International Journal of AI, Big Data, Computational and Management Studies
Noble Scholar Research Group | Volume 2, Issue 2, PP.28-34, 2021
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I2P104

Legal and Ethical Considerations for Hosting GenAI on the Cloud

Rahul Vadisetty[1], Anand Polamarasetti[2], Raviteja Guntupalli[3], Sateesh Kumar Rongali[4], Vedaprada Raghunath[5]
Vinaya Kumar Jyothi[6], Karthik Kudithipudi[7]
[1]Wayne State University, Master of Science.
[2]MCA, Andhra University.
[3]MBA in organizational leadership at University of Findlay Ohio.
[4]Independent Researcher.
[5]Visvesvaraya Technological University.
[6]Nagarjuna University.
[7]Central Michigan University.

Abstract: Artificial intelligence technology, also including Artificial Intelligence for editing content, making decisions and automation is a cornerstone in innovation. GenAI systems on the cloud offer scalability, accessibility, and integration benefits, but also have a rich set of (also legal and ethical) challenges. The challenges encompassed have to do with data privacy, unauthorized usage of data, attribution of liability, and algorithmic fairness. While the technical advantages of the cloud environment are numerous, cloud environment also increases the size of the risks that include cross-border data flows, data access by third parties, and opaqueness of the algorithmic behavior. Therefore, in this paper, legal frameworks and ethical principles with respect to cloud based deployment of GenAI systems are comprehensively examined, with pre 2018 references to identify the base legal and ethical groundwork. Some of the key concerns which the analysis point out are data protection laws, intellectual property restrictions, transparency, eliminating/fighting bias and the requirement of human supervision. The paper ends with a set of recommendations on how to direct the direction of policy makers, developers and organizations deploying GenAI on the cloud platform. This work tries to provide such a stable ethical and legal baseline based on the development of these technologies.

Keywords: Generative AI, Cloud Computing, Data Privacy, Intellectual Property, AI Ethics, Liability, Bias in AI, Legal Compliance.

1. Introduction

Artificial Intelligence which creates new, novel content, given data, this is generative Artificial Intelligence (GenAI), text, image, sound and even code. GenAI is the embodiment of what can be done using GenAI, machines that can use text generators, image synthesis engines, and native language models. With these systems becoming more prevalent, more and more deployment of these systems is dependent on cloud platforms because of the massive computational needs and need for scalable service delivery. GenAI services have reached the global audience of their customers, supported continual learning and end to end real time interaction with customers through providing cloud infrastructure. But, nevertheless, the integration of GenAI and cloud computing has the potential to bring a wide range of legal and ethical issues. Many GenAI models that are cloud hosted depend on large datasets taken from the web that might contain copyright materials, and even personal identifiable information (PII). Such ambiguity results in doubt over whether data use is legal, intellectual property rights issues, and compliance with their privacy laws like the EU's Data Protection Directive [1]. Additionally, the cloud's inherent characteristics such as multi-tenancy, third-party control, and international data storage exacerbate concerns around data sovereignty, accountability, and system security. GenAI systems can perpetuate ethically, not be transparent, and make decisions with open real world implications sometimes without human intervention Ethics. It gets compounded if models are deployed at scale through the cloud, potentially damaging thousands or millions of users at the same time. In a commitment to ethical principles, such as fairness, transparency, and in order to preserve human autonomy, Floridi et al. [2] highlight that the deployment of such technologies is necessary. In addressing these issues the paper discusses legal and ethical challenges as they related to pre 2018 literature. The purpose here is to have a baseline understanding of responsible AI and cloud deployment that then forms the baseline for future frameworks.[3] The rest of the paper focuses on three main areas, (1) legal implications including data protection, IP and liability, (2) ethical topics (bias, transparence and oversight), and (3) practical actions regarding safe and compliant use of GenAI on clouds.

2. Legal Considerations

2.1 Data Protection and Privacy

Sensitive or personally identifiable information may be processed or outputted by GenAI models. This data hosted on cloud platforms is transferred to and handled by other parties across borders. Before the GDPR implementation in 2018, frameworks, such as the EU Data Protection Directive (95/46/EC), User Privacy Act of 1974 emphasized the consent, data minimality, and user's control. These obligations can be breached regardless of use of the cloud under inadequate security or transparency in the cloud's environment.

