Ethical Obligations to Protect Client Data when Building Artificial Intelligence Tools: Wigmore Meets AI

Daniel W. Linna Jr. & Wendy J. Muchman

27 Professional Lawyer 1 (Oct. 2, 2020)

October 02, 2020 **FEATURE**

Ethical Obligations to Protect Client Data when Building Artificial Intelligence Tools: Wigmore Meets AI

By Daniel W. Linna Jr. & Wendy J. Muchman

Introduction

Artificial intelligence and data analytics ("AI")[1] tools are regularly proposed as critical tools that will lead to the transformation of many legal tasks: legal research, contract review, contract management, the prediction of litigation outcomes, and more.[2] While roughly two-thirds of in-house attorneys are ready to try new technology and say they have access to client data, only around half of that number of lawyers feel they are effectively using client data.[3] What is holding them back?[4] Is it a fear that AI will replace lawyers? If so, it is worth clarifying the functionality and capabilities of AI tools that exist now and that are likely to exist soon. Moreover, developing tools that automate and augment legal tasks provides lawyers with more time to employ emotional intelligence, still unique to lawyers, and give creative and strategic advice when handling client matters.[5] There is no shortage of complex problems to be solved. There are countless ways in which lawyers can help develop AI to provide value to clients and society, while at the same time increasing the value provided with uniquely human skills.

> The advent of new technology requires an ongoing assessment of how a lawyer's ethical obligations intersect with the use of technology

Getty Images

Despite the growth in opportunities that AI offers, it also presents new ethical issues. The intersection between legal ethics and AI is an emerging and rapidly changing area. This can cause confusion when lawyers try to understand what is required of them. Ethics opinions, case law, data breach notification requirements, and disciplinary cases will continue to illuminate the specifics of a lawyer's ethical obligations concerning AI in this evolving landscape.

The advent of new technology requires an ongoing assessment of how a lawyer's ethical obligations intersect with the use of technology.[6] In this piece, we will examine lawyers' ethical obligations when using client data to build AI tools and how lawyers can minimize the potential ethical risks that arise. Use of client data in AI tools encompasses a variety of ethical responsibilities including those regarding competent representation (Model Rule 1.1), client communication (Model Rule 1.4), client informed consent (Model Rule 1.6), protection of client property (data) (Model Rule 1.15), and client confidential information (Model Rule 1.6).

A Look at Wigmore's Data Analytics Tools: Four Scenarios

Scenario One

Let us start with a hypothetical: the Wigmore law firm. Imagine that Wigmore creates a data analytics group. A Wigmore attorney believes that there is a market for a data analytics tool that predicts the likelihood of success in litigation involving commercial leases. This Wigmore attorney and the data analytics group collect data from hundreds of commercial lease cases from publicly available dockets of local courts. Wigmore launches a product (Lease Dispute Analyzer 1.0), which predicts the likelihood of a commercial lessor prevailing in a lawsuit to collect unpaid rents for the duration of a lease after a lessee abandons the property. Wigmore wants to use Lease Dispute Analyzer 1.0 to help its clients predict the likelihood of success in future litigation. In this scenario, assuming no Wigmore client data is used in Lease Dispute Analyzer 1.0, Wigmore has the general obligation to represent all firm clients competently, to properly supervise its data analytics group,[7] and in most jurisdictions, to avoid assisting in the unauthorized practice of law or sharing legal fees with nonlawyers.[8]

Scenario Two

Let us now change the hypothetical and create a second scenario. Imagine that Company X is a large commercial real estate company that owns and manages hundreds of commercial buildings. Company X is the plaintiff in a pending case at the summary judgment stage, and it retains

Wigmore to advise it whether to settle or continue to litigate. Company X has a significant amount of data regarding prior cases in which it was a party. Wigmore is interested in developing a data analytics tool using Company X's data to advise Company X about the strength of its case and the benefits of pursuing a settlement at this stage. Company X provides its data to Wigmore. What are Wigmore's ethical obligations to Company X?

Scenario Three

Consider now a third scenario, in which Wigmore has a longtime client Company Y, another large lessor of commercial properties. Through its past representations of Company Y, Wigmore has extensive records on the results of hundreds of cases Company Y has litigated, providing for considerable data points for data analytics.[9] Many of these data points have been obtained by Wigmore as a result of, and in the course of, its representation of Company Y. Because there are many thousands of data points, Wigmore would like to have its in-house analytics department include Company Y's data in the development of the model for Company X. What obligations does Wigmore now have to Company Y? To Company X?

