Volume 2, No. 1 | January–February 2019

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 2, No. 1 | January–February 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 I

John Frank Weaver*

For some time now—in response to the California Online Privacy Protection Act,[1] Canada's Personal Information Protection and Electronic Documents Act,[2] and similar statutes and regulations from other jurisdictions—any company with any web presence to speak of has provided a public-facing privacy policy on its website, explaining what it does with each user's information, how it complies with the relevant laws, what rights users have to access their information, etc. These policies have become much more prominent in 2018, as the EU's General Data Protection Regulation (the "GDPR") became effective and thousands of companies notified their contact lists that their privacy policies had been updated.[3]

As I have noted frequently in this space, artificial intelligence ("AI") is not nearly as well regulated as data privacy and is, in fact, hardly regulated at all. However, there are some requirements, expectations, and norms that are emerging from a combination of expert opinion (like the Institute of Electrical and Electronic Engineers ("IEEE")),[4] pending legislation,[5] and the limited black-letter law.[6] In response, some attorneys have begun advising clients about AI policies. These are public-facing policies that state certain information about how companies use AI in their business operations.

In light of the expansion of AI use and the expected increase in legislation and regulations governing AI, this column is the first of two that will look at issues to consider when preparing an AI policy. In this piece, I look at how to disclose that AI performs customer service and how to disclose the decisions AI makes.

Will Customers Interact with the AI?

Organizations that use AI and other autonomous technologies solely for data processing and analysis, warehouse management, and other backhouse functions have different policy needs than

Robotics, Artificial Intelligence & Law / January–February 2019, Vol. 2, No. 1, pp. 59–65.

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

companies that have begun relying on chatbots and other forms of autonomous communication technologies. This is particularly true in the wake of the 2016 presidential election, during which there was widespread use of autonomous twitterbots disguised as real human beings to interact with potential voters and disseminate information.[7]

Concern regarding this activity has been widespread, leading to bills in the California legislature and United States Senate that would prohibit autonomous bots from promoting political candidates without self-identifying as bots.[8] The idea of requiring this notice from bots has animated groups like IEEE and the Electronic Frontier Foundation ("EFF"). In response to an early version of the California bill that prohibited unidentified bots more broadly, the EFF wrote a public letter worrying that the bill would "restrict and chill protected speech" and that it would "not withstand First Amendment scrutiny."[9] In contrast, the IEEE has suggested that a "government-approved labeling system like the skull and crossbones found on household cleaning supplies that contain poisonous compounds could be used for this purpose to improve the changes that users are aware when they are interacting with" AI or autonomous bots.[10] The California and U.S. bills represent an attempt to walk a tight rope between the positions staked out by the EFF and the IEEE: bots have to give notice to the real humans they interact with when they are speaking about or advocating for concerns, like commercial and political decisions, where human beings are particularly vulnerable, but not when bots interact with people in most situations.[11]

Between the direction legislation is going and the conflicted perception public opinion has about AI-based customer service,[12] it is best to get out in front of this issue by including in AI policies a statement addressing customer service chat bots or other autonomous communications technology, as relevant. Indeed, the California bot bill became law this past fall, requiring businesses to either refrain from using autonomous online chatbots to incentivize commercial activity or to disclose the bots' existence to users. A company's AI policy, therefore, should make that disclosure (in addition to posting the disclosure on the bot account itself) and explain the requirement under California law. Additionally, the policy can reflect the company's actual use of AI and its concerns about its customers' experience. This advice is intended to comply

with existing and expected regulations and demonstrate transparency to their customers concerning a topic that can be somewhat unpopular and controversial.

What Decisions Are Made By the AI?

The GDPR's language addressing "automated processing"[13] suggests that the decisions made by AI should be stated clearly for customers and other members of the public, or at least as clearly as the organization is comfortable with due to trade secrets, patents, business practices, etc. The GDPR 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," although there are carve outs for certain situations.[14] If the automated processing relies on special categories of personal data—which include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, and data concerning a natural person's sex life or sexual orientation—the controller is obligated to use "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."[15] Given that non-compliance with these requirements carries potential "administrative fines up to 20,000,000 EUR" or "up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher,"[16] companies are incentivized to affirmatively show that they are using AI and autonomous technology in a way that complies with this requirement. An AI policy can be an appropriate platform to do that.

The first step is to determine whether or not you rely on AI for profiling or automated decision making. The GDPR 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."[17]

In its draft "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (the "Guidelines"), the Article 29 Working Party provided further

guidance, noting that profiling (1) is an automated form of processing, (2) carried out on personal data, with (3) the objective of the profiling being to evaluate personal aspects about a natural person.[18] That document also defines automated decision-making as "the ability to make decisions by technological means without human involvement."[19] If your organization does not have AI-performing functions that match these descriptions, you do not fall under this provision of the GDPR, and you may want to affirmatively assert that in your AI policy.