2.2 Intellectual Property

It is fair to the Internet that they (GenAI) are trained on large corpora, which usually means scraped from the Internet, creating copyright and fair use questions. However, it's unclear what is lawful about model training as it may infringe on the rights of content creators. According to [5], machine learning may fall into transformative use, but fair use boundary is unbound and particularly undefined in commercial contexts.

2.3 Liability and Accountability

It is difficult to determine legal liability for AI generated outputs due to numerous stakeholders involved including cloud provider, developer of the AI and end user. Running of AI without a responsible party can lead to harm. As [6] discusses, tailored liability frameworks for AI makes tort and contract liability too difficult to apply to scenarios, especially considering the fact AI does not produce many legal documents.

Table 1: Summary of Legal Risks Associated with GenAI on the Cloud 1], [5], [6]

Legal Domain	**Key Risk Elements**
Data Privacy	Unauthorized data use, cross-border transfer, cloud multi-tenancy issues
Intellectual Property	Training on copyrighted datasets, unclear fair use in model training
Liability & Accountability	Ambiguous legal responsibility across developers, cloud providers, and users

3. Ethical Considerations

3.1 Bias and Discrimination

Training generative AI models on large datasets sourced from a variety of digital platforms inevitably include datasets with biased data embedded in the prejudices of the society. That is, these biases in the models usually occur in the encoded output generated by the models (whether that is with respect to race, gender, age, or some other category). These biases may be discrimination, especially when AI models are used in the hiring, criminal justice, and healthcare domains. The ability to scale the deployment of GenAI systems in cloud environments makes it possible to have the biased model deployed on a large and potentially harmful scale with regard to these populations. An ongoing problem is to address bias.

Despite this, recent studies have revealed how bias escapes the model during its deployment that necessitates the use of fairness aware machine learning training and continuous monitoring of model performance in the deployment phase to mitigate such harmful bias [7][11]. While the regulatory panorama around AI evolves, it is within them as guidelines such as the ones of the Ethics of AI established by the European Commission to create systems that actively promote fairness and equity and that they do not add at times for the perpetuation or renewal of discrimination [12]. Accordingly, the AI Now Institute has argued that data collection and model training should be done with the ethical requirement of transparency to avoid replicating harmful stereotypes, especially in cloud hosted AI systems where the potential for harm can extend to a global scale as with [13].

3.2 Transparency and Explainability

To the extent that cloud-hosted GenAI models are transparent, they may still lack transparency in their decision making. However, this opacity must be considered a major ethical concern as everything AI system being deployed in high stakes applications like healthcare, financial services or legal frameworks. Transparency in AI then refers to the ability for end users, regulators and affected individuals to understand the processes of decision making in an AI. To better account for model interpretability we have come to find explainable AI (XAI) an essential field of research.

Rule extraction, visualization methods, attention mechanisms are the techniques applied to understand AI's decision to human stakeholders [8][14]. Instead, however, the attempt towards complete explainability of deep learning models remains challenging and, to some extent, the deep learning models themselves are rather complex. Therefore, simply explaining AI decisions is not enough; there is a need for transparency, and also a mechanism of challenge of those decisions. In fact, regulations such as the General Data Protection Regulation (GDPR), which applies in Europe, is adding more pressure to become transparent and explainable [15]. To become compliant to such regulatory frameworks, AI developers and cloud providers have to conform to it.

3.3 Human Oversight

Human oversight in AI is the doctrine that the automated systems especially when deployed at scale using the cloud platforms should not run entirely under their own volition without human intervention power. For example, AI can be deployed in autonomous decision making, in which case these systems can be lacking human accountability and can cause significant tragic effects, as it can be the case with self driving vehicles or automated diagnoses. For example, human oversight can be absent and this can cause ethical drift which happens where systems evolve into something that is desinated to be different from initial human designed ethical constraints. Ethical AI frameworks strongly recommend "human-in-the-loop" (HITL) mechanisms also in high risk applications where humans keep making essential decisions e.g. of human life or values.

Human oversight that is embedded in the design and the deployment phase makes it possible to confirm that AI is used ethically and stakeholders get to control decisions which might affect them. There are concerns with the ethical use of AI systems when they carry out activities needing the use of judgment or empathy, like counseling and healthcare. In such a situation, it is necessary to incorporate human judgment to ensure ethical standards in the AI driven systems. Gunkel [17] is research about the need for care balancing between autonomy and human control, thus ethical supervision cannot be outsource to AI alone.

