Published on *The National Law Review* https://natlawreview.com

NY State Bar Association Joins Florida and California on AI Ethics Guidance – Suggests Some Surprising Implications

Article By:

James G. Gatto

The NY State Bar Association (NYSBA) Task Force on Artificial Intelligence has issued a nearly 80 page report (Report) and recommendations on the legal, social and ethical impact of artificial intelligence (AI) and generative AI on the legal profession. This detailed Report also reviews AI-based software, generative AI technology and other machine learning tools that may enhance the profession, but which also pose risks for individual attorneys' understanding of new, unfamiliar technology, as well as courts' concerns about the integrity of the judicial process. It also makes recommendations for NYSBA adoption, including proposed guidelines for responsible AI use. This Report is perhaps the most comprehensive report to date by a state bar association. It is likely this Report will stimulate much discussion.

For those of you who want the "Cliff Notes" version of this report, here is a table that summarizes by topic the various rules mentioned and a concise summary of the associated guidance.

The Report includes four primary recommendations:

1. Adopt Guidelines: The Task Force recommends that NYSBA adopt the AI/Generative AI guidelines outlined in this report and commission a standing section or committee to oversee periodic updates to those guidelines.
2. Focus on Education: The Task Force recommends that NYSBA prioritize education over legislation, focusing on educating judges, lawyers, law students and regulators to understand the technology so that they can apply existing law to regulate it.
3. Identify Risks for New Regulation: Legislatures should identify risks associated with the technology that are not addressed by existing laws, which will likely involve extensive hearings and studies involving experts in AI.
4. Examine the Function of the Law in AI Governance: The rapid advancement of AI prompts us to examine the function of the law as a governance tool. Some of the key functions of the law in the AI context are: (i) expressing social values and reinforcing fundamental principles; (ii) protecting against risks to such values and principles; and (iii) stabilizing society and increasing legal certainty.

The Report addresses of some of the risks of AI, including:

- **The Widening Justice Gap:** noting that while AI may be a solution to democratization of justice, it may create a “two-tiered legal system,” relegating individuals in underserved communities or with limited financial means relying on inferior AI-powered technology. This may be exacerbated by obstacles in accessing the benefits that AI may bring to others, including: i) lack of access to computers/internet; ii) limited facility/literacy in how to use AI; and iii) a high level of distrust in government institutions, law as a tool that operates to protect them, law enforcement as a positive influence and/or legal professionals as people who are available to help.
- **Data Privacy & Surveillance:** concerns about the potential of AI to corrupt civil liberties and data privacy based on the ability for AI systems to aggregate vast amounts of personal data, which could lead to privacy invasions, including: i) governments and corporations using AI for comprehensive surveillance and social control; and ii) hackers using AI tools to synthesize personal data to impersonate individuals via deepfakes and committing cyber theft. The Report also notes concerns with lack of transparency in training data, biases built into models and ownership of intellectual property.
- **Security:** In addition to cyber threats, general security concerns accompanying AI use which concerns are amplified when AI is used in high-risk applications, such as in conjunction with biometric data and infrastructure systems.
- **Social and Ethical Issues:** noting that AI algorithms have been used to perpetuate and amplify societal biases, including: i) gender and racial bias; ii) an increase in adverse psychological issues related to AI (e.g., AI chatbot suicide); iii) the assignment-of-liability when decisions are made by AI systems; iv) ideological bias, especially when used in conjunction with social media; and v) the creation of an “echo chamber” by generating spurious content to use as future training data, leading to ideologically based “hallucinations” and inaccuracies.
- **Misinformation:** making “deepfakes” more believable by combining them with biometric data (e.g., voice prints and facial mapping
- **Economic Impact and Disruption:** noting that the economic impact of AI is multilayered, including the direct effect of job displacement where tasks are automated and the indirect effect of devaluing services traditionally offered by a human (e.g., legal services).
- **Safety:** expanding on the general societal issues noted above, the Report notes several safety concerns including how we respond when AI systems that operate in critical roles fail and cause harm AI’s potential to manipulate emotions that could lead to psychological harm, an overdependence on AI that could lead to loss of human skills and abilities and that AI has been shown to behave unpredictably, which may result in harmful or unintended consequences.
- **Legal and Regulatory Challenges:** the Report comments on how the law struggles to assign liability when AI causes damage or harm, how courts are grappling with issues involving intellectual property, including copyright (e.g., training data protections), ownership of output and invention patenting, that current laws and regulations have failed to keep pace with AI development and that there will continue to be difficulty in enforcing laws across borders as most technology companies offer global AI systems.
- **Loss of Human Centricity and Control:** it mentions concerns where AI develops autonomously, creating an existential threat where AI systems operate beyond human understanding and control, risks that AI may make critical decisions without human oversight or ethical considerations and that AI decisions may not value human life nor human generated output, resulting in us being imperiled by AI that makes moral decisions without human empathy or understanding.

