paragon
CORPORATE COUNSEL ON DEMAND

JLSheridan
Tech, IP & Privacy Law

Law firm articles re CPPA regulations:

- WilmerHale
  - CCPA publishes additional proposed regulations – including proposed revisions to CCPA regulations. 12/6/23
- Covington
  - CCPA releases draft risk assessment regulations. 12/7/23
- Ogletree
  - CPPA releases first draft regulations of AI and other ADMT. 11/29/23
- Morrison Foerster
  - Keeping Pace with Changes to the CPPA's Draft Regulations on Cybersecurity Audits, Risk Assessments and ADMT. 12/6/23
- WSGR
  - Draft California AI Regulations Become One Step Closer to Reality: An Analysis of Requirements on the Horizon. 12/18/23
- IAPP
  - CPPA publishes draft CPRA cybersecurity audit regulation revisions. 11/9/23
- IAPP
  - CPPA's draft automated decision-making rules unpacked. 11/27/23
- CPPA
  - A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for ADMT. 11/27/23
- IAPP

- A look at CPPA's draft cybersecurity regulation. 9/13/23

- Seyfarth Shaw
  - CPPA considers next set of CPRA regulations covering cybersecurity audits and risk assessments. 12/5/23
- Frankfurt Kurnit
  - Takeaways from CPPA Board Meeting December 8. 12/9/23
- Frankfurt Kurnit
  - Cybersecurity Audit Regulations under CCPA. 8/31/23

Other Resources:

1. Karen Levy, Data Driven (Truckers, Technology and the New Workplace Surveillance). Princeton University Press. 2023.
2. Nita A. Farahany, The Battle for Your Brain. St Martin's press. 2023.
3. State of California OAL process for new regulation.
4. Sacramento County Superior 6/30/23 decision delaying enforcement of the CCPA regulations.

WEBINAR

Part II: CPRA & the 2024 Alphabet Soup of US Privacy Regulations

Jennifer ("Jenny") Sheridan, Principal, JLSheridan Law

Megan Kelly, Director of Attorney Development, Paragon Legal

January 24, 2024

BACKGROUND

- Started as corporate attorney – wall street NYC law firm; Palo Alto corporate firm.
- In-house counsel for several Silicon Valley tech companies.
- Headed WW licensing team for BEA Systems (now part of Oracle).
- GC privately held and publicly traded software companies.
- Teaching law as adjunct at Santa Clara Law and USF Law, as well as visiting full-time at Drexel Law School.
- Founded JLSheridan Law boutique firm focused on tech transactions, privacy compliance, and IP counseling in 2014.
- Certified IAPP privacy professional with the CIPP/US and CIPP/E certifications.

TODAY'S TOPICS

Part I quick review: Privacy Policy updates (right to correct); opt-out update (sell or share); employee/contractor notices; review PI for sensitive information; and new thresholds of what is a business (buy, sell or share).

Part II rulemaking from CPPA – review the current state of these draft regulations as of 12/8/23:

I. ADMT rulemaking guidance;

II. Cybersecurity audit rulemaking guidance;

III. Risk Assessments for high risk processing (including targeted advertising) rulemaking guidance.

Looking forward to 2024-2025 and new US state laws coming into effect.

WHAT IS THE CPPA PROCESS FOR FINALIZING PART II REGS?

- Once CPPA board votes to finalize the regulations, then it proceeds to formal rulemaking – a 45 day process for public comment. There may be a public hearing following that period. If CPPA makes substantive further changes there could be an additional 15 day review period. Once CPPA votes that the regulations are final, then they can proceed to the OAL (office of administrative law) 30 working day process for final review before being issued.
- Once issued, there will be a 12 month delay before enforcement can begin.
- There are three sets of Part II regulations pending. It is estimated that they could be finalized between summer-fall 2024 and then enforceable mid-to-late 2025.
- Part I regs were finalized 3/30/23 and per Sacramento Superior Court enforcement begins 3/29/24 (one year grace period).

RISK ASSESSMENTS: HIGH LEVEL SUMMARY

- Any CCPA covered business must conduct a Risk Assessment ("RA") if it engages in high risk processing of personal information.
- An abridged summary of the Risk Assessment must be filed annually with the CPPA.
- Upon request by the Agency, the company will provide the full Risk Assessment to the Agency.

RISK ASSESSMENTS: WHAT IS CONSIDERED HIGH RISK PROCESSING?