If AI is profiling or performing automated decision-making as defined and envisioned by the GDPR, your next step is to isolate what decisions are made by the AI and then to 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. The Guidelines address this, as well. With regard to "legal effects":

> A legal effect suggests a processing activity that has an impact on someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract. For example, automated decisions that mean someone is:
>
> - entitled to or denied a particular social benefit granted by law, such as child or housing benefit;
> - refused entry at the border;
> - subjected to increased security measures or surveillance by the competent authorities; or
> - automatically disconnected from their mobile phone service for breach of contract because they forgot to pay their bill before going on holiday.[20]

Similarly, the Guidelines analyze the phrase "similarly significantly affects" data subjects, noting that "even where no legal (statutory or contractual) rights or obligations are specifically affected, the data subjects could still be impacted sufficiently to require the protections under this provision" and that "the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned" to qualify.[21] Examples of

such decisions include automatic refusal of an online credit application or e-recruiting practices without any human intervention.[22]

It should be noted that the Guidelines also provide guidance as to whether or not relying on AI to make decisions about targeted online advertising can produce legal effects concerning data subjects or similarly significantly affect data subjects. Briefly, the Article 29 Working Party stated that targeted advertising can have a significant impact on individuals, depending on the characteristics of the incident, including:

- the intrusiveness of the profiling process;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; and
- the particular vulnerabilities of the data subjects targeted.[23]

When reviewing your practices, consider the nature of the decisions your AI makes. Do they produce a legal effect? Do they make decisions that could affect your customers as significantly as a legal decision? How intrusive is your advertising designed to be? How intrusive is it actually?

Based on the answers to these questions and others, you may decide to address in the AI policy the decisions your AI makes as part of demonstrating compliance with the GDPR and educating your customers and users about the AI you use. Your policy could include, as relevant, language explaining and emphasizing the limited nature of the decisions made by the AI or that there is always a "man in the loop" to interpret and act on the AI's advice and analysis.

Conclusion

Please note that I have not provided recommended language for AI policies in this column. Each policy should be written to fit the needs of the organization based on input from the chief technology officer, the IT department, marketing, and in house or outside counsel. Full disclosure of an organization's use of AI is not necessary for an AI policy to be beneficial, in the same way that revealing all of an organization's internal security and privacy protocols is not necessary for a privacy policy to be beneficial. Customer interaction with AI and decisions made by AI are just two of the issues to think about when considering an AI policy.

In the next issue of *The Journal of Robotics, Artificial Intelligence & Law*, I will discuss two other topics that are appropriate to address in an AI policy in response to legislation and expert opinions: the data relied on by AI and disclosing how AI reaches any particular decision.

Notes

* John Frank Weaver, an associate at McLane Middleton and a member of the firm's privacy and data security practice groups, 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. Cal. Bus. & Prof. Code §§22575-22579.

2. S.C. 2000, s. 5.

3. I would cite to a news article or journal article, but as this experience was arguably the most universal web experience of the year, no citation seems necessary.

4. *See Ethically Aligned Design,* v.2, IEEE, *available at* http://standards.ieee.org/develop/indconn/ec/ead_v2.pdf ("Ethically Aligned Design"). Full disclosure: I assisted in preparing a portion of that document.

5. *See* S. 3127, 115th Congress ("U.S. Bot Bill"); Cal. SB 1001, §1 ("CA Bot Bill").

6. **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, Arts. 22(1) (data subjects "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") & 13(2)(f) (data subjects have the right for "meaningful information about the logic involved" in automated decision-making which produces legal effects concerning the data subject) ("GDPR").

7. Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

8. U.S. Bot Bill, *supra* note 5, at §§4(b) (requiring the Federal Trade Commission to promulgate regulations that would require "a social media provider to establish and implement policies and procedures to require" any user of its social media service "to publically disclose the use" of any bot) & 5 (prohibiting political committees, corporations, and labor organizers from

using bots intended to impersonate or replicate human activity online to advocate for the election or defeat of a candidate or to send electioneering communications); CA Bot Bill, *supra* note 5, at §1 ("It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot.").

9. Jamie Williams, "EFF Letter Opposing California Bot Disclosure Bill, SB 1001—First Amendment Concern," *Electronic Frontier Foundation,* May 21, 2018, https://www.eff.org/document/eff-letter-opposing-california-bot-disclosure-bill-sb-1001-first-amendment-concerns.

10. Ethically Aligned Design, *supra* note 4, at 159.

11. The California Bot Bill attempts this tight rope act more directly, as it applies only to bots designed to incentivize commercial transactions or influence a vote, whereas part of the U.S. Bot Bill applies more broadly to bots on social media platforms.

12. Dom Price, "Yes, Chat Bots Are Incredibly Efficient. But Your Customers Hate Them," *Inc.,* March 27, 2018, https://www.inc.com/dom-price/yes-chat-bots-are-incredibly-efficient-but-your-customers-hate-them.html (noting that 64 percent of American consumers "feel brands are so myopic about automation … they've 'lost touch' with the human element of creating a great customer experience").

13. GDPR, *supra* note 6, at Art. 22(1).

14. *Id.* at Art. 22(1). That language does not apply if the decision "is necessary for entering into, or performance of, a contract between the data subject and a data controller … is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or … is based on the data subject's explicit consent." Art. 22(2).

15. *Id.* at Art. 22(4).

16. *Id.* at Art. 83(5)(b).

17. *Id.* at Art. 4(4).

18. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* October 3, 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=47742, 6 ("Guidelines").

19. *Id.* at 7.

20. *Id.* at 10.

21. *Id.* at 10.

22. GDPR, *supra* note 6, para. 71.

23. Guidelines, *supra* note 18, at 11.