Volume 4, No. 2 | March–April 2021

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL The Journal of Robotics, Artificial Intelligence & Law

Volume 4, No. 2 | March–April 2021

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Everything Is Not *Terminator*

AI Under the California Privacy Rights Act

John Frank Weaver*

On November 3, 2020, the United States not only elected a new president, its largest state also voted to adopt the most sweeping privacy law in the nation, the California Privacy Rights Act ("CPRA"). The new law, which expands the privacy rights and protections created by the California Consumer Privacy Act ("CCPA"), incorporates many concepts from the European Union General Data Protection Regulation ("GDPR"), including its treatment of "automated-decision making." That term is not defined in the CPRA or in the GDPR, but is generally understood as "making a decision solely by automated means without any human involvement."[1] In other words, the CPRA will permit California to regulate decisions made by certain artificial intelligence ("AI") functions and applications if the new state agency created by the CPRA, the California Privacy Protection Agency (the "CPPA"), decides to pursue that strategy, which it should.

CCPA's (Non-)Treatment of AI

The CCPA was conspicuously silent on automated decision-making and AI, although some provisions had AI implications. For example, the CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[2] The modifying "reasonably" is not in similar definitions of personal information and personal data in Canada's Personal Information Protection and Electronic Documents Act or the GDPR, respectively. With the inclusion of "reasonably," de-identified data could unwittingly become re-identified personal data if an AI application is able to connect it with a particular consumer or household with reasonable contextual data. That has serious implications for the companies

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

and organizations that rely on AI tools to enrich their data. Other AI-related issues include the problems the right to erasure potentially creates for training data sets and the problems the right to be informed potentially creates for engineers using data sets to train new AI applications.[3]

GDPR's Treatment of Automated Decision-Making and Profiling (That Is, AI)

The CPRA, in contrast, speaks directly to AI through its treatment of automated decision-making, borrowing from the GDPR. As a principle, the GDPR holds that individuals have the right not to be subject to a decision that is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her.[4] Where automated decision-making or automated processing occurs, it "should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."[5] Automated decision-making includes profiling, which is "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[6] The idea is that if an organization is making important decisions about an individual without any human involvement (such as the refusal of a credit application or any hiring decisions) the individual has the right to know about that and to object, forcing the organization to include a human being in the final decision.[7] Best practices for complying with these requirements include:

- Conducting a data protection impact assessment to consider and address the risks before starting any automated decision-making or profiling;
- Giving notice to customers and users about automated decision-making and profiling that produces legal effects concerning the individuals or similarly significantly affects them, including the sources of the personal data relied on,

meaningful information about the logic involved in the automated decision-making or profiling (in other words, how does it use personal data), and the potential consequences of the processing to the individuals; and
- Providing instructions on how to opt out of automated decision-making and how to contest the decision.[8]

CPRA's Treatment of Automated Decision-Making and Profiling (That Is, AI)

The CPRA does not include the same obligatory language contained in the GDPR governing automated decision-making and profiling. Unlike the GDPR, it does not: affirmatively grant individuals the right to object to AI in automated decision-making and profiling; provide examples of those activities; obligate organizations to give notice of significant automated decision-making and profiling; require human intervention upon request; or grant individuals the opportunity to express their point of view or to object. Rather, it establishes the CPPA and instructs it to issue "regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."[9] That is an ambiguous assignment, leaving open the possibility that the CPPA's regulations impose few requirements on automated decision-making, but also the possibility that the final regulations create obligations similar to the GDPR's.