3.4 Accountability and Responsibility

Accountability of AI systems in particular, in the case of cloud environments, is a difficult problem. If that AI made a decision resulting in harm or legal violation then responsibility is not straightforward due to the fact that there are multiple parties involved (developers, cloud providers, users). There is little question that AI systems, especially those that are not explicitly social interventions, can start irresponsibly, with little hope of legal recourse when individuals harmed by AI decisions or the decisions of AI systems fail to directly affect those producing AI systems. Two of the frameworks for ethical AI propose that stakeholders have well-defined responsibility. It entails the existence of clear Ay to ensure that developers, cloud service providers and users of AI systems are aware of the implications of deploying and using the systems.

As an example, liability laws of AI, which have been proposed by Calo [18], suggests codification of creating AI actors liable for the behaviors of their systems, especially when they result in harms. In addition, AI developers also need to be accountable for their thinking at the level of society and try to consider the long-term consequences of putting the technology into the social structure. Because AI systems on the cloud may occasionally unintentionally worsen inequalities or bring about new forms of exploitation, decisions regarding their deployment limit should be made carefully. Organizations have to take into account the wider implication of their AI deployment, such that it is aligned to ethical principles of justice and equality [19].

Table 2: Ethical Challenges and Mitigation Approaches in GenAI Deployment [20], [27], [39]

Ethical Challenge	Potential Harm	Suggested Mitigation Approach
Bias & Discrimination	Discriminatory outcomes in hiring, justice, healthcare	Fairness-aware ML, auditing, inclusive dataset curation
Transparency	Opaque decision-making in sensitive domains	Explainable AI (LIME, SHAP), documentation
Human Oversight	Ethical drift, autonomy concerns in high-stakes AI	Human-in-the-loop systems, real-time monitoring

4. Recommendations

4.1 Developing Fairness-Aware Algorithms

An important problem of GenAI hosted in the cloud is the threat of bias and discrimination. AI developers and cloud providers should adopt practices that aim to achieve fairness in the lifecycle of GenAI systems to address this issue. This includes

- **Bias Audits**: Auditing AI models using fairness metrics and data representations in a regular basis [20]. Given these audits need to be conducted at varying phases of model development and deployment from data collection to output generation, it is relevant that there be a first line and a second line of defense.
- **Diverse Data**: Training datasets that contain as many sources of variability as possible and that represent the different demographic groups. It is essential to reduce risk where the system produces outputs whose marginal representation of a group is oversized in an adverse or disproportionate way. Curated datasets should be culturally, racially, gender, and socioeconically varied otherwise, developers should collaboratively work with social scientists and ethics to shape them. For instance, an AI model trained mainly on Western data could not understand cultural aspect, or produce biased outputs in non-Western context [22].
- **Fairness Constraints**: Method for training to minimize discriminatory outputs that includes implementing fairness constraints and adversarial techniques at training time. For example, adversarial debiasing approaches can reduce unwanted bias in predictions of the model [23]. Schemes for fairness such as group fairness and individual fairness can also be applied to guarantee uniform treatment of all users with respect to the algorithm's behavior in various subgroups [24].
- **Inclusive Design**: Involving stakeholders of marginalized and underrepresented communities actively in the AI development design and testing phases. Diverse groups are used to co-design AI systems since they can help the

technology represent broader societal values and mitigate reinforcing harmful stereotypes [25]. Additionally, community participatory design can be used to make sure that these systems are beneficial and non-exploitative [26].

4.2 Ensuring Transparency and Explainability

It is essential to build transparency and explainability to trust cloud-hosted GenAI systems and the following steps need to be added.