Regarding lawyers’ ethical obligations, the Report discusses the legal profession impact, noting that when using any technology in legal practice, attorneys must remain compliant with the Rules of Professional Conduct. It notes that with generative AI tools, the number of rules implicated may be "surprising." A brief overview of *some* of the rules it identifies as being implicated include:

- Duty of Competency/Techno-solutionism: "*A refusal to use technology that makes legal work more accurate and efficient may be considered a refusal to provide competent legal representation to clients*." RPC Rule 1.1. While some attorneys are avoiding the use of AI, this point suggests that a refusal to do so might be an ethical violation.
- Duty of Confidentiality & Privacy: RPC Rule 1.6 extends to what client information a lawyer may share when using certain generative AI tools, including information entered into AI engines, such as chatbots, and when such entries are then added to the training set for the AI. The Report notes this may violate protective orders.
- Duty of Supervision: RPC Rule 5.3, which imposes a duty to supervise non-lawyers involved in client representation, covers non-human entities (e.g., AI).
- Unauthorized Practice of Law (UPL): noting that there is no nationally agreed definition of what constitutes UPL, the Report notes that AI programs that do not involve a human-lawyer in the loop in providing legal advice arguably violate the rules and may be considered UPL.
- Attorney-Client Privilege and Attorney-Work Product: RPC Rule 1.6 (and model rules) may be violated when revealing attorney[1]client privileged information or attorney-work product when directly and indirectly using generative AI tools, such as through:
    - Direct Use of AI as an app (e.g., the user directly enters a prompt that contains private or confidential information, which then goes into the app)
    - Indirect Use of AI that is embedded in search engines (e.g., the user enters a prompt that contains private or confidential information, which then goes into the AI app)
    - Use of Application Programming Interface/API (using some other application that connects to AI via the API, private or confidential information is inputted into the AI)
    - AI plugins (accessing other applications from within AI via plugins, which conveys private or confidential information further into AI or other places too (e.g., when other users/persons can see/view your private or confidential information).

The Report further notes that in connection with these issues, attorneys need to be mindful of how the AI tools they are using work and should consider: i) Licensing Information; ii) Terms of Use; iii) Privacy Policies; iv) Frequently Asked Questions/FAQs list; v) whether data supplied to or inputted into the AI may be used for training purposes or to refine/improve the AI model; vi) whether data that is supplied to or inputted into the AI may be viewed by and disclosed to third parties/vendors in the training of the AI model; and vii) whether data output by the AI may be viewed by third parties, including opponents and adversaries.

- AI and Cybersecurity Risks Open: AI may raise both ethical violations and cybersecurity issues. For example, "if there is a cyber intrusion … not only will that data potentially be lost to threat actors, but they could conceivably also obtain the firm's searches… access into the mind of a lawyer and the arguments they might be raising."
- Preservation of Data: Data preservation and litigation hold obligations may present similar challenges for attorneys and the court. The Report notes that if the data input into the AI application is temporary/ephemeral, but also relevant and responsive to the litigation, the parties have the duty to preserve this electronically stored information. Yet, it notes it may not be clear how do preserve what may no longer exist. [*Note*: *While not specifically mentioned, this suggests that there may be a duty to log and maintain the inputs and potentially the outputs*.]
- Candor to the Court: not surprisingly, the Report notes that attorneys must verify the accuracy

of the information and legal authority produced by such tools. It adds that Attorneys' signatures and attestations on legal documents submitted to the court, make representations about case law and other authorities relied upon in support of the attorney's case. RPC Rule 3.3(a) (1). The Report discusses that the attorney's responsibility extends to AI hallucinations and deepfakes.

- Judges' Ethical Obligations: the Report notes that the model rules state "A judge shall uphold and promote the independence, integrity and impartiality of the judiciary." It concludes that while AI can and does assist judges in a variety of ways, judges will always have the responsibility of exercising their own judgment: the human trait of independent judgment.

The Report covers some items beyond those addressed in the ethical guidelines published by the Florida State Bar, which we discussed here and the State Bar of California Guidance For The Use Of Generative Artificial Intelligence In The Practic-e Of Law.

National Law Review, Volume XIV, Number 99

Source URL:https://natlawreview.com/article/ny-state-bar-association-joins-florida-and-california-ai-ethics-guidance-suggests