Unlocking the Mysteries of Privacy (Part I)

AI Regulation and the Intersection with Privacy Laws

April 11, 2024

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
Elaine.Harwell@Procopio.com
619.906.5780

Yulian Kolarov
Associate
Yulian.Kolarov@Procopio.com
619.906.5683

Overview of Discussion

- What's New in Privacy
  - American Privacy Rights Act
  - State data privacy laws
- Increased AI Regulation
  - General overview
  - California Privacy Protection Agency's new regulations for AI and automated decisionmaking technology
- How can companies prepare?

What's New in Privacy:
American Privacy Rights Act

- New bipartisan federal legislation unveiled on Sunday, April 7, 2024 (American Privacy Rights Act)
  - Introduced by key legislators: Maria Cantwell (D-Wash), Senate Commerce Committee Chair and Cathy McMorris Rodgers (R-Wash), House Energy and Commerce Committee Chair
- Intended to set national baseline for how companies can collect, use, and transfer data on the internet, including:
  - Providing the right to opt out of targeted advertising and stop the sale of personal data
  - Setting data minimization requirements (collect only as much information as needed to offer specific products to consumers)
  - Providing the right to access, delete, and transport data between digital services
  - Obtain affirmative express consent before transferring sensitive data to third party
- How does it resolve the two prior key issues preventing passage of federal privacy law?
  - Preempt the dozen plus "comprehensive" state privacy laws, including CCPA, while allowing more targeted laws like health or financial data privacy laws
  - Allows private right of action, with attorneys' fees

What's New in Privacy:
American Privacy Rights Act (con't)

- How would it regulate AI?
  - Prevent companies from using personal information to discriminate against them
  - Notice and opportunity for individuals to opt out of companies' use of algorithms to make important eligibility decisions
- Enforcement
  - Federal Trade Commission
  - State enforcement: State attorneys general, chief consumer protection officer of a State, or officer of the State authorized to enforce privacy or data security laws
  - Consumers
- Thresholds for application; would not apply to "small businesses"

What's New in Privacy:

New state comprehensive privacy laws

- All new state privacy laws include general requirements for consumer-facing AI (automated decision-making)
  - California, Colorado, Connecticut, Utah, Virginia: effective 2023 or earlier
  - Texas, Oregon, Florida: effective July 1, 2024
  - Montana: effective October 1, 2024
  - Iowa, Delaware, New Hampshire: effective January 1, 2025
  - New Jersey: effective January 15, 2025
  - Tennessee: effective July 1, 2025
  - Indiana: effective January 1, 2026
  - Kentucky and Maryland – passed laws in 2024
- State laws generally provide consumers opt-out rights when AI algorithms make high-impact decisions
- California Privacy Protection Agency currently drafting regulations (expected in 2025)
- Colorado privacy regulations includes requirements for companies to include AI-specific transparency statements in privacy policies
- Data privacy impact assessments (DPIAs) documenting:
  - Explanations of training data
  - Explanations of logical and statistical methods used to create AI
  - Evaluations of accuracy and reliability of AI
  - Evaluations for fairness / disparate impact

Increased AI Regulation:
What else is happening?

- 2023 saw Executive Action by the White House on AI: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House
  - Sets priorities in the areas of AI safety and security, privacy, equity and civil rights, workers rights, promoting innovation and competition, and responsible use of AI
- EU AI Act: risk-based approach that applies across all industries, includes transparency requirements
- State and federal lawmakers will continue to introduce a variety of AI-related proposals (generally focused on specific AI-use cases)
  - AI in recruitment or employment (New York, Illinois, and Maryland all regulate automated employment decision tools for screening candidates or employment decisions)
  - EEOC and DOJ jointly issued guidance on use of AI tools in employee hiring

Increased AI Regulation:
What else is happening? (con't)

- FTC will continue to be active in the AI space
  - Rulemaking authority – aimed at "commercial surveillance" and data security, but also ADMS
  - Using existing authority under various consumer protection laws to expand AI enforcement
    - Section 5 of the FTC Act (unfair business practices)
    - Fair Credit Reporting Act
    - Equal Credit Opportunity Act
    - Children's Online Privacy Protection Act (COPPA)
  - Recent AI-related enforcement actions by the FTC:
    - Weight Watchers: Required WW to delete entire AI algorithm it developed for a weight-loss app, including algorithms that had been trained using data from the weight-loss app. FTC contended WW marketed app to kids under 13 in violation of COPPA.
    - Everalbum: Online photo-storage platform required to delete a facial-recognition algorithm it trained using photos users stored on its platform. FTC alleged company told users they could turn off facial recognition features, but even if they did, company continued to use photos to train facial-recognition AI. FTC contended this was deceptive conduct that violated Section 5 of FTC Act.

AI Privacy Law Developments:

California Privacy Protection Agency AI regulation

- California Privacy Protection Agency (CPPA) continues work on its next rulemaking package relating to cybersecurity audits, risk assessments, and automated decision making.
  - Draft regulations would require "every business whose processing of consumers' personal information *presents significant risk to consumers' security*…complete a cybersecurity audit."
  - Draft cybersecurity audit regulations would require businesses that meet the applicability thresholds to assess and document "how the business' cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information."

CPPA Rulemaking

Definitions

Section 7001:

- "Artificial intelligence" — a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments.
- "Automated decision-making technology" (ADMT) — technology that processes personal information and uses computation to execute a decision, replace human decision-making, or substantially facilitate human decision-making.
  - This includes "profiling" — automated processing of personal information to evaluate a person's personal aspects in order to analyze or predict aspects concerning their intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements.

CPPA Rulemaking

Risk Assessments: Who is subject?

Section 7150

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy . . . must conduct a risk assessment before initiating that processing.