Scenario Four

Finally, envision a fourth and final scenario, in which Company Z, a large lessor of commercial properties, wishes to engage Wigmore to file numerous lawsuits against commercial lessees who have vacated properties before the expiration of their leases. Company Z has asked Wigmore to use the models created for Company X and Company Y, and the underlying data, to create a tool that will help Company Z analyze and evaluate their prospective lawsuits. What are Wigmore's obligations to Company X, Y, and Z?

We will consider various ethical issues arising from Wigmore's use of its three clients' data to develop AI tools in these four scenarios.

Competence

Under all scenarios, Wigmore is required to provide competent representation.[10] "The legal rules and procedure, when placed alongside everchanging technology, produce professional challenges that attorneys must meet to remain competent."[11] Competent representation requires an awareness of the "benefits and risks associated with relevant technology."[12] For example, lawyers need to be knowledgeable about and able to advise clients on the selection of appropriate AI-driven predictive coding tools for e-discovery.[13] A lawyer's duty of competence is nondelegable to a nonlawyer, even when the client employs an expert in any of the processes.[14] Although a lawyer may not delegate the duty of competence, he or she may rely on advisors of established technological competence in the relevant field.[15] Therefore, if the lawyer or law firm and its data scientists are developing models to predict acceptable settlement ranges, the lawyers must satisfy their duty of competence which means the lawyers must understand the model, how the data was obtained and input, and be satisfied that the settlement amount is within an appropriate range.

If Wigmore is developing predictive analytics for Company X, Company Y, and Company Z, competent representation requires that Wigmore understand the benefits and risks of using client data in developing those programs. The possible benefits of the use of client data include more accurate and therefore more effective predictions of litigation outcomes, with less effort, faster, increasing efficiency and perhaps producing cost savings. A possible risk includes the model producing low-quality predictions, but the accuracy of the predictions should be evaluated in comparison predictions made by other means, including by other technology tools and by humans.[16]

When accumulating data that triggers lawyers' confidentiality obligations, the risks of a data breach and possible inadvertent revelation of confidential information are of concern.[17] Additional risks that should be considered include lack of representativeness of the data used and bias introduced in data collection, data cleaning, and data creation. Like all humans, data scientists, engineers, and lawyers alike have biases, and these biases can impact decisions about what data to gather, how models are created, the resulting predictions those models make, and more.[18]

Part of being competent requires using tools that are effective. To assess an AI tool's effectiveness, the Wigmore lawyers must understand the risk of bias and how it will impact the tools developed by the technologists in its data analytics group. Additionally, lawyers must have heightened awareness of possible discriminatory bias that could be incorporated into, and perhaps be exacerbated by, AI tools.[19] In addition to exercising care to mitigate bias when using AI for decisions that history tells us are fraught with bias, such as hiring and evaluating employees, lawyers should carefully consider the ways in which bias could be replicated or exacerbated by any AI tool. That said, lawyers can also consider the ways in which AI tools may reduce bias in human decision-making processes and serve as a positive force for equity.[20]

Communication

Lawyers are required to communicate with their clients in certain ways. They are required to promptly inform clients of any decision or circumstance requiring the client's informed consent, as defined in Rule 1.0(e).[21] If Wigmore wants to use a client's data to build a tool, Wigmore must communicate with that client about the plans to build the tool and obtain the client's informed consent to use the client's data.[22]

Informed consent is a fundamental principle of lawyers' representation of clients. The requirement to obtain it is contained in almost one-third of all ethics rules. Informed consent is a substantial part of building good client communication.[23] As explained in Comment [6] to Model Rule 1.0, consent is *informed* when it is given after explaining (1) "the facts and circumstances" that apply to the situation, (2) the "material advantages and disadvantages" of the proposed action, and (3) any "options and alternatives."[24]

Thus, as part of proper client communication, Wigmore must explain the AI tool and obtain each client's informed consent for the use of client data and the use of the tool. Lawyers must make

plain: how the AI tool works, its purpose, the information that will be used in its development, the value it adds to the litigation, and what the lawyer will do with the information. The lawyers' explanations must be sufficient to allow the client to participate intelligently in decisions concerning the objectives of the representation and the means by which they are pursued.[25] For example, courts have found a lack of *informed consent* when a lawyer failed to explain "possible ramifications" and "potential consequences" of a proposed course of action to the client.[26]