- 'targeted advertising' or 'behavioral advertising' under CCPA; "selling or sharing PI;"
- Sensitive PI;
- ADMT (automated decision making technology);
- Consumers under age 16 that business has actual knowledge of;
- Processing PI using technology to 'monitor Employees, IC, job applicants, students.' Examples: keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial or speech recognition or detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application or social media monitors;
- Processing PI of consumers in publicly accessible places…..

[as of 12/8/23]

RISK ASSESSMENTS: CPPA DRAFT REG EXAMPLES

1. ADMT – ride sharing provider– employer/employee decisions re fares and bonuses for drivers;
2. sensitive PI – mobile dating – customer sensitive PI;
3. behavioral advertising – personal budget app where consumers are targeted based on income for loans;
4. video cameras monitoring employees behavior for a driving service;
5. grocery chain monitoring customers for profiling their shopping patterns in the store;
6. facial recognition technology to train AI based on extracted faceprints from consumers photographs.

RISK ASSESSMENTS: REQUIREMENTS

1. Summary of the processing;
2. Categories of PI processed;
3. Context of the processing;
4. Reasonable expectation regarding purpose and compatibility with context.
5. Operational elements of the processing: adherence to data minimization principles, protocols for data retention; number of consumers affected; technology to be used; names of all service providers or third parties whom the information is shared (or provide explanation for not sharing their names);
6. Purpose of the processing – specific description of the purpose and how processing achieves it;
7. Benefits resulting from the processing; with specificity, including discussion of benefits probability and scale;
8. Negative impacts on privacy from the processing: with specificity, encompassing sources of impact, as well as probability and extent of benefits. See Section 7152 (a) A-J pp 9-10.
9. Safeguards the business plans to implement to address the negative impacts, including an explanation of how they mitigate risks, and whether there are any residual risks; and
10. Evaluation of whether the safeguards' mitigation of negative impacts outweighs the benefits.

[as of 12/8/23]

CYBERSECURITY AUDITS: HIGH LEVEL SUMMARY

1. Certain businesses that meet the threshold must conduct annual (prescribed & independent) audits on their cybersecurity practices. Who is covered?
2. ALL data brokers (d)(1)C);
3. Other businesses who meet the two prong criteria:
4. $25m or greater revenue ((d)(1)(A) AND
5. Process certain types and volumes of PI as defined in (A), (B) and (C) – if the business processes any of them then it needs to conduct an audit.
6. PI of 250,000 consumers in preceding calendar year;
7. Sensitive PI of 50,000 consumers in preceding calendar year;
8. PI of 50,000 or more consumers that business had actual knowledge were under 16 years old in preceding calendar year.

[as of 12/8/23]

CYBERSECURITY AUDITS:WHO CONDUCTS IT?

- The draft regs prescribe that the audit must be 'independent' but they claim that it can be internal auditor IF meets definition and criteria of independent. See 7122 (1) and (2).
- Internal auditor 'cannot participate in activities that could compromise its independence.'
- Internal auditor must 'report director to Board' or equivalent.

CYBERSECURITY AUDITS: WHAT IS COVERED/REQUIRED & WHEN DOES IT START?

The draft reg specify 18 specific technical and organizational safeguards. (See Section 7123)

"Zero trust architecture" See Rick Borden article about difficulty of implementing this standard. He notes this makes the standard the toughest in country and maybe the world.

How far does SOC 2 or ISO certification get a company toward CPPA compliance?

The initial audit is DUE 24 months following the finalization of the regs, and then EVERY 12 months following.

ADMT (AUTOMATED DECISION MAKING TECHNOLOGY): SUMMARY

What does ADMT cover:

I. Definitions: In whole or in part; facilitate human decision making; any technology;

II. Decision that produces legal or similarly significant effects, e.g. employment, loan, insurance. Is there a financial or health effect for the consumer?

III. Includes "profiling" – evaluation, preferences, employee productivity.

What is required?

I. Risk Assessment (must be filed in abridged form)

II. Pre-use notice

III. Opt-out right

ADMT: WHAT ARE EXCEPTIONS TO THE OPT-OUT NOTICE?

I. Very narrow exceptions – fraud or security.

II. "Provide good or opportunity or perform service specifically requested by consumer" provided there is no reasonable alternative to business.

III. There is a rebuttable presumption that the business has a reasonable alternative if there is an alternative method of processing that has been used for similar good/service.

IV. Exception not available for behavioral advertising.

ADMT: WHAT IS REQUIRED IN THE RISK ASSESSMENT?