(b) "Significant risks" includes:

(i) selling or sharing personal information

(ii) Processing sensitive information

(iii) Using ADMT for a significant decision concerning a consumer or for extensive profiling

(iv) Processing personal information of consumers to train ADMT or AI for specific purposes under the statute

- Statute provides examples.

CPPA Rulemaking

Risk Assessments: What is required?

Section 7152:

- Identify its purpose for processing consumers' personal information.
- Identify the categories of personal information to be processed and whether they include sensitive personal information.
- Identify certain operational elements of its processing.
- Identify the negative impacts to consumers' privacy associated with the processing.
- Safeguards the business plans to implement to address the negative impacts.

Section 7153 sets out additional requirements for processing personal information to train ADMT or AI

Section 7155 sets out requirements for timing and retention of risk assessments

- At least every 3 years business must review and update its risk assessment for accuracy
- Immediately update when there is a material change to processing activity
- Retain for as long as processing continues or 5 years after completion of assessment, whichever is later

CPPA Rulemaking

Risk Assessments: Compliance with other laws & submission to Agency

Section 7156:

- If the other law or regulation meets all the requirements of California, the business is not required to conduct a duplicative risk assessment.
- Must supplement the risk assessment if the other law or regulation does not meet all parts of the California requirements.

Section 7157:

- First Submission — 24 months from date of regulations to submit assessment to the agency.
- Annual Submission — after the first submission, it must submit one every year
- Statute lists what materials must be submitted.
- Must be provided within 10 days of a request by the Agency or Attorney General

CPPA Rulemaking

ADMT: Who is subject to the ADMT regulations?

Section 7200:

Businesses that use ADMT in the following manner:

(1) For a significant decision concerning a consumer

(2) Extensive profiling of a consumer

(3) Training ADMT

CPPA Rulemaking

ADMT: “Significant Decision”

- “Significant decision” means a decision using information that results in access to or denial of:
  - Financial or lending services, housing, or insurance;
  - Education enrollment or opportunity;
  - Criminal justice;
  - Employment or independent contracting opportunities or compensation;
  - Healthcare services; or
  - Essential goods or services.

CPPA Rulemaking

ADMT: Pre-use Notice Requirement

Section 7220:

- Pre-use Notice must inform consumers about the business's use of ADMT and consumers' rights to opt-out of and to access information about the business's use of ADMT.
- Presented prominently and conspicuously before processing of personal information using ADMT.
- Presented in the manner in which the business primary interacts with the consumer.
- Include:
  - Plain language explanation of the specific purpose for which business proposes.
  - Description of right to opt-out and how to submit a request.
  - Description of right to access information
  - That business is prohibited from retaliating against consumers for exercising their rights.
  - Additional information about how ADMT works.

CPPA Rulemaking

ADMT: Requests to Opt-Out

Section 7221(c):

- Must provide two or more designated methods for submitting opt out requests. At least one method must reflect the manner in which the business primarily interacts with the consumer.
- Statute provides various examples.

Exceptions:

- Use of ADMT is necessary to achieve, and used solely for, security, fraud prevention, or other safety purposes (three listed under statute).
- If business allows the consumer to appeal the decision to use ADMT to a human reviewer with authority to overturn the decision.
- For admission, acceptance, or hiring decisions (subject to additional restrictions).
- For allocation/assignment of work and compensation (subject to additional restrictions).
- For work or educational profiling (subject to additional restrictions).
- These exceptions do not apply to behavioral advertising or training ADMT.

CPPA Rulemaking

ADMT: Right to Access Information

Section 7222:

- Right to access information about business's use of ADMT.
- Business must provide:
  - Specific purpose
  - Output of ADMT with respect to the consumer
  - How business used that output
  - How ADMT worked
- Business must respond no later than 45 days from receipt.
- Business must verify identity.
- If business denies consumer's verified request, business must inform consumer and explain reason unless prohibited by law.
- Additional notice requirements for significant decisions that were adverse to the consumer.

Increased AI Regulation:
How can companies prepare?

- Understand how the business is using AI
  - What key operational decisions is the company making by or materially depending upon non-human technology?
  - Map and assess current and future AI dependencies
- Develop policies that govern how AI will be used in the organization.
- Conduct risk assessments and consider implementing an AI risk management framework:
  - National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework
    - Published January 2023
    - Baseline control set to support compliance with existing and emerging AI regulations
    - Note: EU AI Act requires providers of high-risk AI systems to implement and document a risk management system

Increased AI Regulation:
How can companies prepare?

- Prepare to communicate
  - If company is integrating automated decision-making into business models, be prepared to respond to regulator and consumer inquiries regarding the same
- Prepare to ask questions
  - If relying upon third party software utilizing AI, ask vendors and service providers to provide documentation for underlying models that power the systems
- Prepare to document
  - Keep records to establish that the AI system does not lead to disparate outcomes
  - Apply existing information security programs, privacy programs, risk management programs, Foreign Corrupt Practices Act programs or other similar compliance programs to AI governance

Unlocking the Mysteries of Privacy (Part II)

Insights from Industry Titans

- Wednesday, May 22, 2024 – 5:00 – 7:00pm
  - La Jolla Square, 4225 Executive Square, La Jolla
- Industry Titans:
  - Hailun Ying, Head of Privacy, Legal, Roblox
  - Amy Lawrence, Chief Privacy Officer and Head of Legal, SuperAwesome
  - Paige Boshell, Global Privacy Counsel, Chevron

Procopio

Thank you!

Questions?

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
Elaine.Harwell@Procopio.com
619.906.5780

Yulian Kolarov
Associate
Yulian.Yolarov@Procopio.com
619.906.5683

Procopio