Care of Property: Client Data is Property

When Wigmore uses client data to build predictive analytics tools, the lawyers and the firm are required to safeguard the client data with the care of a professional fiduciary.[27] Ethics opinions suggest that "property" includes information stored in electronic form.[28] ABA Ethics Op. 483 starts by noting that lawyers' obligations to protect client information do not change based upon whether the information is in paper or electronic form.[29] Recognizing that many courts have moved to electronic filing and law firms routinely transfer and store client information in electronic form, the realities of today's practice of law dictate that the requirement to safeguard client property extends to client property in electronic form.[30] These ethics opinions also recognize that when lawyers hold client information in an electronic form, they must still exercise reasonable precautions to safeguard client data under Rule 1.15, make sure the information remains in an accessible form, and guard against the risk of unauthorized disclosure.[31]

Confidentiality

Lawyers are required to protect all client information from both intentional and inadvertent disclosure.[32] Given the prevalence of law firm data breaches,[33] lawyers must be especially careful when acquiring and storing client data.[34] The ethical rules establishing a lawyer's duty of confidentiality to her clients explicitly allow for the disclosure of confidential information when it is authorized by the client's informed consent.[35] However, the confidentiality rule and interpretative ethics opinions are clear that absent informed consent, all client information is confidential and cannot be revealed regardless of its source and regardless of whether it is available in the public record.[36]

Confidential information may be revealed when permitted or required by an exception, but lawyers' use of confidential information to develop a software tool that will be used to assist other clients does not fall within any express exception.[37] Further, while the confidentiality rule allows for disclosure when it is impliedly authorized to carry out the representation, in most circumstances it would be risky to conclude that building a software tool is the type of disclosure contemplated by this exception.[38] As a general rule, building a analytics tool is not a routine part of representation covered under this exception. Therefore, lawyers should obtain the client's informed consent before using client information to develop AI tools.

As discussed above, informed consent is part of good communication with a client and requires the lawyer to communicate the underlying facts giving rise to the proposed course of conduct.[39]

For example, when a lawyer seeks informed consent to use the client's information to develop an AI tool, the lawyer should also disclose if and how that tool may be used in the future for both the current client and other clients. In light of historical breaches of law firm data, communicated risks should include the possibility of a data breach and subsequent responsibilities under applicable rules of professional conduct and state data privacy laws.[40]

Notably, depending upon the task to be performed, informed consent requires a discussion of the possible alternatives to the proposed conduct.[41] The lawyer must communicate the possibility of achieving a similar result without the use of AI. Lawyers should also consider advising the client on various AI options: categorizing and clustering documents; flagging and extracting information from documents; generating drafts of contracts, pleadings, motions, briefs, and other documents; and predicting litigation outcomes; to name a few, and the multitude of potential uses.[42] All of these disclosures should be made with the intention of ensuring that the client has enough information to make an informed decision.[43] While informed consent for the disclosure of confidential information is not typically required to be in writing, best practices would suggest that the consent should be in writing to provide a clear record of the details of the client's consent.[44]

The initial engagement letter is a good vehicle by which to memorialize the client's informed consent. By obtaining informed consent to use client information to develop AI tools from the start of the representation, the lawyer minimizes potential ethical issues. While many of the potential confidentiality concerns surrounding the use of AI technologies can be addressed in the initial engagement letter, situations will inevitably arise that were not originally contemplated. For example, if after a representation has begun a lawyer begins to develop AI tools and later wishes to use the client's data to further develop the tool. When these situations occur, the lawyer should revisit the informed consent to ensure the required proper discussions with and disclosures to the client have occurred and that the client has provided informed consent.

