



You're Not in Kansas Anymore, Tarheels: Navigating the Complex Landscape of Privacy Law

November 6, 2024
The Hamilton
Sponsored by Troutman Pepper



1

Panelists



Josh Davey
Partner | Charlotte
Troutman Pepper



Matt Mrkobrad
Associate General
Counsel | Wells
Fargo



Lissette Payne
Associate Counsel
Privacy, AVP |
(Formerly) LPL
Financial



Kim Phan
Partner | Washington,
D.C.
Troutman Pepper



2

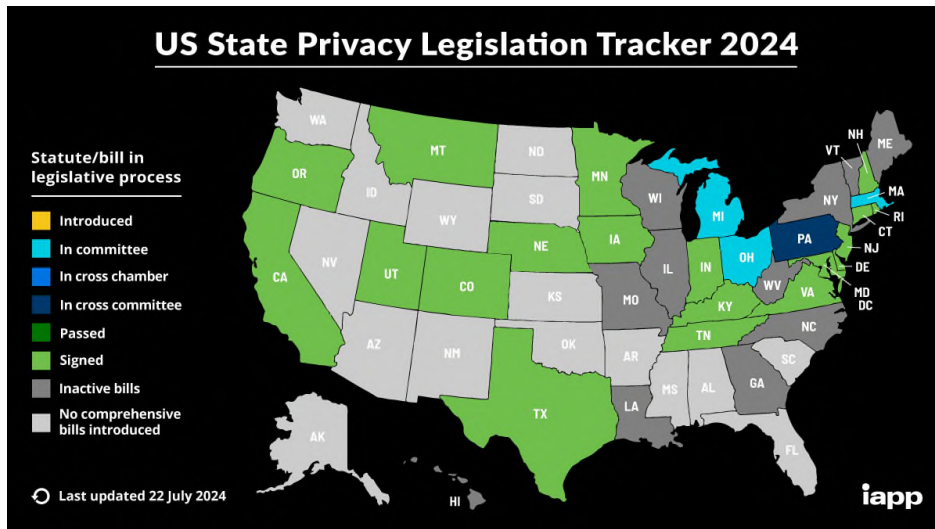
State Activity

Kim Phan



3

New State Comprehensive Privacy Laws



4

State Data Breach Notification Laws

Utah now requires
AG notification.
(5/1/24)

Texas AG shortened
to 30 days. (9/1/23)

Florida Adds
biometric and
geolocation
information. (7/1/24)

Pennsylvania adds
online credentials,
medical, and health
insurance
information. (5/2/23)



troutman
pepper

7

5

New York Department of Financial Services

- On November 1, 2023, New York Governor Kathy Hochul announced that the state's Department of Financial Services (NYDFS) has amended its Cybersecurity Regulations to "enhance cyber governance, mitigate risks, and protect New York businesses and consumers from cyber threats."
- According to the NYDFS, key changes in the regulations include:
 - enhanced governance requirements;
 - additional controls to prevent unauthorized access to information systems and mitigate the spread of an attack;
 - requirements for more regular risk assessments, as well as a more robust incident response plans;
 - updated notification requirements; and
 - updated direction for companies to invest in at least annual training and cybersecurity awareness programs that are relevant to their business model.
- The newly amended compliance requirements will take effect in phases.

troutman
pepper

21

6

Contracting & Vendor Agreements

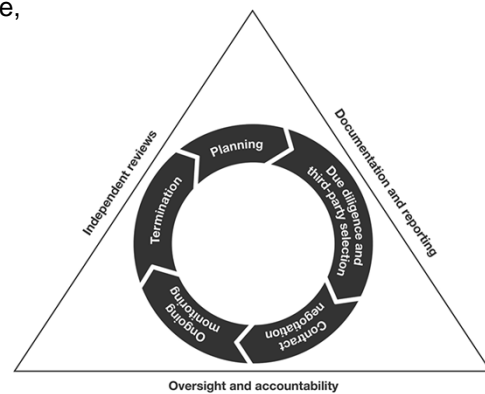
Lissette Payne



7

Interagency Guidance on Third-Party Relationships

- **Planning** (assess risk and complexity, strategic purpose, PII volume, etc.)
- **Due Diligence** (business strategy, financial condition, experience, insurance, etc.)
- **Contract** (performance metrics, ownership, liability, insurance, complaints, etc.)
- **Ongoing Monitoring** (quality control, escalation of issues, etc.)
- **Termination** (breach, alternatives, transition, data retention, etc.)



June 2023 Federal Bank Regulatory Agencies Guidance



8

How to Manage Third-Party Service Provider Risks

- There are several different ways to structure third-party service provider risk management processes.
- Important factors to consider:
 - Due diligence during the selection process
 - Contract protections
 - Periodic independent reviews, monitoring, audits, and corrective action
 - Managing subcontractors
 - Internal oversight and accountability (e.g., risk assessments, ownership, etc.)
- Overall, the establishment of a clear and thorough risk management process is crucial to assess and mitigate risk from third-party relationships.



