PRE-RULEMAKING STAKEHOLDER SESSIONS

MAY 2024

PLEASE NOTE:

The California Consumer Privacy Act (CCPA) directs the Agency to make rules about automated decisionmaking technology (ADMT), risk assessments, and cybersecurity audits. The Agency has drafted regulations on these topics but has not yet started the formal rulemaking process.

This presentation explains the draft regulations to help people understand and participate in the rulemaking process. These draft rules are not in effect and are subject to change.

This presentation does not implement, interpret, or make specific the law enforced or administered by the Agency and is not legal advice. Businesses should consult the statute, in-effect regulations, and/or an attorney before taking any action to ensure compliance with the law.

AGENDA

BACKGROUND ON CCPA AND CURRENT ACTIVITY

AUTOMATED DECISIONMAKING TECHNOLOGY (ADMT)

RISK ASSESSMENTS

CYBERSECURITY AUDITS

HOW TO PARTICIPATE IN FORMAL RULEMAKING

BACKGROUND ON CCPA AND CURRENT ACTIVITY

CALIFORNIA CONSUMER PRIVACY ACT: A BRIEF HISTORY

1

2018
CCPA passed and signed into law

2

January 2020
CCPA goes into effect

3

November 2020
CA voters approve Proposition 24 (CPRA), which amends and expands CCPA and establishes **CPPA (Agency)**

4

January 2023
CPRA amendments go into effect

Three Key Roles of the Agency

Rulemaking

Promoting Public Awareness

Auditing and Enforcement

Current Preliminary Rulemaking Activity

AUTOMATED DECISIONMAKING TECHNOLOGY

RISK ASSESSMENTS

CYBERSECURITY AUDITS

AUTOMATED DECISIONMAKING TECHNOLOGY (ADMT)

WHAT IS “AUTOMATED DECISIONMAKING TECHNOLOGY” (ADMT)?

ADMT

- Technology that processes **personal information**
- Uses **computation**
- Replaces or substantially facilitates **human decisionmaking**
- Includes **“profiling”**

Generally, does **NOT** include routinely-used technologies (e.g., spreadsheets)

WHAT IS “PROFILING”?

ADMT

- **Automated** processing of personal information
- To **evaluate** a person (e.g., predict their intelligence or performance at work)

WHO WOULD NEED TO COMPLY WITH ADMT REQUIREMENTS?

ADMT

- **“Business”** that must comply with CCPA
- That uses ADMT in any of **three ways:**

1. **SIGNIFICANT DECISION**
2. **EXTENSIVE PROFILING**
3. **TRAIN ADMT**

1 BUSINESS USES ADMT FOR A SIGNIFICANT DECISION CONCERNING A CONSUMER

ADMT

What is a significant decision?

- Decision that has **important consequences** for consumers

For example, results in providing or denying:

- Financial services
- Housing
- Educational or employment opportunities
- Healthcare services
- Essential goods or services (e.g., medicine)

2 BUSINESS USES ADMT FOR EXTENSIVE PROFILING

ADMT

What is extensive profiling?

- **Work or educational** profiling
- **Public** profiling
- Profiling for **behavioral advertising**

3 BUSINESS USES PERSONAL INFORMATION TO TRAIN ADMT THAT COULD BE USED FOR

ADMT

- **Significant** decisions
- To **identify people**
- **Physical or biological** identification or profiling
- Generating **deepfakes**

WHAT WOULD A BUSINESS HAVE TO DO IF IT USED ADMT IN ONE OF THOSE THREE WAYS?

ADMT

Provide:

- **Pre-Use** Notice
- **Opt-Out** of ADMT
- **Access** to information about ADMT

WHAT WOULD BE IN A PRE-USE NOTICE?

ADMT

WHY BUSINESS WANTS TO USE ADMT

HOW ADMT WOULD WORK

RIGHT TO **OPT-OUT** AND TO **ACCESS**

NO RETALIATION FOR EXERCISING RIGHTS

WHAT WOULD A BUSINESS HAVE TO DO IF A CONSUMER OPTED OUT OF ADMT?

ADMT

- Business would **NOT** process their personal information using that ADMT.

- There are **three exceptions** to providing the ability to opt-out.

NOTE: Consumers can always opt out from profiling for behavioral advertising and from the use of their personal information to train ADMT. Exceptions don't apply to those uses.

Exception #1: Security, Fraud Prevention, and Safety

ADMT

- Applies only in two circumstances:
  - Work/Educational Profiling
  - Public Profiling

- ADMT must be used SOLELY for security, fraud prevention, and safety.