1. Why the business would like to use ADMT to achieve the purpose over manual methods;
2. The PI processed and used to train the ADMT;
3. The outputs and how the business will use them;
4. The steps the business has taken or plans to take to maintain the quality of PI processed by the ADMT, including PI used by the business to train the technology;
5. The logic of the ADMT, including any underlying assumptions;
6. How the business evaluates its use of the ADMT for validity, reliability, and fairness. This should include metrics used for assessment, why they are appropriate metrics, how any third party components meet these requirements (including internal assessments of the technology), whether and how alternative versions or ADMT technologies were evaluated for validity, reliability, and fairness, and reasons for their non-selection. Results of evaluations should also be included;
7. Why the business has not consulted external third parties and how protection has been accounted for without such consultation;
8. The degree and specifics of human involvement in the business's use of ADMT, including detailed requirements for the qualifications of the involved personnel and how they can influence the output and;
9. Any safeguards that the business plans to implements to address negative impacts on consumers' privacy specific to its use of automated decision-making technology or for data sets produced or derived from the automated decision-making technology.

[as of 12/8/23]

CPPA BOARD MEETING 12/8/23

Some of the hot topics at the board meeting included:

1. What is the scope of employee monitoring that should be included in the ADMT regulations? Should there be a definition of 'intrusive employee monitoring' so every instance of electronic monitoring like badge attendance is not included?

2. Are the list of negative harms in the Risk Assessment too broad and difficult to ascertain?

3. What is the economic impact of the cybersecurity audit thresholds?
   What is the likely scope of # CA businesses impacted?
   What is likely cost for a CA company to carry out the audit?

PRACTICAL USE CASES

1. Screening resumes from job applicants (ADMT)
   - The draft regs have a narrowly tailored possible exception to the ADMT opt-out for businesses using ADMT for recruiting "same day job opportunity." They had very time bound restrictions on this example. Will that be expanded more generally?
2. Employee productivity monitoring (ADMT)
3. Cybersecurity audit for small companies
4. Risk assessment for ADMT for small companies
5. Behavioral advertising for small companies

WHAT SHOULD COMPANIES BE REVIEWING FOR 2024? PART I REGS

Review the CCPA Part I regs for compliance including:

I. Privacy Policy updates (right to correct);
II. Opt-out update ("sell or share");
III. Employee/contractor notices;
IV. Review PI for sensitive information; and
V. New thresholds of what is a business ("buy, sell or share" replaced "buy, sell or receive").

WHAT SHOULD COMPANIES BE REVIEWING FOR 2024? PART II REGS

I. Risk Assessments
   - Evaluate if your company (client) is engaging in high-risk processing and a risk assessment is required. Likely you will have until later in 2025 to file initial abridged version of the RA. Start your process in 2024.

II. Cybersecurity Audits
   - Evaluate if your company (client) meets the thresholds (once finalized) for the cybersecurity requirement. Do you have SOC 2 and/or ISO? IF not need to get head start on this requirement in 2024.

III. ADMT
   - Evaluate if your company (client) use of ADMT qualifies for the pre-use notice and opt-out. Is there a valid exception? Have you documentation the reasons supporting the exception. This will be a big lift of companies so get started in 2024.

CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA) - REGULATIONS

- Part I – finalized 3/30/23 (Per 6/30/2023 court decision enforceable after 4/1/24)
- Part II – CPPA issued draft regs in 2023. Risk Assessments, Cybersecurity Audits and ADMT will be finalized some time in 2024. Then enforcement will begin in 2025.
- Sign up to receive messages from CA Privacy Protection Agency
- https://cppa.ca.gov/about_us/contact.html
- Recent CPPA regs: https://cppa.ca.gov/meetings/materials/20231208.html

THANK YOU!

Paragon Legal

Website: https://paragonlegal.com

Email: info@paragonlegal.com

Jennifer (Jenny) Lynn Sheridan, Esquire
Principal, JLSheridan Law

Email: jenny@jlsheridan.legal

Website: https://www.jlsheridan.legal

LinkedIn: https://www.linkedin.com/in/jenny-lynn-sheridan-cipp-us-aba6843

paragon
CORPORATE COUNSEL ON DEMAND

CPRA & THE ALPHABET SOUP OF U.S. PRIVACY REGULATIONS - PART II

JENNIFER SHERIDAN
PRINCIPAL
AT JLSHERIDAN LAW

MEGAN KELLY
ATTORNEY DEVELOPMENT
AT PARAGON LEGAL

ON-DEMAND WEBINAR REPLAY
NOW AVAILABLE