PREVIEW OF KEY ISSUES FOR FUTURE BOARD DISCUSSION

CPPA

AGENDA

- Introduction
- Cybersecurity Audits
- Risk Assessments
- Automated Decisionmaking Technology

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

INTRODUCTION: STATUS UPDATE

- **Prior Work:**
  - Fall 2021 and Spring 2022: Agency conducted preliminary rulemaking activities.
  - December 2022: Subcommittee recommended, and Board approved, engaging in additional preliminary rulemaking.
  - February 2023: Agency solicited preliminary written comments from the public.
  - May 2023: Staff updated Board that Subcommittee and staff would identify key issues for Board discussion.

- **Current Status:**
  - Subcommittee has been working with staff to review public comments and draft regulatory text.
  - Subcommittee and staff have identified key issues for further Board discussion, to inform the drafting of regulatory text.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

INTRODUCTION: OVERVIEW OF KEY ISSUES

Cybersecurity Audits: Assess and improve how businesses protect personal information.

- **What thresholds should trigger a cybersecurity audit?**
- What does a cybersecurity audit require a business to do?
- What ensures that a cybersecurity audit is thorough and independent?

Risk Assessments: Require businesses to assess and mitigate privacy risks.

- **What thresholds should trigger a risk assessment?**
- What does a risk assessment require a business to do?
- How specific should the risk assessment's requirements be?
- What is the end result of a risk assessment?

Automated Decisionmaking Technology ("ADMT") Requirements: Meaningfully inform consumers and give them control over their personal information by allowing them to opt out of ADMT.

- **What is ADMT?**
- **What thresholds should trigger consumers' access and opt-out rights?**
- What is "meaningful information" to a consumer?
- What does it mean to opt out of ADMT?

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

PART I: CYBERSECURITY AUDITS

CCPA DIRECTION TO AGENCY: CYBERSECURITY AUDITS

Topic	Rulemaking
Cybersecurity Audits §1798.185(a)(15)(A)	Issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to "[p]erform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities."

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

BACKGROUND ON CYBERSECURITY AUDITS

Examples of frameworks and resources considered:

- CA OAG and FTC data security orders and guidance
- CIS Critical Security Controls
- NIST Cybersecurity Framework
- NIST Special Publication 800-53
- NY DFS cybersecurity regulations
- GLBA Safeguards Rule
- FFIEC Council's Audit IT Examination Handbook
- CA Insurance Code

Most privacy and data protection laws do not require cybersecurity audits.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL CYBERSECURITY AUDIT THRESHOLDS

RECOMMENDED BY SUBCOMMITTEE FOR IMPLEMENTATION:

1. Businesses primarily or significantly engaged in sale/sharing of personal information (e.g., data brokers), OR

2. Larger businesses. For example, businesses that meet a particular revenue threshold, AND
   A. Annually process the personal information of a threshold number of consumers or households; or
   B. Annually process the sensitive personal information of a threshold number of consumers; or
   C. Annually process the personal information of a threshold number of consumers that the business has actual knowledge are less than 16 years of age.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

ENSURING THOROUGHNESS AND INDEPENDENCE

Potential Requirements to Ensure Thoroughness:

- Cybersecurity audit must articulate scope and criteria, and identify specific evidence examined
- Regulations list the components of a cybersecurity program that cybersecurity audits must assess and document
- Cybersecurity audit must assess and document all applicable components of the business's cybersecurity program

Potential Requirements to Ensure Independence:

- Business must provide independent auditor with all information relevant to the audit
- Independent auditor must determine the scope of the cybersecurity audit and criteria the cybersecurity audit will evaluate

Cybersecurity audit requirements will take into account cybersecurity audits, assessments, or evaluations a business has completed for other purposes.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

PART II:
RISK ASSESSMENTS

CCPA DIRECTION TO AGENCY: RISK ASSESSMENTS

Topic	Rulemaking
Risk Assessments §1798.185(a)(15)(B)	Issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to "[s]ubmit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL RISK ASSESSMENT THRESHOLDS

RECOMMENDED BY SUBCOMMITTEE FOR IMPLEMENTATION:

1. Selling or sharing personal information.
2. Processing sensitive personal information, with an exception for employers processing sensitive personal information for limited employment purposes.
3. Processing the personal information of consumers that the business has actual knowledge are less than 16 years of age.
4. Using Automated Decisionmaking Technology in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities.

RECOMMENDED BY SUBCOMMITTEE FOR DISCUSSION:

1. Processing the personal information of employees, independent contractors, job applicants, or students using a technology to monitor or surveil employees, independent contractors, job applicants, or students.
2. Processing the personal information of consumers in publicly accessible places through a technology that tracks consumers' behavior, location, movements, or actions.
3. Processing the personal information of consumers to train artificial intelligence.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL RISK ASSESSMENT REQUIREMENTS

- Summary and purpose of the processing.
- Necessity of the processing to achieve the purpose.
- Consumers' reasonable expectations regarding the purpose of processing, or the purpose's compatibility with the context in which the personal information was collected.
- Minimum personal information that is necessary to achieve the purpose.
- Nature and scope of processing (e.g., how long the business will retain the information).
- Benefits resulting from the processing (to the business, the consumer, other stakeholders, the public).
- Risks to consumers' privacy associated with the processing, and safeguards the business implements to address those risks.
- Assessment of whether the risks outweigh the benefits.
- Names and titles of individuals responsible for preparing and reviewing the risk assessment.
- Additional assessment requirements for Automated Decisionmaking Technology.