With respect to inadvertent disclosures of confidential information, the ABA has issued guidance related to the use of technology. Ethics opinions and the Model Rules require a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of client information.[45] To determine what constitutes "reasonable efforts," lawyers should consider factors such as: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients."[46]

Complex confidentiality issues arise when Wigmore wants to use one client's data for another client, such as X's data for Y or X and Y's data for Z. Because AI tools are generally most effective in learning to make predictions when they have access to the largest pool of relevant data,[47] Wigmore has an incentive to feed as much relevant client information into the tool as possible. In this situation, the client's confidential information essentially becomes part of the tool, thus providing value to other clients. Wigmore should also consider that using this tool with other clients may expose the underlying confidential information to those other clients.[48]

Wigmore should consider how to minimize the amount of confidential information that is used in the creation or application of the tool. A common thread through the ethical rules involving the disclosure of confidential information, when not authorized by the client, is that the lawyer should take pains to disclose the minimum amount of information necessary.[49] This concept applies to the use of client information in AI tools as well. To minimize the risk of disclosure of information, lawyers should tailor the client data used to the actual needs of the tool to accomplish its task. To do this, lawyers must have a basic understanding of what the AI tool is doing and what types of information are necessary. For example, an AI tool designed to predict litigation results at various stages of a dispute has little need for the social security numbers of each party to the disputes that it analyzes.

Another way to minimize the risk that AI tools can pose to client confidentiality is by contemplating the deliverable or end product given to the client. For example, if each client is given access to not only the AI tool but also the underlying training data, there is a much higher risk that confidential information will be learned about other clients. This risk is reduced by providing only the output generated by the AI tool instead of all the input data.[50] Regardless of what the deliverables look like, the form of deliverable is important to discuss at the time that the lawyer obtains informed consent.

Third-Party Vendors and Confidentiality

Now consider one more scenario. Assume that Wigmore decides not to make the tool in-house. Not all firms have an analytics department, or the capacity or the desire to produce complex models. Lawyers may seek to contract out the development of an AI tool to an independent developer, or they may seek to purchase and use commercially available AI tools.[51] When hiring an outside expert or vendor, the attorney retains responsibility for the work.[52] If Wigmore uses a third-party service provider to develop its tool, the firm's duty to supervise nonlawyers is implicated.[53] When a third-party is used to create an AI tool, or when a third-party cloud provider is used to store data used to develop an AI tool, lawyers must take steps to fulfill their duties of confidentiality to their clients.

When a lawyer uses a third-party to incorporate AI into her practice, either through contracting for the development of a proprietary tool or by purchasing a commercially available tool, additional confidentiality risks arise when working with the third-party. It is imperative that the lawyer remember that ethical obligations do not change because she is working with a third-party and consider how those obligations impact the particular situation.

As an example, the rise of cloud computing, and its subsequent treatment by the legal community, provides a template for how lawyers should approach situations where confidential information will be shared with third-party technology providers. Storing client information in the cloud presents potential confidentiality issues because it requires a lawyer to place confidential information in the possession of a third-party: the cloud storage provider.[54] Despite this, states

have routinely held that lawyers may use online storage for confidential client information as long as they take reasonable care to ensure that confidentiality will be maintained.[55]

Taking reasonable care that confidentiality will be maintained in these situations includes: ensuring that the third-party provider has an enforceable obligation to preserve confidentiality and security and that the provider will notify the attorney if the disclosure of client information is ever required; investigating the provider's security measures, policies, and recovery methods to ensure that they are adequate under the circumstances; employing technology to guard against reasonably foreseeable attempts to access the client's data without authorization, and; investigating the storage provider's ability to purge and wipe the client's data.[56]

These same guidelines can be applied in the context of dealing with third parties to incorporate AI tools into a legal practice. First, in many of the situations in which a third-party is involved in the development of an AI tool, cloud computing and storage will be directly involved, either because it will involve a commercially available AI tool that is cloud-based, or because the third-party who was contracted to develop a proprietary tool will take advantage of the benefits of cloud storage.[57]

Second, even if cloud storage is not directly involved, the principles set forth in opinions dealing with the confidentiality concerns of cloud computing apply when developing AI tools. In both scenarios, there is a legitimate risk that client information may be disclosed because of the use of an emerging branch of technology. Further, the same measures described in the various opinions on cloud storage[58] will likewise help to minimize the confidentiality risks of involving third parties in the context of AI tool development.

Therefore, whenever a third-party or third-party tool is used to develop an AI tool, the lawyer should ensure that the third-party has an enforceable obligation to protect the confidentiality and security of the client's information. This agreement should include language that limits the third-party's use of the client information exclusively to the purpose that was agreed to by the client. The agreement should also require that the third-party take adequate precautions to ensure the safety of the data from theft.