9

9

CCPA Requirements and Impact on Third-Party Relationships

The California Consumer Privacy Act (**CCPA**) requires covered entities to manage service provider and third-party relationships

Notification

Remediation

PII – Limited and Specified Purposes

Business Obligations

Other Considerations

- Know the definitions of service provider
- Businesses may monitor service provider compliance
- Retention limitations
- Segregation of data



10



11

Current and Proposed Laws and Regulations for AI Governance

Current Laws and Regulations

- US Sectoral Laws with Privacy Focus Financial (FCRA, FACT), Employment (ADA, EPA, Title VII), Health housing (HIPAA), Housing (FHA), Education, Insurance
- US State and Local AI Laws (Colorado AI Act, [NYC AI Bias Law](#), [Nevada](#))
- US Executive Orders and Acts* – [National AI Initiative Act of 2020 \(NAIIA\)](#)
- US Consumer Protection Laws – FTC Act
- EU & UK GDPR & US State Privacy Laws – Regulations of ADM and profiling
- EU Digital Strategy – [EU AI Act](#)
- Chinese Regulations on AI – [2021 Rec. Algos](#) & [2022 Deep Synthesis](#)

Proposed and Pending Laws and Regulations

- US Federal Laws – [US Algorithmic Accountability Act](#)
- More US State Privacy Laws with AI in mind + [CA AB-311](#) & [CT SB 1103](#)
- Other International Laws – [Brazil draft regulation](#) & [Canada AI and Data Act \(AIDA\)](#)



Overlapping obligations and considerations may require the simultaneous consideration of specific and conceptual requirements, and analysis of inputs, outputs, and outcomes



Technologically & Jurisdictionally Complex – Generally additive to existing compliance obligations with extended timelines for implementation

12

12

Emerging Best Practices for AI Governance

AI Governance and Key Principles	Data Governance Understand & Account	Data Governance Control	Data Governance Security	Risk Assessments Core Privacy	Risk Assessment AI Focus
<ul style="list-style-type: none"> Adopt Data Collection, Use and Sharing Principles Adopt an AI Risk Framework (e.g., NIST) & Policies Establish an AI Governance Committee* 	<ul style="list-style-type: none"> Conduct and maintain dynamic data inventories and system maps Operationalize data lineage and hygiene controls Adopt and adhere to data retention and deletion policies 	<ul style="list-style-type: none"> IP/Scraping, Bias and Privacy Guidelines Standard Rate Limiters to Detect Data Extraction Robot Exclusion Protocol (robots.txt) to protect WCG content 	<ul style="list-style-type: none"> Encryption at rest and in motion, heightened access controls, more complex passwords, enhanced log monitoring 	<ul style="list-style-type: none"> Privacy Threshold Assessment (PTA) Data Protection Impact Assessments (DPIAs) Vendor Risk Assessments 	<ul style="list-style-type: none"> Targeted Assessments & AI Specific Assessments Third-Party Bias Review of Ingest and Output

13



13

Emerging Best Practices – Commercial & Operational

Marketing & Commercial Terms	Marketing & Commercial Terms	Training and Awareness	Regulatory Readiness
<ul style="list-style-type: none"> Don't promise or market "AI" before conducting the assessments described. Ensure your commercial Terms clearly spell out roles, responsibilities, assumptions and accountability for personal information and AI risk 	<ul style="list-style-type: none"> Enable your sales team with documentation/ product compliance sheets Ensure product documentation that accompanies sold products meets regulatory disclosure requirements 	<ul style="list-style-type: none"> Enhance compliance training to address AI use for internal (productivity) and product development purposes Develop job aids and guidelines for roles 	<ul style="list-style-type: none"> Stay abreast of legislation and ensure your story is supported by your internal diligence


14



14

Litigation Trends

Josh Davey



troutman
pepper

15

AdTech in the headlines

Video Streamer FloSports Sued Over Data Sharing with Facebook

18 hospitals, health systems facing lawsuits for healthcare data-sharing

Louisiana systems hit with lawsuits for allegedly sharing patient data with Facebook

New Wave of "Live Chat" and "Key Stroke" Wiretapping Class Actions Hits California Courts

Netflix Settles Privacy-Violations Lawsuit for \$9 Million

Is the Video Privacy Protection Act a New Litigation Weapon for Consumers?

SPORTS TV NEWS

NBA Sued For Providing Digital Data To Meta Without Consent

NFL Is Latest Target in Lawsuits Over Data-Sharing With Meta

ESPN Accused Of Data Sharing Without Consent In Class Action Lawsuit

Boston Globe Class Action Claims Newspaper Shares Subscriber Data With Facebook Without Consent

Privacy Law Trends to Watch: Wiretapping Class Actions Focused on Session Replay

Sephora to pay \$1.2m to settle Cali privacy law claims

troutman
pepper

16

Litigation and Regulatory Issues on the Rise!

