EDITOR IN CHIEF **JEFFREY VOAS**
IEEE Fellow; j.voas@ieee.org

Algorithms as Defendants?

Jeffrey Voas, IEEE Fellow
Keith Miller, University of Missouri–St. Louis

This EIC message ponders what can be legally done now (and in the future) to algorithms when they misbehave and create problems for the humans they were designed to serve.

Seventy-plus years ago, the word algorithm was probably only known to mathematicians, programmers, and engineers. Today it is a common word, and often associated with black boxes, whose inner workings are mysterious and may even be malicious. We ponder what can be legally done now (and in the future) to algorithms when they misbehave and create problems for the humans they were designed to serve. And perhaps you have similar questions.

As we know, when people are harmed, sooner or later someone may get sued (pretty likely in the United States). But lately, the "someone" might turn out to be silicon-based instead of a human or a corporation. In this short message, we will take a quick look at whether you *can* sue an algorithm (for now the answer is no), and we will also comment on whether or not you *should* be able to sue an algorithm (if that were to become possible in the future).

At this writing, people are going to court because they think they (or someone they care about) has been treated badly because of an algorithm. For example, a group of web content providers are suing generative artificial intelligence (AI) companies because their algorithms harvest the providers' content without compensation.[1] Patients are suing their health insurer because they contend an algorithm unfairly denied the patients' claims.[2] In two criminal cases, judges have ordered its developers to reveal the inner workings of software used to supposedly identify minute DNA samples.[3] (Readers wanting more information about that last example can read about it in an earlier issue of *Computer*.[4])

Many more examples exist, but you may have noticed something: People are upset with the algorithms in question, but it is not the algorithms themselves that are being sued or are being ordered about by judges. Corporations

DISCLAIMER

The authors are completely responsible for the content in this message. The opinions expressed here are their own.

Digital Object Identifier 10.1109/MC.2024.3355536
Date of current version: 26 June 2024

users, identifies challenges, and provides recommendations for improving the adoption of NDIDs.

In summary, I hope you enjoy this issue, and I thank the authors for their patience in waiting for their accepted articles to be published. *Computer* has seen an uptick in the number of submissions, and we have a backlog of accepted articles. Feel free to write to me about this issue or any others at j.voas@ieee.org.

—*Jeffrey Voas*, *Editor in Chief*

APPENDIX: RELATED ARTICLES

A1. J. Chandrasekaran et al., "Leveraging combinatorial coverage in the machine learning product lifecycle," *Computer*, vol. 57, no. 7, pp. 16–26, Jul. 2024, doi: 10.1109/MC.2024.3366142.

A2. W. Yao et al., "Considerations for decision makers and developers toward the adoption of decentralized key management systems technology in emerging applications," *Computer*, vol. 57, no. 7, pp. 27–38, Jul. 2024, doi: 10.1109/MC.2023.3339390.

A3. J. B. Abdo, S. Zeadally, and J. Demerjian, "Compartmentalization-by-design: Usability-aware web privacy," *Computer*, vol. 57, no. 7, pp. 39–52, Jul. 2024, doi: 10.1109/MC.2023.3341050.

A4. A. Karati and S. K. Das, "Effective data sharing in an edge–cloud model: Security challenges and solutions," *Computer*, vol. 57, no. 7, pp. 53–65, Jul. 2024, doi: 10.1109/MC.2024.3367590.

A5. M. de Castro et al., "The role of field-programmable gate arrays in the acceleration of modern high-performance computing workloads," *Computer*, vol. 57, no. 7, pp. 66–76, Jul. 2024, doi: 10.1109/MC.2024.3378380.

A6. Z. Zheng et al., "Metamorphic fault tolerance: Addressing the oracle problem of reliability assurance for contemporary software systems," *Computer*, vol. 57, no. 7, pp. 77–86, Jul. 2024, doi: 10.1109/MC.2024.3390759.