As in the case of cloud computing, the lawyer has an obligation to investigate and determine the adequacy of the precautions, safety measures, and policies of a third-party AI developer or service. In conducting these investigations, if the lawyer lacks sufficient understanding of the technology, the lawyer should seek the advice of technologists, data scientists, or others with an understanding sufficient to enable the lawyer to ensure the safety of the client's data.[59] Relying on the advice of experts to explain the workings of the particular technology under consideration should help the lawyer in taking "reasonable care" to safeguard the client's information.[60]

Conflicts of Interest

The Wigmore firm must also consider possible conflicts of interest between clients X, Y, and Z, or any combination of current or former clients' interests, or the interests of the law firm in building

and marketing the tool. Will the tool be used for the benefit of future clients of the firm?[61] If so, then Wigmore's duties to former clients pose an ethical dilemma.[62] Would it be appropriate to use confidential data from client X or Y to develop a tool that Wigmore would then use to help Company Z?

There are many scenarios that could create a conflict of interest in the development of data analytic tools to be used by the firm for multiple clients.[63] Resolution of the conflict of interest issues under Model Rules 1.7 and 1.9 require a careful analysis of the facts and, again, possibly informed consent and a waiver. Knowing that those risks are present and seeking guidance in resolution of those risks before using client data to benefit one client or the firm can help Wigmore steer clear of ethics issues.

Conclusion

The increasing prevalence of AI technologies is an exciting development for lawyers. AI holds the promise to help lawyers and other legal-services professionals to improve their services to clients and find new ways to deliver value for clients and society. However, like all new things, technology presents certain risks that lawyers must understand in order to utilize it and fulfill their ethical obligations to clients. While the law regarding lawyers' ethical obligations in the context of AI continues to develop, the Rules of Professional Conduct, Ethics Opinions, and related laws provide guidance for lawyers incorporating AI into their practices.

Endnotes

1. We use "AI" to refer broadly to various forms of artificial intelligence tools and the use of data analytics. The specific analyses that follow may differ, for example, when using deep learning versus traditional linear regression. But given our focus on the use of client data and lawyer confidentiality obligations, we aim to identify generally applicable principles without parsing the nuances of potential risks and benefits of the specific types of tools lawyers and technologists create and use. These are discussions that lawyers and technologists should have with their clients and customers.

2. Justine Rogers & Felicity Bell, *The Ethical AI Lawyer: What is Required of Lawyers When They Use Automated Systems?*, 1 Law, Tech. & Humans 80 (2019), *available at* https://lthj.qut.edu.au/article/view/1324/843.

3. *Thomson Reuters Report Highlights Legal Departments' View of Technology*, Artificial Intelligence (Oct. 3, 2017), *available at* https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-report-highlights-legal-departments-view-of-technology-artificial-intelligence.html.

4. Roy D. Simon, *Artificial Intelligence, Real Ethics*, New York State Bar Association Journal (Apr. 2018), *available at* https://www.nysba.org/Journal/2018/Apr/Artificial_Intelligence,_Real_Ethics/.

5. W. Bradley Wendel, *The Promise and Limitations of Artificial Intelligence in the Practice of Law,* 72 Okla. L. Rev. 21 (2019).

6. For a broad overview of AI and Ethics, *see* Drew Simshaw, *Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using Artificial Intelligence in the Practice of Law*, 70 Hastings L.J. 173 (2018); Eduard Fosch Villaronga, Peter Kieseberg & Tiffany Li, *Humans forget, machines remember: Artificial intelligence and the right to be forgotten*, 34 Comp. L. & Sec. Rev. 304 (2018); David Lat, *The Ethical Implications of Artificial Intelligence*, Above the Law, https://abovethelaw.com/law2020/the-ethical-implications-of-artificial-intelligence/ (last visited Aug. 26, 2020); Ed Walters, *The Model Rules of Autonomous Conduct: Ethical Responsibilities of Lawyers and Artificial Intelligence*, 35 Ga. St. U.L. Rev. 1073 (2019); Katherine Medianik, *Comment: Artificially Intelligent Lawyers: Updating the Model Rules of Professional Conduct in Accordance with the New Technological Era*, 39 Cardozo L. Rev. 1497 (2018).