Regulatory

- International Focus for years
- New Comprehensive state laws
- New focused state laws (health care information)
- New FTC focus (sensitive data sharing—health care again?)

Litigation

- Wiretapping/Surveillance
- Invasion of Privacy
- Video Privacy Protection Act
- Confidential Medical Information Protections
- HIPAA

17



17

Meta Pixel Litigation

In re Meta Pixel Healthcare Litigation, (N.D. Cal.) and *Alistair Stewart v. Advocate Aurora Health Inc., et al.*, (N.D. Ill.).

- Putative class actions alleging millions of patients had their medical privacy violated through use of tracking technologies used to track their actions with regard to patient portals and patient scheduling applications.
- Plaintiffs contend the Meta Pixel shares with Meta certain confidential medical information associated with their activities on patient portals used by medical providers.
- Claims: (a) violations of CIPA; (b) violations of CMLA; (c) Wiretap Act; (d) invasion of privacy; (e) breach of express and implied contract; (f) negligence; and (f) unjust enrichment.
- Defenses: (a) consent; (b) information is deidentified; (c) no intent; (d) medical information is filtered and not shared; (e) lack of ascertainability of class; (d) lack of commonality and typicality making class certification improper.

18



18

Video Privacy Protection Act

- The Video Privacy Protection Act (“VPPA”) is a federal statute that has its origin in the 1987 confirmation hearings concerning Judge Robert Bork’s nomination to the United States Supreme Court.
- The VPPA prevents a “video tape service provider” from “knowingly” disclosing “personally identifiable information” about one of its consumers “to any person.”
- The VPPA provides for liquidated damages in the amount of \$2,500 per violation and reasonable attorneys’ fees. 18 U.S.C. §§ 2710(b) and 2710(c)(2).
- Being pursued on a class claims to challenge website providers who offer video content that utilizes pixel and cookie technology
 - Digital
 - Streaming companies
 - Social Media Companies
- States have similar laws precluding sharing of video watching activities of an identifiable individual

19



19

State Surveillance Law Claims

- Individuals are asserting claims under various state surveillance laws for the unlawful collection of information through use of tracking technologies.
- Theory - entities are using tracking technologies to intercept, wire or electronic communications, in violation of applicable state surveillance law.
- State laws typically provide for a private right of action to recover liquidated damages, attorneys’ fees and costs and injunctive relief.
- Defenses include: actual or implied consent, statute of limitations, lack of commonality and typicality.

20



20

California Information Privacy Act (CIPA)

- Prohibits recording, monitoring, eavesdropping on a confidential communication.
- Anyone who “reads, or attempts to read, or to learn the contents” of a communication “without the consent of all parties to the communication” is in violation of CIPA.
- Four elements:
 - Intentional act
 - Neither party consented to the act
 - The communication was confidential
 - An electronic device was used during the act
- CIPA provides for a \$5,000 per violation statutory penalty, with no requirement to prove actual damages.



21

21

Confidentiality of Medical Information Act (CMIA)

- Among other things, the CMIA (1) prohibits covered health care providers from disclosing medical information regarding a patient, enrollee, or subscriber without first obtaining authorization, and (2) requires covered health care providers that create, maintain, store or destroy medical information to do so in a manner that preserves the confidentiality of such information.
- Defines “medical information” as any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment. “Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that reveals the individual’s identity.
- **Damages**
 - For negligently released confidential information or records, either or both nominal damages of \$1,000 and the amount of actual damages, if any, sustained by the patient. **It shall not be necessary to prove that the plaintiff suffered or was threatened with actual damages to recovery nominal damages.**
 - For knowingly and willfully disclosing or using medical information shall be liable for an administrative fine not to exceed \$2,500 per violation.

22

22

Tracking Technologies Existing and Emerging Regulations

US State Laws:

- **California**—Opt out of “sale” or “sharing for cross-contextual advertising”
 - Cross Contextual Advertising defined as targeting of ads to a consumer based on consumer’s personal information obtained from the consumer’s activities across businesses, distinctly-branded websites, apps, or services, other than the one with which the consumer is intentionally interacting.
- **Other states**—(CO, CT UT, and VA in 2023 with others to follow in 2024):
- Opt out of “Targeted Advertising” or automatic decision making/profiling in furtherance of decisions that produce legal or similarly significant effects.
 - Targeted Advertising usually defined as: displaying ads to consumer where ad selection is based on personal data obtained or inferred from that consumer’s activities over time and across nonaffiliated websites or apps to predict such consumers preferences or interests. Usually exceptions for contextual ads or ads on companies own properties.
- GPC and Sales
 - Most states also require opt-outs for “sale” of personal information, which can be narrowly defined as exchange for monetary consideration or broad to include any consideration or value.
 - CA and other states, including CO require that company’s honor Global Privacy Controls

23



23



24

