Volume 2, No. 2 | March–April 2019

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 2, No. 2 | March–April 2019

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. 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)

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 inquires 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*

Public-Facing Artificial Intelligence Policies—Part II

John Frank Weaver*

In my last column,[1] I explored the first two components that I recommend clients address in their public-facing AI policies: disclosure of AI that interacts with customers and disclosure of the decisions AI makes. In light of the California bot bill (the "California Bot Bill")[2] that became law last fall, I advised businesses that rely on AI-based customer service to include a statement in their AI policies disclosing the existence of any chat bots and explaining the requirements of the new law. In light of the EU's General Data Protection Regulation (the "GDPR"),[3] I advised that organizations conduct a two-part self-analysis of their business practices: (1) determine if they rely on AI for profiling or automated decision making, as the GDPR defines it;[4] and (2) isolate those decisions and classify them as either (a) decisions that produce legal effects concerning data subjects or similarly significantly affects data subjects, or (b) decisions that produce no legal effects concerning data subjects or do not similarly significantly affects data subjects. I then recommended that your AI policy be drafted to reflect how your answers comply with Article 22(1) of the GDPR, which states that each "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[5]

In this second part, I review the final two components that should be standard considerations when preparing an AI policy: disclosure of the types of data relied on and disclosure of how AI reaches decisions.

Types of Data Relied On

This topic bridges the last part of the previous column—disclosure of the decisions your organization relies on AI to make—and the last part of this column—disclosure of how AI in your

Robotics, Artificial Intelligence & Law / March–April 2019, Vol. 2, No. 2, pp. 141–146.

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

organization reaches decisions. Those two sections of an AI policy are governed by AI-specific sections of the GDPR. In contrast, Article 15 of the GDPR grants data subjects the right to obtain from controllers the categories of data being processed, a requirement that applies to all processing of data, not just automated decision making. Similarly, American laws like the California Online Privacy Protect Act of 2003 ("CalOPPA")[6] and California Consumer Privacy Act of 2018 (the "CCPA")[7] also address disclosure of the types of data organizations have collected.

The central issue in including this information in your AI policy is transparency. Most companies that collect personal data or personally identifiable information on the internet maintain a privacy policy that discloses the categories of that data or information collected, consistent with the GDPR[8] and CalOPPA.[9] Why restate this information in an AI policy or make a new disclosure in an AI policy?

The biggest reason is to stay ahead of the trend of required and preferred disclosures. The GDPR and CCPA are the most current and widely applicable privacy laws that your organization is likely to encounter in the near future. They not only require the disclosure of the categories of data your organization relies on, but upon the request of an individual, they also require your organization to release a copy of the personal data and personal information from that person that your organization has processed[10] and to disclose the purposes for which you are using that person's information.[11] Canada's Personal Information Protection and Electronic Documents Act contains similar requirements.[12] The legal trend is toward requiring greater disclosure of the data you rely on; more transparency, not less.

This is true for AI as well, both in terms of public policy recommendations and advice from industry groups, even if the black letter law does not reflect this yet. For example, the National Science and Technology Council's 2016 report, *Preparing for the Future of Artificial Intelligence,* called for the establishment of open data sets to train AI and for the private sector AI to rely on.[13] Other entities emphasize that not only should data be more available, but the algorithms the AI relies on when analyzing the data should also be reviewable in some way. The Institute of Electrical and Electronic Engineers has warned about the dangers of the "black box," the locked up algorithm that produces decisions in response to data it receives, but without public scrutiny.[14] Similarly, although there is

no federal law addressing disclosure of AI data sets or algorithms, the Office of Technology Research and Investigation in the Federal Trade Commission relies on the Commission's power to prevent deceptive trade practices to investigate algorithmic transparency issues that are potentially deceptive and unfair to consumers.[15]

As the trend continues to move in the direction of disclosure of and transparency around the data you use and how you use it, your organization's AI practices will come under scrutiny. I recommend that clients get ahead of public opinion and legal requirements by making considered disclosures in their AI policies about the data their AI uses.

First, the disclosure should address Article 22(4) of the GDPR, which specifically prohibits companies from using special categories of personal data in automated decision-making unless the data subject consents. Special categories include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation.[16] Your AI policy should either affirm that your organization's AI does not use special categories of personal data or explain which special categories your organization's AI uses, how it uses them, and how it obtains consent from data subjects.[17]

Second, disclosing the categories of data your AI processes is an opportunity to demonstrate to your consumers that you are aware of privacy law and foresighted enough to recognize the trend toward more disclosure in AI. In doing so, you should explain your understanding of the current requirements in the GDPR, CalOPPA, and the CCPA and how those laws inform how your AI handles personal data. A properly drafted AI policy can provide useful information to your consumers without disclosing sensitive information or other trade secrets. In short, in addition to demonstrating compliance with the GPDR, your AI policy is an opportunity to market yourself as a leader in AI thought and policy without disclosing any of the intellectual property that has made your organization a leader in AI thought and policy.