A7. M. Hilowle et al., "Leveraging human-centric cybersecurity to improve usage of national digital identity systems in Australia," *Computer*, vol. 57, no. 7, pp. 87–98, Jul. 2024, doi: 10.1109/MC.2024.3395523.

and organizations that deploy and use the algorithms are being sued, not the algorithms themselves. This seems straightforward at first glance; an algorithm is an abstract notion, perhaps even just a thought. It is only when an algorithm is implemented in a particular computing machine that it becomes a concrete entity.

Further, an algorithm does not have deep pockets, so it is likely to be useless as a target in a lawsuit. And an algorithm does not fear incarceration or a fine, so criminal proceedings against it are unlikely to be effective. However, corporations often *do* have deep pockets, and the humans who develop and deploy systems that implement algorithms *do* have something to fear from criminal proceedings. Thus, it is not surprising that companies and humans are bearing the brunt of legal actions that target the consequences of algorithms.

But is that fair? Especially as algorithms becoming increasingly sophisticated, and particularly when they are designed to *learn* (and thus change their behavior after deployment), is it fair to demand accountability from developers long after deployment, or should we shift our focus to the artifact that has been deployed? An increasingly important example of this question is found in medical ethics. Duffourc writes about the potential legal liability of an "autonomous AI physician."[5] If not with the artifact, where does the responsibility for the effects of AI algorithms properly reside?

As a legal question, determining responsibility for the effects of AI algorithms is not a settled question, although there is quite a bit of discussion about it. (We cannot go into details about legal wranglings in this short message. For more information, see recent articles that describe proposed legislation in the European Union[6] and in the United States.[7])

In addition to the legal questions, the issue of responsibility for the effects of AI algorithms is also a hot topic among ethics scholars. Writers interested in computer ethics have been working on this issue for years. For example, 30 years ago, a paper suggested the possibility that sophisticated machines could someday be recognized as "electronic personae" who would have both accountability and some well-defined rights.[8] Other writers insist that artificial intelligence artifacts should never be regarded as persons[9] and should not be thought of as targets of accountability. Instead, the humans who design, deploy, and use the artifacts should be held accountable for the consequences of the AI artifacts' use.[10,11,12]

Most scholars and most AI practitioners think that AI artifacts are

currently not sophisticated enough to be considered as truly autonomous entities. Philosophers think that you need autonomy if you are to be held accountable for your actions. However, when thinking ahead to machines that are more advanced than today's machines, future machines that can learn after deployment, people are less sure that AI artifacts will not become fully autonomous "moral agents." Some oppose that idea, but others embrace it.[13]

The issue of accountability for algorithms, especially for AI algorithms, is likely to remain a hot topic for the foreseeable future. Computing professionals are on the front line of designing and developing these algorithms. It seems prudent that they pay attention to the legal and ethical ramifications of that work, even though some people are dubious about the progress being made so far. (We are not convinced that Munn is correct when he writes that "AI ethics are useless."[14])

And remember that IEEE publications are a good source of information about attempts to better understand this question. For example, see Huang et al.[15] and De Franco at al.[16] and the February 2024 *Computer* special issue on ethics. We invite you to stay tuned to *Computer* for additional thoughts about this question.