Exception #2: Human Appeal

ADMT

- Applies only to significant decisions
- Consumers can appeal the significant decision to a qualified human decisionmaker.

Exception #3: Evaluation

ADMT

- Applies only in three circumstances:
  - Admission, acceptance, hiring decisions
  - Allocation or assignment of work decisions
  - Work/educational profiling

- Business must:
  - Evaluate ADMT, and
  - Implement accuracy and nondiscrimination safeguards

WHAT A BUSINESS WOULD HAVE TO PROVIDE IF A CONSUMER REQUESTED ACCESS:

ADMT

WHY THE BUSINESS USED ADMT

HOW ADMT WORKED FOR THE CONSUMER

OTHER CCPA RIGHTS AND **NON-RETALIATION**

Wouldn’t apply to business processing personal information to train ADMT.

Business that made an **adverse significant decision** using ADMT would have additional notice requirements.

“PHYSICAL OR BIOLOGICAL IDENTIFICATION OR PROFILING”

ADMT

WHAT ADDITIONAL REQUIREMENTS WOULD APPLY?

A business using this kind of ADMT for a significant decision or for extensive profiling would have to:

- Evaluate the ADMT; and
- Implement accuracy and nondiscrimination safeguards

RISK

RISK ASSESSMENTS

WHO WOULD NEED TO CONDUCT A RISK ASSESSMENT?

RISK

A business would need to conduct a risk assessment before:

- Selling or sharing personal information
- Collecting, using, disclosing, retaining, or otherwise processing sensitive personal information (e.g., health information)
- Using ADMT for a significant decision or extensive profiling
- Training ADMT or AI in certain ways

WHAT WOULD A RISK ASSESSMENT INCLUDE? (PART 1)

RISK

1. Why the business needs to do the activity
2. Types of personal information the business would collect, use, disclose, and retain
3. How the business would do the activity

WHAT WOULD A RISK ASSESSMENT INCLUDE? (PART 2)

RISK

4. *For uses of ADMT for significant decisions or extensive profiling*, additional information about how the ADMT works

5. Benefits and consequences to consumers, and any relevant protections put in place

6. Whether the business will initiate the activity, and details about who contributed to, reviewed, and approved the risk assessment

Note: A business would NOT be allowed to start an activity if the risks to consumers' privacy outweighed the benefits of the activity.

WHEN WOULD A BUSINESS CONDUCT OR UPDATE A RISK ASSESSMENT?

RISK

Conduct a risk assessment **before** starting the activity

Review **every three years**, update if needed

Immediately update risk assessment **whenever there is an important change**

WHAT WOULD A BUSINESS HAVE TO SUBMIT TO THE AGENCY, AND WHEN?

RISK

Must submit a certification of compliance and abridged risk assessments.

24 months to submit first certification and abridged risk assessments to Agency, and then annually after.

10 days to submit unabridged risk assessment to the Agency or Attorney General if requested.

NO REQUIREMENT TO DUPLICATE RISK ASSESSMENTS

RISK

If a business does a risk assessment for the same activity to comply with other laws, it would not have to redo it for CCPA. The business would have to add to it as needed.

ADMT

RISK

Illustrative Examples

Retailer wants to use facial-recognition technology in its stores solely to identify shoplifters

ADMT

RISK

What would the retailer be required to do under the proposed regulations?

- ✓ Conduct a risk assessment
- ✓ Evaluate the facial-recognition technology to ensure it works as intended for the retailer's use and does not discriminate
- ✓ Implement accuracy and nondiscrimination protections
- ✓ Provide a Pre-use Notice
- ✓ Provide consumers with the ability to access more information about the use of ADMT
- ✗ No opt-out of ADMT required if used solely for fraud prevention

A business's HR team wants to use a spreadsheet to input junior employees' performance evaluation scores from their managers and colleagues, and then calculate each employee's final score that the manager will use to determine which of them will be promoted.

ADMT

RISK

What would the business be required to do under the proposed regulations?

The CCPA's risk assessment and ADMT requirements would not apply. The business would not be required to comply with the risk assessment and ADMT requirements because the business is using the spreadsheet merely to organize human decisionmakers' evaluations.

CYBERSECURITY AUDITS

WHO WOULD NEED TO COMPLETE A CYBERSECURITY AUDIT?

CYBER

Business made 50% or more of its annual revenue the prior year from selling or sharing consumers' personal information;

OR

Business made over $28 million annual gross revenue last year; **AND**

Collects, uses, retains, discloses, or otherwise processes the personal information of 250,000 or more consumers or households;

OR

Collects, uses, retains, discloses, or otherwise processes the sensitive personal information (includes the personal information of consumers the business has actual knowledge are <16 years of age) of 50,000 or more consumers.