7. Model Rules of Prof'l Conduct R. 5.3 (2016) [hereinafter MODEL RULES].

8. Model Rules R. 5.4 - 5.5.

9. Data points might include things that are clearly relevant to the facts of each case, such as (1) whether the case involved residential or commercial tenants; (2) the reason for the lawsuit (nonpayment of rent, breach of lease, holding over); (3) the amount of damages requested by Company X; and (4) the court type (landlord-tenant, county, state, federal district), the specific court, the jurisdiction, and judge. In addition, leases, court documents and Company X's own records would hold significant other information with less obvious significance, such as (5) the age, gender and nationality of the tenant; (6) the type of business involved in a commercial case; (7) the size of the space being leased; (8) the annual rent collected under the lease; (8) the number, if any, of missed payments; (9) the solvency of the business or individual at the time of the dispute; (9) the duration of the lease; (10) the firm and specific lawyers representing the counterparty, and so on.

10. Model Rules R. 1.1.

11. State Bar of Cal., Formal Op. 2015-193 (2015).

12. Model Rules R. 1.1 cmt. 8. Many ethics opinions speak to the lawyer's obligations to protect the confidentiality of client data and what to do in the event of a breach. *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018); State Bar of Cal., Formal Op. 2010-179 (2010); Ill. State Bar Ass'n, Advisory Op. 16-06 (2016).

13. For some resources on e-discovery, see Maura R. Grossman & Gordon Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective And More Efficient Than Exhaustive Manual Review,* XVII Rich. J.L. & Tech 11 (2011)https://www.natlawreview.com/article/everything-you-need-

to-know-about-e-discovery; Harry Surden, *Machine Learning and Law*, 89 Wash. L. Rev. (2014); Tom O'Connor, *Will Lawyers Ever Embrace Technology in eDiscovery*, New Orleans Bar Association (Feb. 13, 2019), https://www.neworleansbar.org/news/committees/will-lawyers-ever-embrace-technology-in-ediscovery.

14. *See* Anthony Davis & Steven M. Puiszis, *An Update of Lawyers' Duty of Technological Competence: Part 2*, 261 N.Y.L.J. No. 86, at 3 (2019). Lawyers can be sanctioned for failing to comply with the duty of technological competence *See, e.g.*, State ex rel. Oklahoma Bar Ass'n v. Oliver, 369 P.3d 1074 (2016); *In re* Goudge (Ill. 2013), reprimand, *available at* http://www.iardc.org/HB_RB_Disp_Html.asp?id=10819.

15. Katy Ho, *Defining the Contours of an Ethical Duty of Technological Competence*, 30 Geo. J. Legal Ethics 853, 864 (2017).

16. *See* Dan Linna, *Evaluating Legal Services: The Need for a Quality Movement and Standard Measures of Quality and Value – Chapter in Research Handbook on Big Data Law* (Mar. 12, 2020), https://www.legaltechlever.com/2020/03/evaluating-legal-services-the-need-for-a-quality-movement-and-standard-measures-of-quality-and-value-chapter-in-research-handbook-on-big-data-law/.

17. *See* Susan N. Mart, *The Algorithm as a Human Artifact: Implications for Legal [Re]Search*, 109 Law Libr. J. 387 (2017), *available at* https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=1997&context=articles.

18. *Id.*; *see also* A.B.A. Resolution 112 re Artificial Intelligence (Aug. 12, 2019), *available at* https://www.americanbar.org/content/dam/aba/images/news/2019/08/am-hod-resolutions/112.pdf.

19. Jamie Baker, *Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society*, 69 S.C. L. Rev. (2018), *available at* https://ssrn.com/abstract=3097250. *See also* State of Wisconsin v. Loomis, 881 N.W. 2d 749 (Wis. 2016); Sean La Roque-Doherty, *Not all litigation analytics products are created equal*, A.B.A. J. (Aug. 1, 2020) (discussing differences in data available from various litigation analytics products).

20. See Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan & Cass R. Sunstein, *Discrimination in the Age of Algorithms*, 10 J. Legal Analysis 113 (2019), *available at* https://doi.org/10.1093/jla/laz001.

21. Model Rules R. 1.4.

22. Model Rules R. 1.4(a) (A lawyer shall: (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules."); *See also* cmts. 1, 2 & 5.

23. Charles J. Northrup, *Inform Yourself about Informed Consent*, 105 Ill. B.J. at 52 (Oct. 2017), https://www.isba.org/ibj/2017/10/informyourselfaboutinformedconsent.

