Volume 3, No. 1 | January–February 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law

Volume 3, No. 1 | January–February 2020

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 2020 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 call:

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 8am–8pm 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 Issues Raised by the California Consumer Privacy Act

John Frank Weaver*

Following efforts by a California real estate developer to place a new privacy law, the Consumer Right to Privacy Act of 2018, on the November 2018 California ballot, California legislators passed a substitute bill, the California Consumer Privacy Act of 2018 (the "CCPA"), which was signed into law by then-Governor Jerry Brown on June 28, 2018. By passing the CCPA as quickly as it did in the spring of 2018, the legislature avoided having the alternative bill appear on the November ballot that year.[1]

The CCPA, effective January 1, 2020, is easily the toughest privacy law in the United States, granting privacy rights to California residents akin to rights granted to EU residents by the General Data Protection Regulation ("GDPR"), including the right to require a business to delete their data,[2] the right to be informed of the data a business holds about them,[3] the right to require businesses to stop selling their data,[4] and the right to data portability.[5]

Due to the state's large population and the statutory civil damages available to California residents,[6] many of my clients are attempting to implement the CCPA's requirements across their operations nationwide, not just in California. The administrative burden is easier, and those organizations are less likely to accidentally violate the statute in California. I expect this trend to continue and for many of the rights granted to California residents by statute to be available to Americans nationwide due to a combination of practices implemented by private companies and copycat state statutes.

Although the CCPA is essentially silent on the topic of artificial intelligence ("AI"),[7] the statute cites the Cambridge Analytica scandal as an inciting incident.[8] And even though the legislation notes that because of Cambridge Analytica, "our desire for privacy controls and transparency in data practices is heightened," it does not

Robotics, Artificial Intelligence & Law / January–February 2020, Vol. 3, No. 1, pp. 73–79.

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

mention AI by name.[9] However, Cambridge Analytica is as much an AI scandal as a personal information scandal. The seriousness of what occurred is due in part to the invasion of privacy, but also to what Cambridge Analytica's AI was able to do with personal information from Facebook.

As was reported after the company's activities were revealed, the AI was able to mislead, manipulate, and even control individuals. With knowledge of 150 likes, the company's AI could predict someone's personality better than their spouse.[10] "With 300, it understood you better than yourself."[11] Jonathan Rust, the director of the Psychometrics Centre at the University of Cambridge, has expressed concern regarding the capabilities of the company's AI, which he claims "can predict and potentially control human behavior. It's what the scientologists try to do but much more powerful. It's how you brainwash someone. It's incredibly dangerous."[12] With this as part of the CCPA's backdrop, it is impossible for the statute to have no impact on AI usage, even if AI is not mentioned specifically in its text.

Below, I discuss three sections of the CCPA that will affect how companies use and consider AI:

(1) Section 1798.140(o)—Definition of personal information;
(2) Section 1798.105—Right to erasure; and
(3) Section 1798.100(b)—Right to be informed.

Definition of Personal Information

The CCPA as originally passed in 2018 defined personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[13] An amendment passed in September 2019 changed this definition to "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" (emphasis added).[14] The intent appears to be to limit the data that is subject to the CCPA. Although the original definition is similar to the definitions of "personal information" in Canada's Personal Information Protection and Electronic Documents Act ("information about an identifiable person")[15] and "personal data" in the GDPR ("any information relating to an identified or identifiable natural person"),[16] there seems to have been a concern that the California definition was too broad, meaning that businesses[17] in California would have to apply the privacy rights granted in the CCPA to too much data.

However, the amended definition might make it more difficult in some ways for entities to comply with the CCPA, at least from a conceptual perspective. With fairly basic application program interfaces ("APIs"), *i.e.*, sets of routines, protocols, and tools for building software applications, to retrieve personal information from various web resources, it would not take a particularly sophisticated AI application to use personal information from APIs to associate nonpersonal or deidentified information with an actual person. In a famous example, Latanya Sweeney, Director of Harvard University's Data Privacy Lab, was able to use the LexisNexis newspaper archive and public records to re-identify much of the anonymized data in a Washington state database of hospitalizations that she purchased.[18] Professor Sweeney did not rely on APIs or AI, but those tools make the re-identification of personal information much easier. If it is not difficult for an AI program to associate nonpersonal information with a person, what's the line between information that is not "reasonably" associated with a person and information that is?

Before the amendment to the CCPA, California businesses were largely required to treat any associated with a real person as personal information under the statute. With the amended definition, that requirement supposedly does not exist, but organizations that use AI to enrich their data may want to ignore the amendment and use the original definition of personal information for purposes of CCPA compliance in order to avoid inadvertently violating it when their AI makes nonpersonal information personal information.

Right to Erasure

Under the CCPA, a consumer, defined as a natural person who is a California resident,[19] has the right to request that a business delete any personal information about the consumer that the business has collected from the consumer.[20] A business that receives such a request must delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records as well.[21]

Businesses that use AI to enrich consumers' personal information or that rely on consumers' personal data to train their AI should keep in mind that one or more consumers may request that their personal information be deleted. How will a business's AI function when one or more sets of personal information are removed? When a business builds AI applications and infrastructure, the programmers need to keep this consideration in mind. Similarly, businesses need to make sure that their AI applications are technologically capable of complying with this requirement. Can a business track and delete all personal information in datasets that are entered into its AI and that are among the output of its AI?