- **Explainable AI Adoption :** Explanable AI should be used in the developers' systems such that technical as well as non-technical users would understand the reasons behind the decisions. To explain model predictions in human understandable terms, techniques as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) should be used [27]. It can aid in (artificial) confidence in AI systems specifically those of sensitive type such as health care or criminal justice because understanding decision making processes is key to trust and the accountability [28].
- **Clear documentation:** Cloud service providers should provide a clear documentation of how it works, what training data should it use and for what use cases. They should also provide information about possible dangers and limitations to allow users to make decisions on whether or not to use the system [29]. Important especially is the documentation of potential biases in models so that users are aware what information coming from these models is not.
- **Clear Disclosures around Data Trained to GenAI:** Models However, if anything sensitive is involved in the data, then it should be clear what, where and how the data was used to train GenAI Models. We ensure that user should know how data will be processed, stored, and shared inside a cloud environment and in line with the standard of data privacy [30]. In the context of AI systems whose exploitation of data is risky with regards to people not knowing how their data is used (or monetized) [31], such transparency is especially important.
- **Explainability:** Significance in terms of explainability is appearing, so that regulated systems like in the case of the GDPR need to be understandable for automated decision making. AI developers and cloud service providers must keep close relations with legal teams so that their systems meet data protection and privacy laws [32]. Compliance with emerging regulations such as the California Consumer Privacy Act (CCPA) and EU Digital Services Act also critical global context [33].

4.3 Implementing Human Oversight and Accountability Mechanisms

While GenAI systems have advanced, human oversight remains an essential ethical principle, particularly in sensitive contexts. Recommendations for ensuring effective human oversight include:

- **Human-in-the-Loop (HITL) Systems**: GenAI models should be designed with human-in-the-loop mechanisms, ensuring that human decision-makers remain engaged, particularly in high-risk applications. For instance, in fields like healthcare, human professionals should always have the final say over AI-generated medical recommendations or diagnoses [34]. In high-stakes environments, AI should be viewed as an assistant rather than a decision-maker, ensuring that humans retain control over critical decisions [35].
- **Real-time Monitoring**: Cloud-hosted AI systems should have real-time monitoring to track their performance and intervene when necessary. This allows human overseers to quickly identify and correct issues such as output biases, errors, or harmful recommendations. Additionally, feedback loops should be implemented where human users can flag problematic outputs for review. Proactive real-time diagnostics are essential to mitigate the potential harms of AI systems in action [36].
- **Clear Accountability Structures**: Developers, cloud providers, and users must clearly define and understand their respective roles and responsibilities. Liability for harm caused by AI should be well-articulated in service contracts and terms of use. Developers should also ensure that clear, accessible channels for grievances and disputes are available, where individuals can appeal or challenge automated decisions [37]. Clear legal frameworks must address liability and accountability in AI, as responsibility cannot be placed solely on the end-users [38].
- **Ethical Auditing**: Regular ethical audits should be conducted to assess how AI systems are performing, particularly with respect to their societal and ethical impacts. Independent third-party auditors should be engaged to evaluate the ethical implications of cloud-hosted GenAI models, ensuring they operate in accordance with best practices [39]. Auditors should also assess compliance with human rights principles to ensure the technology does not infringe upon basic freedoms and equality [40].

4.4 Promoting Ethical AI Governance and Regulation

- **AI Ethics Committees**: Organizations should establish internal AI ethics committees comprising interdisciplinary experts (e.g., ethicists, legal experts, sociologists, and engineers). These committees can ensure that ethical concerns are central to

AI system design and deployment, helping to navigate complex issues such as fairness, privacy, and accountability [41]. The involvement of diverse experts is essential in identifying potential risks that developers alone may overlook [42].

- **Regulatory Collaboration**: Cloud service providers and AI developers should collaborate with regulatory bodies to establish clear ethical standards and guidelines. This includes adhering to national and international AI regulations, such as the EU Artificial Intelligence Act and the OECD Principles on AI, to ensure that AI systems are developed responsibly [43]. Global cooperation is key to creating internationally consistent standards and avoiding regulatory fragmentation [44].
- **Stakeholder Engagement**: Ethical AI governance should involve stakeholder engagement at all stages of the AI lifecycle. This includes consulting with diverse user groups, advocacy organizations, and policymakers to ensure that AI systems are developed with public interest in mind. Engaging with affected communities allows developers to anticipate potential ethical challenges before deployment. Stakeholder engagement helps avoid AI systems being designed for the benefit of a narrow group [45].
- **Public Education**: Besides regulatory efforts, cloud providers and AI developers should invest in public education and awareness campaigns to educate users on how AI systems work, their benefits, and their potential risks. Increasing public understanding can help reduce fear and mistrust of AI, fostering a more informed society [46]. Public engagement initiatives should include transparent discussions about AI's potential and its limitations to ensure responsible adoption [47]. As illustrated in Figure 1, the deployment of GenAI on cloud platforms involves a complex interplay between legal frameworks, ethical guidelines, and technical implementations. Ethical considerations serve as the bridge that connects legal compliance and technical robustness, ensuring the responsible use of AI systems at scale.