REFERENCES

1. B. Lutkevich. "AI lawsuits explained: Who's getting sued? Authors, artists and others are filing lawsuits against generative AI companies for using their data in bulk to train AI systems without permission." TechTarget. Accessed: Jan. 6, 2024. [Online]. Available: https://www.techtarget.com/WhatIs/feature/AI-lawsuits-explained-Whos-getting-sued,
2. C. Ross and B. Herman. "UnitedHealth faces class action lawsuit over algorithmic care denials in Medicare Advantage plans." STAT. Accessed: Jan. 8, 2024. [Online]. Available: https://www.statnews.com/2023/11/14/unitedhealth-class-action-lawsuit-algorithm-medicare-advantage/
3. L. Kirchner, "Powerful DNA Software Used in Hundreds of Criminal Cases Faces New Scrutiny: After decades of secrecy, two judges have ruled defendants can investigate whether TrueAllele's probabilistic genotyping algorithm works as advertised," *The Markup*. Mar. 9, 2021. Accessed: Jan. 6, 2024. [Online]. Available: https://themarkup.org/news/2021/03/09/powerful-dna-software-used-in-hundreds-of-criminal-cases-faces-new-scrutiny
4. J. M. Voas and K. W. Miller, "Confronting your digital accuser," *Computer*, vol. 54, no. 4, pp. 11–13, Apr. 2021, doi: 10.1109/MC.2020.3038516.
5. M. N. Duffourc, "Malpractice by the autonomous AI physician," *Univ. Illinois J. Law Technol. Policy*, vol. 2023, no. 1, p. 1–49, 2023. [Online]. Available: https://illinoisjltp.com/journal-archive/volume/null/article/malpractice-by-the-autonomous-ai-physician
6. P. Hacker, "The European AI liability directives – Critique of a half-hearted approach and lessons for the future," *Comput. Law Secur. Rev.*, vol. 51, Nov. 2023, Art. no. 105871, doi: 10.1016/j.clsr.2023.105871.
7. D. S. Schiff, "Looking through a policy window with tinted glasses: Setting the agenda for US AI policy," *Rev. Policy Res.*, vol. 40, no. 5, pp. 729–756, 2023, doi: 10.1111/ropr.12535.
8. C. J. Orwant, "EPER ethics," in *Proc. Conf. Ethics Comput. Age*, Nov. 1994, pp. 105–108, doi: 10.1145/199544.199595.
9. J. J. Bryson, "Robots should be slaves," in *Close Engagements Artificial Companions: Key Social, Psychological, Ethical Design Issues*, vol. 8, Y. Wilks, Eds., Amsterdam, The Netherlands: John Benjamins Publishing Company, 2010, pp. 63–74.
10. F. S. Grodzinsky, K. W. Miller, and M. J. Wolf, "The ethics of designing artificial agents," *Ethics Inf. Technol.*, vol. 10, nos. 2–3, pp. 115–121, 2008, doi: 10.1007/s10676-008-9163-9.
11. D. G. Johnson and K. W. Miller, "Un-making artificial moral agents," *Ethics Inf. Technol.*, vol. 10, nos. 2–3, pp. 123–133, 2008, doi: 10.1007/s10676-008-9174-6.
12. D. G. Johnson, "Algorithmic accountability in the making," *Social Philos. Policy*, vol. 38, no. 2, pp. 111–127, 2021, doi: 10.1017/S0265052522000073.
13. P. Formosa and M. Ryan, "Making moral machines: Why we need artificial moral agents," *AI Soc.*, vol. 36, no. 3, pp. 839–851, 2021, doi: 10.1007/s00146-020-01089-6.
14. L. Munn, "The uselessness of AI ethics," *AI Ethics*, vol. 3, no. 3, pp. 869–877, 2023, doi: 10.1007/s43681-022-00209-w.
15. C. Huang, Z. Zhang, B. Mao, and X. Yao, "An overview of artificial intelligence ethics," *IEEE Trans. Artif. Intell.*, vol. 4, no. 4, pp. 799–819, Aug. 2023, doi: 10.1109/TAI.2022.3194503.
16. J. DeFranco, J. Voas, and N. Kshetri, "Algorithms: Society's invisible puppeteers," *Computer*, vol. 55, no. 4, pp. 12–14, Apr. 2022, doi: 10.1109/MC.2021.3128675.

JEFFREY VOAS, Gaithersburg, MD 20899 USA, is the editor in chief of *Computer*. He is a Fellow of IEEE. Contact him at j.voas@ieee.org.

KEITH MILLER is a member of the Advisory Panel of *Computer* and the Orthwein Endowed Professor for Lifelong Learning in the Sciences at the University of Missouri–St. Louis, St. Louis, MO 63121 USA. Contact him at keith.w.miller@umsl.edu.