third parties to whom controllers disclose consumer's PI.

- *Documentation Requirements*. **Maryland** requires DPIA for processing activities presenting heightened risk of harm to consumer, includes an assessment of each algorithm used. **Minnesota** requires controllers maintain written description of policies/procedures adopted to comply with state privacy law.

Sensitive Personal Information

- Most state laws require opt-in consent to process SPI
- Utah and Iowa – require clear notice and right to opt-out
- California is unique – offers a ***right to limit*** the use of SPI
- SPI definitions vary among state laws, especially in relation to medical/health related information

Other Types of State Privacy Laws

- Consumer health data laws (CHD) (WA, NV, CT) and their broad scope
- Children's age-appropriate design codes (AADC) (CA, MD, U.K., state bills)
- Data broker laws (VT, CA, OR, TX)
- Aspects of artificial intelligence in laws (e.g., CO's AI law C.R.S. 6-1-1701)

Digital Advertising Ecosystem

GT GreenbergTraurig

2024 Advertising Technology Updates

- Momentum towards—and then abandonment—of plan to sunset support for cross-site 3rd party cookies in Google's market-dominant Chrome web browser
  - Status of Google's Privacy Sandbox proposals
  - Open questions re: the path ahead
- Further states' adoption of "opt-out preference signals" (OOPS!)
- NY AG guidance on website privacy controls and cookie banners (in the absence of a consumer privacy law, on the basis of UDAP deception powers)
- FTC blog posts regarding both hashing and data clean rooms

Possible Cookie Alternatives in 2025

- 1st party data strategies
- Privacy Sandbox – Topics API for web (and maybe mobile)
- Contextual advertising
- CRM-based advertising
- Universal identifiers
- Conversion APIs
- Data clean rooms
- Other possibilities…

FTC and State Regulators' Enforcement Trends

GT GreenbergTraurig

FTC Enforcement

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Recent Priorities

- Health privacy and tracking technologies (*GoodRx*, *PreMom*, *BetterHelp*)
- Location data (*Kochava*, *Gravy Analytics/Venntel*, *Mobilewalla*)
- Deceptive claims re: facial recognition software (*IntelliVision Technologies*, *Evolv Technologies*)
- Final rule adopted for "Click-to-Cancel," for ending recurring subscriptions and memberships
- Dark patterns (*Amazon* and "Bringing Dark Patterns to Light" report)

Impact of New Administration

Recent State Privacy Priorities

- Children's privacy and the use of mobile application software development kits
  - See GT Data Privacy Dish: ***Operational Takeaways from the Latest CCPA Enforcement Settlement (Hint: SDKs and Consent for Children's Data Don't Just Live in a Pineapple Under the Sea…)*** **(link)**
- Texas AG lawsuits for re: car manufacturer selling data to develop "driver scores" or selling driver info to insurance companies without notice or consent
- New rulemakings in California– in November 2024, the CPPA regulator voted to advance the proposed rulemaking package for insurance, cybersecurity audits, risk assessments, automated decision-making technology (ADMT)
- CA enforcement advisories on data minimization and dark patterns

Litigation Trends

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

- **Hundreds of** website-based wiretapping suits filed nationwide, predominantly in California, Pennsylvania, Florida, Massachusetts and Maryland
  - Wiretapping-based suits, increasingly encompassing broader range of torts (invasion of privacy, conversion, trespass to chattels)
- Initially focused on ***session replay*** – then focus on ***chatbots***, website ***pixels*** and ***VPPA***
- Changes in mass arbitration provisions
- Don't overlook HIPAA and the FTC Health Breach Notification Rule

Trends: Where We Are Going

- Expansion to not only litigation re: pixels, but also alleged violations involving:
  - CA Song-Beverly Consumer Warranty Act
  - Embedding tracking pixels in emails
  - Site operators' monetization of website search bar search terms
  - Trap-and-trace claims, including in relation to geolocation
  - Voice recognition software

In-House Counsel Action Plan

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

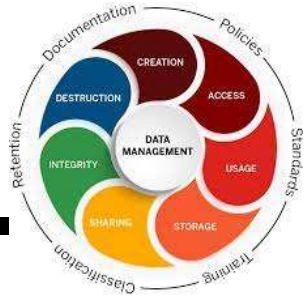
Initial Privacy Program Action Items

- 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?)

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, CO or elsewhere)

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" – security framework to follow?
- Data minimization and retention periods
- Technology to help scale the privacy program (DSARs, cookie banners/opt-outs, ***training*** for employees)

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)

Questions?

Thank You!

Gretchen A. Ramos | T: +1 415.655.1913 | RamosG@gtlaw.com (bio) (LinkedIn)

Darren J. Abernethy | T: +1 415.655.1261 | AbernethyD@gtlaw.com (bio) (LinkedIn)

GT GreenbergTraurig