HOW WOULD A BUSINESS COMPLETE A CYBERSECURITY AUDIT?

CYBER

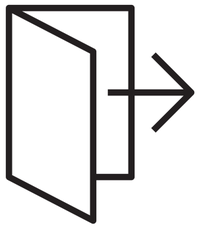
1. Select an auditor.
2. Provide all information the auditor asks for, and not hide important facts from them.
3. Present audit results to the most senior individuals in the business responsible for its cybersecurity program.
4. Submit certification of completion to the Agency.

WHO COULD THE AUDITOR BE?

CYBER

Must be qualified, unbiased, and independent

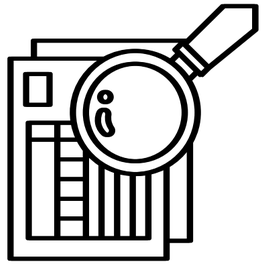
Must use professional auditing procedures and standards



Could work in or outside the business

WHAT WOULD THE AUDITOR HAVE TO DO?

CYBER



Determine which systems need to be audited and how to assess them.

Independently review documents, conduct tests, and interview people.

Certify completion of independent and unbiased audit.

WHAT WOULD A CYBERSECURITY AUDIT INCLUDE? (PART 1)

CYBER

1. Description of systems being audited.

2. Information auditor used to make decisions and why it supported audit findings.

3. Assessment of how business protects personal information through its cybersecurity program.

For example, assessment of:

- Authentication
- Access controls
- Inventory of personal information
- Cybersecurity training
- Encryption
- Incident-response

WHAT WOULD A CYBERSECURITY AUDIT INCLUDE? (PART 2)

CYBER

4. Description of how business follows its own policies and procedures.

5. Description of gaps and weaknesses of cybersecurity program and how business plans to address them.

6. Description or sample copy of data-breach notifications that were sent to consumers or agencies, as well as related information and fixes.

7. Dates of when cybersecurity program was reviewed and presented to most senior individuals in the business responsible for its cybersecurity program.

8. Certifications (from auditor and business) that the audit was independent.

WHEN WOULD A BUSINESS HAVE TO COMPLETE ITS CYBERSECURITY AUDIT?

CYBER

24 months to complete **first** audit and submit certification of completion

After first audit/certification, complete audit and submit certification **annually**

CYBER

NO REQUIREMENT TO DUPLICATE AUDITS

A business that gets a cybersecurity audit or assessment for another purpose, or has a cybersecurity certification, would not have to redo the same cybersecurity audit for CCPA. The business would have to add to it as needed.

JOIN

HOW TO PARTICIPATE IN FORMAL RULEMAKING

KEY STEPS IN THE RULEMAKING PROCESS

JOIN

1

Step 1:
Preliminary Rulemaking

2

Step 2:
Formal Rulemaking

3

Step 3:
Review by Office of Administrative Law

TIPS FOR PARTICIPATING IN THE AGENCY'S RULEMAKING PROCESS

JOIN

SUBSCRIBE TO THE AGENCY'S EMAIL LISTS

Receive notifications about rulemaking activities and upcoming board meetings.

https://cppa.ca.gov/webapplications/apps/subscribe/

ATTEND BOARD MEETINGS AND PUBLIC HEARINGS

Agendas and recordings of past meetings/hearings can be found on our website.

https://cppa.ca.gov/meetings/

SUBMIT PUBLIC COMMENTS

Submit electronically, in writing, or orally during formal rulemaking.

Tips:
https://cppa.ca.gov/regulations/pdf/comments_tips.pdf

PUBLIC COMMENT

APPENDIX

Summary Chart of Proposed Requirements for ADMT Use Cases

Use of ADMT for:	Risk Assessment	Pre-use Notice	Access	Opt-out	Exceptions to Opt-out
The following significant decisions: • Admission, acceptance, or hiring • Allocation/assignment of work and compensation	YES	YES	YES	YES	• Human appeal exception; or • Evaluation exception
All other significant decisions	YES	YES	YES	YES	• Human appeal exception
Work or educational profiling	YES	YES	YES	YES	• Safety, security, & fraud prevention exception; or • Evaluation exception
Public profiling	YES	YES	YES	YES	• Safety, security, and fraud prevention exception
Profiling for behavioral advertising	YES	YES	YES	YES	
Training uses of ADMT	YES	YES	—	YES	

CALIFORNIA RULEMAKING PROCESS