However, even though the issues related to automated decision-making raised in the CPRA mirror those addressed in the GDPR, the language used in the Act suggests that the final regulations could govern AI more broadly than the GDPR. Compare the CPRA terms against the analogous language in the GDPR—the CPPA shall issue regulations:

- *"governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling . . ."*

  This mirrors the GDPR's requirement that the controller inform data subjects of "the existence of automated decision-making, including profiling" that produces legal effects concerning data subjects or similarly significantly affects them, as well as the right of individuals under the GDPR not to be subject to such processing.[10]

- *"requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, . . ."*

  The GDPR contains also identical language, requiring that the controller provide data subjects "meaningful information about the logic involved" in automated decision-making, including profiling, that produces legal effects concerning data subjects or similarly significantly affects them.[11]

- *"as well as a description of the likely outcome of the process with respect to the consumer."*

  The GDPR addresses this issue by requiring notice to data subjects of "the envisaged consequences" on the data subject of automated decision-making, including profiling, that produces legal effects concerning data subjects or similarly significantly affects them.[12]

Stricter AI Regulation Under the CPRA?

The key difference between the CPRA and the GDPR is potentially in the modifying language that the GDPR attaches to all its meaningful requirements for automated decision-making and profiling: for the AI functions to be subject to these GDPR requirements, it must produce legal effects concerning individuals or similarly effects them. The CPRA does not modify automated decision-making with that phrase, giving the CPPA much more latitude to regulate AI. For example, targeted advertising based on profiling is unlikely to have a significant impact on individuals, making it more difficult (though by no means impossible) for supervisory authorities in the European Union to impose the AI-related obligations of the GDPR on companies that accumulate personal data to feed to AI applications for various advertising initiatives.[13] The CPPA will not face that obstacle. That agency will have wide latitude to impose rules on any company relying on automated decision-making and profiling to release meaningful information about what how the company's AI uses personal information, what the outcomes are for individuals subjected to the AI's decision-making, and other access rights.

The question is whether the CPPA will want to take up that fight. An unknown but growing number of companies track mobile phone usage and online behavior and rely on AI applications to analyze personal data before feeding media, advertising, etc., to people based on the analysis. A lot of it is happening in a black box—we do not know how many companies do it or what their AI does with our information. The CPRA has the potential to be a major step forward in AI regulation if the CPPA requires disclosures and individual privacy rights from companies that largely want to keep their AI hidden.

Notes

[*] John Frank Weaver is a member of McLane Middleton's privacy and data security practice group, where he maintains the Artificial Intelligence Attorneys blog (https://artificial-intelligence-attorneys.com/). He is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law* and writes its "Everything Is Not *Terminator*" column. Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse technology practice that focuses on information security, data privacy, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

[1] Rights related to automated decision making including profiling, United Kingdom Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ ("ICO Summary").

[2] Cal. Civ. Code § 1798.140(o).

[3] For a more thorough discussion of AI issues raised tangentially by the CCPA, see John Frank Weaver, "Everything is Not *Terminator*: AI Issues Raised by the California Consumer Privacy Act," *The Journal of Robotics, Artificial Intelligence & Law* (Vol. 3, No. 1; January-February 2020).

[4] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L119) 1, Rec. 71, Art. 22(1) ("GDPR"). There are several exceptions to this right, including if the automated decision-making or processing is necessary for entering into, or performance of, a contract between the data subject and a data controller. *Id.*, at Art. 22(2).

[5] *Id.*, at Rec. 71.

[6] *Id.*, at Art. 4(4).

[7] *See id.*, at Rec. 71, Art. 22.

[8] *See id.*, at Arts. 13(2)(f) & 22(3); ICO Summary, *supra* note 1.

[9] California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, §§21, 24 (the "CPRA"). Similar to the GDPR, the CPRA 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." *Id.*, at §14. Please note that the CPRA does not immediately grant the CPPA the regulatory authority described in this article. Rather, the California Attorney General's office has that authority until mid-2021, at which point the AG assigns that authority to the CPPA. For simplicity, this article only refers to the CPPA.

[10] GDPR, *supra* note 4, at Arts. 13(2)(f) & 22(1).

[11] *Id.*, at Art. 13(2)(f).

[12] *Id.*

[13] Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679, Article 29 Data Protection Working Party, 17/EN WP 251rev.01, p. 21. Criteria that could cause such advertising to have a significant effect on an individual, depending on the circumstances, include: the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices, and services; the expectations and wishes of the individuals concerned; the way the advertisement is delivered; and using knowledge of the vulnerabilities of the data subjects targeted.