24. Model Rules R. 1.0 cmt. [6].

25. Model Rules R. 1.4(b) ("A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."); *See also* cmt. 5.

26. *In re* Ingersoll, 186 Ill. 2d 163 (1999).

27. Model Rules R. 1.15 cmt. 1. *See also, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018); State Bar of Ariz., Advisory Op. 07-02 (2007); D.C. Bar Op. 357 (2010).

28. *Id.*

29. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 at 7.

30. *Id.* at 12

31. *See* State Bar of Ariz., Advisory Op. 07-02 (2007); D.C. Bar Ethics Op. 357 (2010).

32. Model Rules R. 1.6(a) & (c).

33. Anthony E. Davis, *The Ethical Obligation to be Technologically Competent* (Jan. 8, 2018, 3:00 AM), https://www.law.com/newyorklawjournal/almID/1202746527203/The-Ethical-Obligation-To-Be-Technologically-Competent/?mcode=0&curindex=0&curpage=2.

34. Model Rules R. 1.6(a) ("a lawyer shall not reveal information relating to the representation of the client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).").

35. *See id.*

36. *Id.*; *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Ops. 480, 481 & 483.

37. *See* Model Rules R. 1.6(b)(1)-(7).

38. For example, the Model Rules of Prof'l Conduct state that lawyers can disclose client information when the disclosure is "impliedly authorized in order to carry out the representation" of the client. *Id.*

39. Model Rules R. 1.0(e) cmt. [6].

40. Christine Simmons, Xiumei Dong & Ben Hancock, *More Than 100 Law Firms Have Reported Data Breaches. And the Problem is Getting Worse,* Law.com (Oct. 15, 2019), https://www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-

picture-is-getting-worse/; *see also* John G. Loughnane, *2019 Cybersecurity*, A.B.A. (Oct. 16, 2019), https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity201

41. *Id.*

42. *See, e.g.*, Daniel Faggella, *AI in Law and Legal Practice – A Comprehensive View of 35 Current Applications*, EMERJ (Mar. 14, 2020), https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/; *see also* Roy Strom, *Ogletree Deakins Partners With AI Company to Build Better Data*, Law.com (Jan. 9, 2019), https://www.law.com/dailyreportonline/2019/01/09/ogletree-deakins-partners-with-ai-company-to-build-better-data/.

43. *Id.*

44. Model Rules R. 1.6(a) & 1.0 cmt. [7].

45. Model Rules R. 1.6(c); *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018).

46. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018).

47. *See* Harry Surden, Essay, *Machine Learning and Law*, 89 Wash. L. Rev. **87**, 100 (2014).

48. Some research has suggested that, in some circumstances, the possibility exists for an AI tool to be reverse-engineered in ways that could allow a person to obtain information about the tool's underlying set of training data. *See, e.g.*, Nicolas Papernot et al., *Semi-Supervised Knowledge Transfer for Deep Learning from Private Training Data* (2017) https://arxiv.org/pdf/1610.05755.pdf; Reza Shokri et al., *Membership Inference Attacks Against Machine Learning Models*, https://www.cs.cornell.edu/~shmat/shmat_oak17.pdf. The extent to which this is possible, and at what point it would trigger additional confidentiality concerns, requires a thorough understanding of the methods and specific data used, which is outside the scope of this article.

49. For example, the exceptions to the confidentiality rule for preventing death or bodily harm only permit a lawyer to disclose information *to the extent necessary* to prevent such harm. Model Rules R. 1.6(b)(1).

50. As discussed in note 49, it might be possible to reverse engineer a system to learn about the training data. But even if the underlying training data from prior client is not exposed in any way to the latter client using the tool, the latter client benefits from the use of the prior client's data in the process of creating the AI tool.

51. For example, lawyers can purchase commercially available software that allows them to use AI to analyze contracts or predict an opposing litigant's argument based on an analysis of briefs previously filed by the opposing counsel. *See, e.g.*, Kira Inc., https://kirasystems.com/how-it-

works/contract-analysis/ (last visited Feb. 7, 2020); CASETEXT, INC., https://casetext.com/ (last visited Feb. 7, 2020).

52. MODEL RULES R. 5.3 cmt. 3 ("A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. . . . When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. . . . When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.").