Many businesses will deidentify the information they retain to make complying with the CCPA easier (among other reasons). Deidentified information is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.[22] However, businesses must ensure they can satisfy the CCPA's further requirements for deidentification of personal data:

(1) Implementing technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
(2) Implementing business processes that specifically prohibit reidentification of the information;
(3) Implementing business processes to prevent inadvertent release of deidentified information; and
(4) Making no attempt to reidentify the information.[23]

Using APIs to enrich data and AI to analyze data increases the odds that reidentification of information will occur, so developing employee processes and technological safeguards that prevent that from occurring is very important.

Right to Be Informed

A business that collects a consumer's personal information must, at or before the point of collection, inform the consumer of the categories of personal information to be collected and the purposes for which the business will use the personal information. A business may not collect additional categories of personal information or use the consumer's personal information for additional purposes without providing the consumer with notice.[24]

Frequently, the engineers that I work with talk about the "cool to creepy" scale. They are referring to the spectrum of uses for AI and data, which range from cool (like Alexa suggesting a great new song based on your listening habits) to creepy (like Facebook showing you posts for products related to your use of other applications). When they develop new AI applications, engineers often give the new applications a rating on this scale.

The cool to creepy scale hints at how AI uses expand: engineers see the data collected, see what current AI programs can do with it, and explore other uses. The CCPA does not limit the new AI applications that engineers can develop, but it does require proper notice to the consumers whose personal information is used in the development process. Businesses should keep that in mind when drafting their privacy policies and AI policies. They should also remember the CCPA's requirements for deidentifying information if they pursue that option when using data with AI.

Conclusion

It is important that businesses that operate in California and have customers in California carefully review the CCPA's effects on their AI applications. In addition to the bad press that noncompliance can generate, there can be significant monetary fines and damages as well.

First, the California Attorney General may assess fines for noncompliance; a business may be fined up to $7,500 for each intentional violation of any CCPA requirements.[25]

Second, consumers may bring private actions in the event their nonencrypted and nonredacted personal information is subject to "unauthorized access and exfiltration, theft, or disclosure" as a result of a business's failure "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[26] And unlike most other states, California through the CCPA no longer requires proof that the affected individuals have suffered damages. Consumers may recover the greater of $100 to $750 per incident (at the court's determination) or actual damages.[27] This essentially reduces the standard of proof in private data breach claims to one of negligence.

Businesses should expect to see more litigation in California concerning data breaches, and they can minimize their exposure by ensuring that their AI practices are consistent with the requirements of the CCPA.

Notes

* John Frank Weaver, a member of McLane Middleton's privacy and data security practice group, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law* and writes its "Everything Is Not *Terminator*." 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] John Stephens, "California Consumer Protection Act," *ABA Business and Corporation Litigation Committee Newsletter* (July 2, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

[2] *Compare* CAL. CIV. CODE §§ 1798.105, 1798.130(a), & 1798.145(g)(3) *with* 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. 59 & 65-66, Art. 12 & 17 ("GDPR").

[3] *Compare* CAL. CIV. CODE §§ 1798.100(b), 1798.130(a), & 1798.135 *with* GDPR, Rec. 58-63, Art. 5, 12-14.

[4] *Compare* CAL. CIV. CODE §§ 1798.120 & 1798.135 *with* GDPR Rec. 70, Art. 12 & 21.

[5] *Compare* CAL. CIV. CODE §§ 1798.100, 1798.110, 1798.130, 1798.145(g)(3) *with* GDPR Rec. 68, Art. 12 & 20.

[6] CAL. CIV. CODE § 1798.150. This is discussed in more detail below.

[7] The notable exception is the definition of processing: "any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by *automated processing*" (emphasis added). CAL. CIV. CODE § 1798.140(q).

[8] Assem. Bill 345, 2018-2019, Reg. Sess., §2(g).

[9] *Id.*

[10] Carole Cadwalladr, "Robert Mercer: the big data billionaire waging war on mainstream media," *The Guardian*, February 26, 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

[11] *Id.*

[12] *Id.*

[13] Assem. Bill 345, 2018-2019, Reg. Sess., §3.

[14] Assem. Bill 874, 2018-2019, Reg. Sess., §1.

[15] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, Part 1.

[16] GDPR, Art. 4(1).

[17] The CCPA largely limits its requirements to businesses, as defined in Section 1798.140(c) as:

> "A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
>
> (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
>
> (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information."

[18] Latanya Sweeney, "Matching Known Patients to Health Records in Washington State Data," arXiv:1307.1307 [cs.CY] (July 5, 2013), https://arxiv.org/pdf/1307.1370.

[19] CAL. CIV. CODE § 1798.140(g).

[20] CAL. CIV. CODE § 1798.105(a).

[21] CAL. CIV. CODE § 1798.105(c). The wording in CAL. CIV. CODE § 1798.105(a) suggests that the consumer has the right to request that a business delete only the personal information "which the business has collected," meaning that after a consumer's request for deletion, the business could retain any personal information about that consumer that the business obtained from a source *other* than the consumer. However, that appears to be a drafting error, as CAL. CIV. CODE § 1798.105(c) clearly states that the business has the obligation to delete "the consumer's personal information from its records," without the limiting language in 105(a).

[22] CAL. CIV. CODE § 1798.140(h).

[23] *Id.*

[24] CAL. CIV. CODE § 1798.100(b).

[25] CAL. CIV. CODE § 1798.155(a) & (b).

[26] CAL. CIV. CODE § 1798.150(a).

[27] *Id.*