CPPA Proposed Rulemaking Package Part 2—Automated Decision-Making Technology

February 14, 2025

In Part 1 of this series, we discussed the annual cybersecurity audit requirements in the proposed rulemaking package (the "Draft Regulations") of the California Privacy Protection Agency (the "CPPA"). In this Part 2, we discuss the Draft Regulations' provisions on Automated Decision-Making Technology ("ADMT"). Most notably, the Draft Regulations' definition of ADMT is more expansive than other regulatory definitions in that it includes technology that substantially facilitates human decisionmaking. Although certain technologies are presumptively out of scope, the Draft Regulations' expansive definition will likely capture tools that other regulatory frameworks do not. We discuss what constitutes ADMT, which uses are covered, what is required when using ADMT, and some practical considerations below.

What Is Automated Decision-Making Technology?

The Draft Regulations define ADMT as "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." The Draft Regulations also provide that ADMT "includes profiling."

Other key defined terms in the Draft Regulations include:

- **Technology**, which means "software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence."

- **Profiling**, which means "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 intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements." This closely follows the GDPR's definition of profiling in Article 4(4).

- **Artificial intelligence**, which means "a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments." This definition follows the OECD's definition of artificial intelligence ("AI").

The Draft Regulations' definition of ADMT distinguishes a list of technologies, including firewalls, calculators, or spreadsheets, which are presumptively not considered ADMT, provided they do not execute a decision, replace human decisionmaking, or substantially facilitate decision making.

"Substantially Facilitate Human Decisionmaking"

The Draft Regulations' inclusion of technology that substantially facilitates human decisionmaking in its definition of ADMT is more expansive than the majority of current regulations. While Australia and Canada also include the concept of facilitating human decisionmaking in their respective definitions of ADMT, the majority of regulations, including those in Brazil, the European Union, and the United Kingdom, either cover solely automatic decisions, or explicitly exclude decisions made with human involvement from their definitions of ADMT.

The Draft Regulations provide the following examples that demonstrate how even a common-use technology could be swept into coverage by the ADMT requirements:

What Uses Are Covered?

Article 11 of the Draft Regulations applies an activity-based analysis for when a covered business's use of ADMT involving Californian residents ("consumers") is subject to the ADMT requirements. Covered businesses are subject to the CCPA when they use ADMT for the following uses:

- **Significant decisions** concerning a consumer. These include decisions relating to the grant, provision, or denial, of financial/lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services, such as groceries, medicine, hygiene products, or fuel. It is likely that an AI tool that is used to decide whether to issue consumer loans would qualify as ADMT because the tool is used to substantially facilitate human decisionmaking for a significant decision concerning a consumer. On the other hand, an AI tool that is used to produce an investment summary is arguably not ADMT because the

investment summary itself is not a decision. The Draft Regulations note several federal law preemptions, including for entities and data subject to HIPAA, entities and data subject to the FCRA, and data subject to the GLBA.

- **Extensive profiling** of a consumer, *i.e.*, (1) through systemic observation of a consumer while they are acting in their capacity as an applicant to a job/educational program, as a student, employee, or as an independent contractor ("work or educational profiling"); (2) through observation of a publicly accessible place ("public profiling"); or (3) profiling for behavioral advertising. Behavioral advertising means targeted advertising "to a consumer based on the consumer's personal information obtained from the consumer's activity," including cross-context behavioral advertising, but does not include nonpersonalized advertising, "provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party." The CPPA's statement of reasons for the Draft Regulations ("Statement of Reasons") identifies "significant risk of discrimination when using ADMT for profiling for behavioral advertising." To demonstrate what would constitute a "significant risk of discrimination," the Statement of Reasons referenced advertisements for high-paying jobs that were disproportionately served to men, and real estate advertisers using social media to target housing advertisements based on protected classes, such as race, gender, and age.

- **Training**, when the ultimate product can be used for a significant decision concerning a consumer, to establish individual identity, for physical or biological identification/profiling, or for the generation of a deepfake. The Draft Regulations define physical/biological identification/profiling as "identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (*e.g.*, to identify or infer emotion)" and defines deepfakes as "manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer's knowledge and permission." In its Statement of Reasons, the CPPA connects training uses of ADMT to consumer privacy concerns, "including data leakage that can reidentify consumers whose personal information was used to train the model, a lack of transparency and consumer control over the use of their personal information for training, discrimination based on protected classes, and reputational and psychological harm."

ADMT Use Requirements

The Draft Regulations propose sweeping obligations for businesses that use ADMT as described above, including providing a pre-use notice and, for some uses, the rights to (1) opt out of that use, and (2) access the logic of the ADMT. While these obligations are subject to certain exceptions that either narrow or exempt the business from compliance altogether, navigating the complexities of the Draft Regulation will likely pose practical challenges for businesses.

Pre-use Notice to Consumers

A business using ADMT must inform its consumers via a pre-use notice that it is using ADMT and that consumers have the rights to opt-out of ADMT and to access ADMT. Pre-use notices broadly resemble current CCPA privacy notices in that they must be presented prominently and conspicuously before the consumer's personal information is processed using ADMT and must align with the manner in which the business primarily interacts with the consumer (*i.e.*, online, in-person, etc.). Pre-use notices must include (1) the purpose of using ADMT, (2) information about the right to opt-out (or about applicable exceptions to providing this right), (3) information about the right to access ADMT details, (4) a statement that retaliation for exercising rights under the CCPA is prohibited, and (5) additional details on how the ADMT works.