Risk assessment requirements will take into account compliance with other jurisdictions' requirements.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

OTHER JURISDICTIONS' REQUIREMENTS

Other State Laws (e.g., Colorado, Virginia)	General Data Protection Regulation
Key Requirements in Statutory Frameworks; Additional Requirements in Colorado's Regulations	Key Requirements in Article 35; Additional Guidance Documents from European Data Protection Board and Data Protection Authorities
Key Thresholds: • Selling personal data • Processing personal data for targeted advertising • Processing sensitive data • Processing personal data for certain profiling	Key Thresholds: • European Data Protection Board Guidance: Assessment required if processing meets 2 of 9 factors articulated in guidance • Data Protection Authorities: Assessment required/exempted if the processing activities are identified in specific lists

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

PART III: AUTOMATED DECISIONMAKING TECHNOLOGY ("ADMT")

CCPA DIRECTION TO AGENCY: ADMT

Topic	Rulemaking
Automated Decisionmaking Technology §§1798.185(a)(16), 1798.140(z)	Issue regulations "governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer."

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL DEFINITION OF ADMT

"Automated Decisionmaking Technology" ("ADMT") means any system, software, or process—including one derived from machine-learning, statistics, or other data processing or artificial intelligence techniques—that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking. ADMT includes profiling.

CCPA defines ***"profiling"*** *as any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.*
Civ. Code § 1798.140(z).

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL THRESHOLDS FOR ADMT ACCESS/OPT-OUT RIGHTS

RECOMMENDED BY SUBCOMMITTEE FOR IMPLEMENTATION:

1. Uses ADMT in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities.
2. Uses ADMT to monitor or surveil employees, independent contractors, job applicants, or students.
3. Uses ADMT to track the behavior, location, movements, or actions of consumers in publicly accessible places.

RECOMMENDED BY SUBCOMMITTEE FOR DISCUSSION:

1. Processes the personal information of consumers that the business has actual knowledge are less than 16 years of age in the business's use of ADMT.
2. Processes the personal information of consumers to train ADMT.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

APPENDIX FOR BOARD CONSIDERATION

The next four slides include more detailed language on the potential thresholds that could trigger cybersecurity audits, risk assessments, and ADMT access/opt-out rights.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL CYBERSECURITY AUDIT THRESHOLDS

A business shall conduct an annual cybersecurity audit if it:

1) Meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C) ["Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information"], or

2) Meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A) ["As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year. . . "],* and

   (A) Annually processes the personal information of [one million or more consumers or households];* or

   (B) Annually processes the sensitive personal information of [100,000 or more]* consumers; or

   (C) Annually processes the personal information of [100,000 or more]* consumers that the business has actual knowledge are less than 16 years of age.

* Placeholder numbers to guide Board discussion.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL RISK ASSESSMENT THRESHOLDS

A business shall conduct a risk assessment before the business engages in one or more of the following processing activities, which present significant risk to consumers' privacy:

1) Selling or sharing personal information.
2) Processing sensitive personal information, except for employers processing sensitive personal information for [employment authorization, payroll, and wage reporting].
3) Processing the personal information of consumers that the business has actual knowledge are less than 16 years of age.
4) Using Automated Decisionmaking Technology in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities.

[continued on next slide]

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL RISK ASSESSMENT THRESHOLDS

[continued from previous slide]

5) Processing the personal information of employees, independent contractors, job applicants, or students using a technology to monitor or surveil employees, independent contractors, job applicants, or students. Examples of this technology include keystroke logging or tracking, productivity or attention tracking, video or audio recording or live-streaming, facial or speech recognition or detection, automated emotion assessment, location tracking, speed tracking, or monitoring of web-browsing, usage of applications, and social media.
6) Processing the personal information of consumers in publicly accessible places through a technology that tracks consumers' behavior, location, movements, or actions. Examples of this technology include wi-fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, facial or speech recognition or detection, automated emotion assessment, geofencing, location tracking, or license-plate recognition.
7) Processing the personal information of consumers to train artificial intelligence, including but not limited to generative artificial intelligence, large language models, or facial or speech recognition or detection technology.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*

POTENTIAL ADMT ACCESS/OPT-OUT THRESHOLDS

A business shall provide consumers with the right to [access information about/opt-out of] the business's use of Automated Decisionmaking Technology if the business:

1) Uses Automated Decisionmaking Technology in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities;
2) Uses Automated Decisionmaking Technology to monitor or surveil employees, independent contractors, job applicants, or students;
3) Uses Automated Decisionmaking Technology to track the behavior, location, movements, or actions of consumers in publicly accessible places;
4) Processes the personal information of consumers that the business has actual knowledge are less than 16 years of age in the business's use of Automated Decisionmaking Technology; or
5) Processes the personal information of consumers to train Automated Decisionmaking Technology.

NOTE: *This presentation includes conceptual language for future Board discussion, not actual regulatory text. The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology.*