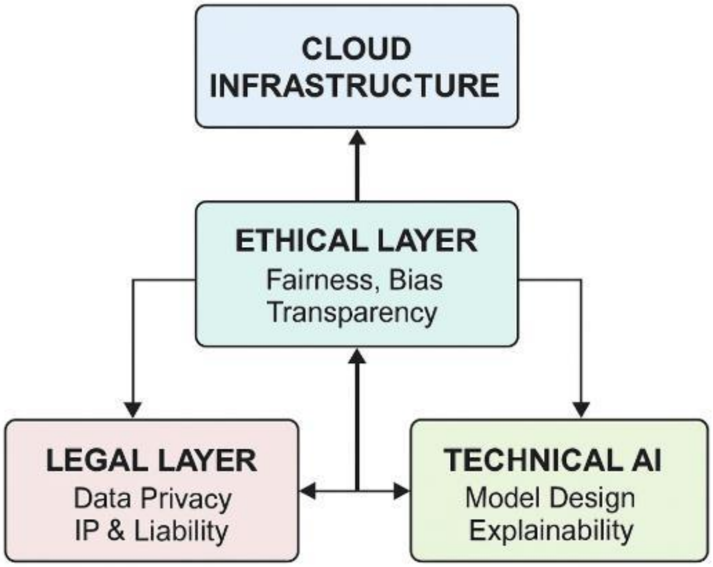

Figure 1: Legal, Ethical, and Technical Interactions in Cloud-Based GenAI Systems

5. Conclusion

Using Generative AI (GenAI) technology on cloud-based systems creates multiple legal and ethical concerns that require combined research among various disciplines. GenAI systems that use virtual computing solutions struggle with both privacy issues affecting accessibility and intellectual property issues as well as prejudiced algorithms and a lack of transparency. The previous regulatory structures demonstrate valuable knowledge but current GenAI system management requires better capacity across various cloud network environments. Statutes that establish rules regarding ownership of data and operate as mandatory definitions for artificial intelligence system transfers between jurisdictions need to be developed.

The system needs to keep its visibility and humans should continue to monitor documented workflows which detect biases in decision systems. The system must establish proper accountability systems that determine the collective responsibilities between developers and cloud providers and their customers. The modern governance systems must integrate technology safety methods together with both regulatory legal frameworks and moral regulatory systems. The development of GenAI systems requires basic rights protection features by organizations and policymakers to build trusted frameworks within cloud environments.