53. *Id.*

54. *See, e.g.*, Davis & Puiszis, *supra* note 14; Stuart Pardau & Blake Edwards, *The Ethical Implications of Cloud Computing for Lawyers*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 71, note 10 (2014); Ill. State Bar Ass'n, Advisory Op. 16-06 (2016). In addition, storing information on the lawyer's computers also creates risks, such as the risk of a data breach discussed above. Also consider that many lawyers may not be aware that they use the cloud indirectly, such as in connection with their email or email-security service. The cloud is ubiquitous and difficult to avoid. Moreover, many cloud solutions may in fact be more secure than what most law firms could offer. These are important questions to discuss with clients, and some clients will clearly dictate their preferences, particularly sophisticated clients.

55. *See, e.g.* Alaska Bar Ass'n, Op. 2014-3 (2014); State Bar of Ariz., Advisory Op. 09-04 (2009); State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010); State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2012-184 (2012); Fla. Bar, Advisory Op. 12-3 (2013); Ill. State Bar Ass'n, Advisory Opinion 16-06 (2016); Iowa State Bar Ass'n Comm. on Ethics & Practice Guidelines, Op. 11-01 (2011); Me. Bd. Overseers of the Bar Prof'l Ethics Comm'n, Op. 194 (2008); Me. Bd. Overseers of the Bar Prof'l Ethics Comm'n, Op. 207 (2013), Mass. Bar Ass'n, Op. 12-03 (2012), N.H. Bar Ass'n, Advisory Op. 2012-13/04 (2012); N.J. Advisory Comm. on Prof'l Ethics, Op. 701 (2006); State Bar of Nev., Formal Op. 33 (2006); N.C. State Bar, Formal Op. 6 (2011); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010); Or. State Bar, Formal Op. 2011-188 (2011); Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility & Philadelphia Bar Ass'n Prof'l Guidance Comm., Joint Formal Op. 2011-200 (2011); Bd. of Prof'l Responsibility of Sup. Ct. of Tenn., Formal Opinion 2015-F-159 (2015); Vt. Bar Ass'n, Advisory Op. 2010-6 (2010); Va. State Bar, Legal Ethics Opinion 1872 (2019); Wash. State Bar Ass'n, Advisory Op. 2215 (2012); Wis. Formal Ethics Opinion EF-15-01 (2017).

56. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010).

57. Some AI tools do offer on premises installation on a law firms' computers.

58. Formal Op. 477R (2017); Ill. State Bar Ass'n, Advisory Op. 16-06 (2016); Ala. State Bar, Op. 2010-2 (2010); State Bar of Ariz., Advisory Op. 09-04 (2009); Iowa State Bar Ass'n Comm. on Ethics & Practice Guidelines, Op. 11-01 (2011); State Bar of Nev., Formal Op. 33 (2006); Bd. of Prof'l Responsibility of Sup. Ct. of Tenn., Formal Opinion 2015-F-159 (2015); Wash. State Bar Ass'n, Advisory Op. 2215 (2012).

59. While lawyers will typically not be required to have the same level of expertise in these technologies as the specialists that they rely on, they should "stay abreast of technological advances and the potential risks" that they pose. Model Rules R. 1.1, cmt. 8.

60. The ABA has indicated that reliance on the technical advice of cyber experts is appropriate when analyzing the security of communicating client information over the internet and the same logic would apply here. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.").

61. Model Rules R. 1.7 - 1.9.

62. Model Rules R. 1.9(c) ("A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter: (1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.").

63. Model Rules R. 1.8(b) ("A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these rules.").

ENTITY:

CENTER FOR PROFESSIONAL RESPONSIBILITY

TOPIC:

ETHICS

Authors

By Daniel W. Linna Jr. & Wendy J. Muchman

Daniel W. Linna Jr., Director of Law and Technology Initiatives & Senior Lecturer, Northwestern Pritzker School of Law & McCormick School of Engineering; Wendy Muchman, Professor of Practice, Harry B. Reese Teaching Professor 2020-2021, Northwestern Pritzker School of Law. Professors Linna and Muchman wish to acknowledge the hard work of Maveric Searle and Abigail Sexton (Northwestern Law JD 2020) without whose assistance this paper would not have been possible. In addition, thank you to Liuzhuoyi Liu (Northwestern Law JD 2021) and David Skoler (Northwestern JD/MBA 2022) for their expert editing skills.