How AI Reaches Its Decisions

The GDPR requires that when you collect information from a data subject, you are obligated to disclose the existence of

automated decision making, including profiling, and "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[18] The right to "meaningful information" about an AI's decision-making is frequently referred to as the "right to an explanation."[19] Jack Dorsey, the CEO of Twitter, focused on this idea briefly when he testified to Congress in September 2018 and describes this as "explainability," a functionality that can explain the decision-making criteria an AI uses.[20] For example, if a bank's machine learning application denies you a loan, the application should be able to explain why. Dorsey admits that explainability, as he describes it, is a functionality that AI cannot perform right now,[21] but the right to an explanation as the GDPR envisions it is not necessarily the same function.

In truth, it is not clear what kind of "meaningful information" about an AI's decision would satisfy the GDPR. For example, does Amazon's Alexa have to explain why it picked a song for you when asked? Do the "Why am I seeing this ad?" boxes that Google, Facebook, and Amazon use qualify? Based on the wording of Article 13(2)(f), the meaningful information could take another form altogether, as that article suggests that the information could be conveyed at the time the company collects the personal data. This contrasts with the idea that the AI needs to explain its decisions in real time in response to a question.

You can explain your interpretation of Article 13(2)(f) in your AI policy. In doing so, you should state that you are aware of the requirement for meaningful information about the logic involved in automated decision-making, disclose the categories of data that your AI relies on and general information about how it relies on them to make decisions, and note that other than general explanations like this, decision-specific, real-time explanations are not possible now. This provides information that your consumers will appreciate and demonstrates compliance with the GDPR.

Conclusion

To summarize this column and my last, when drafting a public-facing AI policy, you should consider whether it needs to do the following:

1. Include a statement disclosing the existence of any chat bots that interact with customers and explain the requirements of the California Bot Bill;
2. Explain how your AI complies with Article 22 of the GDPR and does not subject any consumer to decisions based solely on automated processing, including profiling, which produce legal effects concerning customers or similarly significantly affects them;
3. Affirm that your AI does not rely on special categories of data and disclose the categories of data your AI relies on; and
4. Explain how your AI relies on data categories to reach its decisions, consistent with Article 13(2)(f) of the GDPR.

Depending on your industry and business practices, some of these considerations may not be relevant and/or you should address other considerations. You should consult with your CTO and AI or technology counsel to determine how best to draft your AI policy. Although the legal requirements governing AI usage are fairly minimal now, the trend toward more disclosure is clear, and you can put your organization in a stronger position going forward by preparing a policy now.

Notes

* John Frank Weaver, an associate at McLane Middleton and a member of the firm's privacy and data security practice group, is the "Everything Is Not *Terminator*" columnist for *The Journal of Robotics, Artificial Intelligence & Law.* Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse practice that focuses on land use, real estate, telecommunications, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

1. John Frank Weaver, "Everything Is Not *Terminator:* Public-Facing Artificial Intelligence Policies—Part I," *The Journal of Artificial Intelligence & Law* (Vol. 2, No. 1; January-February 2019).

2. Cal. Bus. & Prof. Code §§17940-17943.

3. 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 (the "GDPR").

4. *See id.* at Art. 4(4), which defines profiling as "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."

5. *Id.* at Art. 22(1).

6. Cal. Bus. & Prof. Code § 22575(b)(1) (A company's privacy policy shall "Identify the categories of personally identifiable information that the operator collects through the Web site or online service").

7. Cal. Civ. Code § 1798.100(a) ("A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories . . . of personal information the business has collected.").

8. GDPR, Art. 14(1)(d).

9. Cal. Bus. & Prof. Code § 22575(b)(1).

10. DPR, Art. 20(1); Cal. Civ. Code § 1798.110(a)(5).

11. GDPR, Art. 15(1)(a); Cal. Civ. Code § 1798.110(a)(3).

12. Personal Information Protection and Electronic Documents Act, SC 2000, c 5, Schedule 1, §§ 4.2, 4.9.

13. National Science and Technology Council, "Preparing for the Future of Artificial Intelligence," *Executive Office of the President* (October 2016), 14, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

14. *Ethically Aligned Design,* v.2, IEEE, 158-19, *available at* http:// standards.ieee.org/develop/indconn/ec/ead_v2.pdf.

15. *See* 15 U.S.C. § 45; Office of Technology Research and Investigation Homepage, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation.

16. GDPR, Art. 9(1)

17. Article 22(4) also permits companies to rely on special categories of personal data on the basis of substantial public interest and on the basis of relevant EU or member state law, "which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject." Currently, this exception is so incredibly small that any companies hoping to take advantage of it are likely better off seeking consent.

18. GDPR, Art. 13(2)(f).

19. *See* John Frank Weaver, "Why Artificial Intelligence Owes You an Explanation," *Slate* (May 8, 2017), https://slate.com/technology/2017/05/why-artificial-intelligences-should-have-to-explain-their-actions.html.

20. Jack Dorsey, interview with Jay Rosen, *recode* (September 14, 2018), https://www.recode.net/2018/9/14/17857486/twitter-jack-dorsey-nyu-jay-rosen-bias-neutrality-presence-politics-recode-media-podcast.

21. *Id.*