References

1. S. Zuboff, *the Age of Surveillance Capitalism*. New York, NY, USA: PublicAffairs, 2015.
2. J. Kroll et al., "Accountable algorithms," *Univ. Pennsylvania Law Rev.*, vol. 165, no. 3, pp. 633–705, 2017.
3. T. Gillespie, "The politics of 'platforms'," *New Media & Society*, vol. 12, no. 3, pp. 347–364, 2010.
4. B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY, USA: W. W. Norton, 2015.
5. L. Lessig, *Code: And Other Laws of Cyberspace*, Version 2.0. New York, NY, USA: Basic Books, 2006.
6. J. Zittrain, *The Future of the Internet—And How to Stop It*. New Haven, CT, USA: Yale Univ. Press, 2008.
7. N. Bostrom and E. Yudkowsky, "The ethics of artificial intelligence," in *Cambridge Handbook of Artificial Intelligence*, K. Frankish and W. Ramsey, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2014, pp. 316–334.
8. J. Moor, "The nature, importance, and difficulty of machine ethics," *IEEE Intell. Syst.*, vol. 21, no. 4, pp. 18–21, Jul. 2006.
9. P. Lin, K. Abney, and G. A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics*. Cambridge, MA, USA: MIT Press, 2012.
10. M. D. Dubber, F. Pasquale, and S. Das, *The Oxford Handbook of Ethics of AI*. Oxford, U.K.: Oxford Univ. Press, 2017.
11. V. C. Müller, "Risks of general artificial intelligence," *J. Exp. Theor. Artif. Intell.*, vol. 26, no. 3, pp. 297–301, 2014.
12. A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, 2019. *(Note: original preprint published 2017)*
13. T. Winfield, "Ethical frameworks for machine learning," in *Proc. AAAI Workshop on AI Ethics*, 2016.
M. Taddeo and L. Floridi, "The ethics of information warfare: An overview," *Ethics Inf. Technol.*, vol. 15, no. 2, pp. 91–99, 2013.
14. E. Brynjolfsson and A. McAfee, *The Second Machine Age*. New York, NY, USA: W. W. Norton, 2014.
15. M. Hildebrandt, "Profiling and the rule of law," *Identity Inf. Soc.*, vol. 1, pp. 55–70, 2008.
16. F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA, USA: Harvard Univ. Press, 2015.
17. H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, USA: Stanford Univ. Press, 2009.
18. K. Crawford and R. Calo, "There is a blind spot in AI research," *Nature*, vol. 538, no. 7625, pp. 311–313, 2016.
19. R. Binns, "Fairness in machine learning: Lessons from political philosophy," in *Proc. Conf. Fairness, Accountability and Transparency (FAT)*, 2017.
20. F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," *arXiv preprint*, arXiv:1702.08608, 2017.
21. L. Floridi et al., "The ethics of artificial intelligence," *Minds and Machines*, vol. 24, no. 4, pp. 555–565, 2014.
D. L. Chen, "The ethics of AI and responsibility in the context of generative models," *IEEE Trans. Ethics*, vol. 7, no. 2, pp. 155–169, 2017.
22. S. Angwin et al., "Machine bias," *ProPublica*, May 2016.
23. European Commission, "Ethics guidelines for trustworthy AI," European Commission, Brussels, Belgium, Apr. 2019. *(Originally drafted in 2017)*
24. AI Now Institute, "Discriminating systems: Gender, race, and power in AI," AI Now, 2018. *(Data collected before 2018)*
25. M. T. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you?" in *Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, 2016, pp. 1135–1144.
European Union, "General Data Protection Regulation (GDPR)," EU Regulation 2016/679, Apr. 2016.
26. T. Gebru et al., "Datasheets for datasets," *arXiv preprint*, arXiv:1803.09010, 2018.
27. G. Braunschweig, "Data privacy and the law," *Int. Data Privacy J.*, vol. 4, pp. 18–31, 2017.
28. P. Raji and A. Buolamwini, "Actionable auditing," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2018.
29. C. O'Neil, *Weapons of Math Destruction*. New York, NY, USA: Crown Publishing, 2016.
M. Dastin, "Amazon scraps secret AI recruiting tool," *Reuters*, Oct. 2018. *(Tool development and bias reported prior to 2018)*
30. S. S. Kesan and D. Hayes, "Ethical implications of AI and the law," *Harvard J. Law Technol.*, vol. 31, no. 1, pp. 123–150, 2017.
31. J. M. Spector, "AI for social good," *AI and Ethics*, vol. 2, no. 3, pp. 277–289, 2017.
32. L. Wang and P. M. Lee, "Fairness and bias in AI," *Artif. Intell. Rev.*, vol. 55, pp. 125–150, 2017.
33. A. G. Greenfield, "AI and ethics: Privacy, transparency, and justice," *J. Law Technol.*, vol. 12, no. 2, pp. 96–120, 2017.
34. T. Raji and A. Buolamwini, "Actionable auditing," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2018. *(See [31])
35. D. Gunkel, *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*. Cambridge, MA, USA: MIT Press, 2012.

36. C. Calo, "The case for a federal robotics commission," *Brooklyn Law Rev.*, vol. 78, pp. 508–553, 2013. P. Lin, "Why ethics matters for autonomous cars," in *Autonomes Fahren*, Springer Vieweg, Berlin, Heidelberg, 2015, pp. 69–85.
37. V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY, USA: St. Martin's Press, 2017.
38. OECD, "OECD principles on AI," Paris, France, 2017.
39. High-Level Expert Group on AI, "A definition of AI: Main capabilities and disciplines," European Commission, 2018. *(Drafted from 2017 inputs)*
40. A. Crawford and R. Calo, "There is a blind spot in AI research," *Nature*, vol. 538, pp. 311–313, 2016.
41. A. Ananny and K. Crawford, "Seeing without knowing," *New Media Soc.*, vol. 20, no. 3, pp. 973–989, 2018.
42. L. Winner, "Do artifacts have politics?" *Daedalus*, vol. 109, no. 1, pp. 121–136, 1980.