For training uses of ADMT, the notice must identify for which specific uses the ADMT is capable of being used, and the categories of the consumer's personal information that the business proposes to process for these training uses. Businesses must provide a notice per each ADMT use but may consolidate their Pre-Use Notices in enumerated cases: (1) the use of a single ADMT for multiple purposes, (2) the use of multiple ADMT for a single purpose, (3) the use of multiple ADMT for multiple purposes, or (4) the systematic use of a single ADMT.

The Right to Opt Out and Primary Exemptions

For some uses, businesses must also provide consumers with the ability to opt out of ADMT and at least two or more designated methods to do so. The Draft Regulations provide detailed requirements for how for businesses must implement the right to opt-out, such as not allowing businesses to make account creation mandatory for a consumer submitting a request to opt-out, or to require a verified consumer to request, rather than simply exercise their right to opt-out.

The Draft Regulations provide several examples where businesses are not required to provide consumers with the ability to opt-out of the use of ADMT for significant decisions concerning a consumer and for public profiling. In these circumstances, a pre-

use notice is still required and additional rights outlined below still apply. These circumstances include:

- **Security, fraud prevention, and safety exception**. Businesses do not need to provide the ability to opt-out when the use of ADMT is necessary to achieve and used solely for security, fraud prevention or safety purposes, such as preventing, detecting and investigating security incidents that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted personal information.

- **Human appeal exception**. For significant decisions concerning a consumer, businesses may choose to implement a human appeals process instead of providing the ability to opt out. This process requires the business to designate a human reviewer qualified to understand the significant decision being appealed and with the authority to overturn an ADMT-driven decision to handle consumer appeals. Businesses relying on a human appeals process must clearly describe to the consumer how to submit an appeal and enable the consumer to provide information for the human reviewer to consider as part of the appeal.

- **Necessity + Accuracy and Nondiscrimination Safeguards**. Businesses using ADMT for (i) admissions, acceptance and hiring decisions, (ii) allocation/assignment of work and compensation decisions, or (iii) work and educational profiling are exempt from providing the right to opt out so long as (1) the ADMT used is necessary to achieve, and is used solely for, that purpose, and (2) the business has conducted an evaluation of the ADMT to ensure it works as intended for these purposes, and does not discriminate based upon protected classes, which may involve reviewing a third-party providers evaluation ("accuracy and nondiscrimination safeguards").

Additional Consumer Rights

The Draft Regulations outline additional consumer rights to promote transparency and fairness in the use of ADMT. These are:

- **Right to Access.** Businesses using ADMT must provide, at the consumer's request, information about the business's use of ADMT with respect to the consumer. These disclosures include the specific purpose of the ADMT, the outputs of the ADMT, and how the business used the ADMT's outputs.

- **Anti-Retaliation Measures.** The CCPA prohibits retaliation against consumers exercising their CCPA rights, including for ADMT. Businesses must inform consumers of this safeguard and provide instructions as to how the consumer may exercise their CCPA rights.

- **Discrimination Safeguards.** Finally, businesses using ADMT for physical/biological identification or profiling must ensure that their ADMT is working as intended for the businesses' proposed use and does not discriminate based on protected classes.

Practical Takeaways

ADMT Mapping

As the Draft Regulations go through the rulemaking process, companies may benefit from a preliminary ADMT mapping survey of their current and proposed uses to determine which uses may qualify as ADMT and therefore be subject to a potential heavy compliance burden. In particular, companies will want to assess whether their use cases would substantially facilitate significant decisions, including decisions on financial/lending services, insurance underwriting, health care services, and employment opportunities.

Leveraging Existing Processes for Consumer Protection

While the specific ADMT-related requirements in the proposed Draft Regulations would implement new requirements, many of the embedded consumer protection expectations such as informed notice, opt-out, and request to access are not. Covered businesses should consider reviewing their existing governance process and capabilities for handling other types of consumer requests under the CCPA (*e.g.*, right to know, delete, or correct), and assess whether any resource augmentation might be advisable to facilitate compliance with the ADMT-related consumer request requirements.

What's Next?

The CPPA states that the Draft Regulations are informed by, and harmonize with, federal, state, and international laws, regulations, frameworks, and guidance on the impact of ADMT to consumer privacy, and the CCPA itself has been influential in shaping privacy laws beyond California. If adopted, these Draft Regulations will likely continue to influence regulatory expectations at the interface between automated decisionmaking (including artificial intelligence) and privacy compliance. As such, even companies that do not currently conduct extensive business in California may wish to note what the Draft Regulations require and consider whether any of the practices outlined in the Draft Regulations would be advisable to include in their AI governance and regulatory compliance roadmap.

The formal public comment has been further extended to February 19, 2025. Any subsequent substantive changes to the Draft Regulations would trigger an additional 15-day comment period.

To subscribe to the Data Blog, please click here.

The Debevoise Data Portal is an online suite of tools that help our clients quickly assess their federal, state, and international breach notification and substantive cybersecurity obligations. Please contact us at dataportal@debevoise.com for more information.

* * *

Please do not hesitate to contact us with any questions.

Avi Gesser
Partner, New York
+ 1 212 909 6577
agesser@debevoise.com

Matt Kelly
Counsel, New York
+ 1 212 909 6990
makelly@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+ 1 212 909 6291
jnskrzypczyk@debevoise.com

HJ Brehmer
Associate, San Francisco
+ 1 415 738 5703
hjbrehmer@debevoise.com

Ned Terrace
Associate, New York
+ 1 212 909 7435
jkterrace@debevoise.com

Mengyi Xu
Associate, San Francisco
+ 1 415 738 5725
mxu@debevoise.com

Amer Mneimneh
Law Clerk, New York
+1 212 909 6023
amneimneh@debevoise.com