SQUIRE PATTON BOGGS

Santa Ethics

Audience Handouts

November 28, 2023

Ken Moore (Kenneth.Moore@squirepb.com)
Steve Delchin (Steven.Delchin@squirepb.com)

I. Overview of How AI is Being Used In The Practice of Law.

A. Electronic discovery.

1. Today's e-discovery tools use a method of predictive coding to classify documents as relevant or irrelevant, among other classifications.

2. Studies show that the AI tools are just as accurate as humans—if not more accurate.

B. Preparing first drafts of discovery responses.

1. AI companies are designing AI tools specifically designed to evaluate discovery requests and produce first drafts of discovery responses.

2. These tools can save time and money and reduce administrative burden.

C. Legal research.

1. AI is revamping the way that lawyers conduct legal research.

2. AI can use machine learning to detect similarities and differences among legal authorities.

3. AI also helps keep attorneys up to date on developments in the law that could impact their matters.

4. AI-assisted research tools ultimately allow lawyers to learn the law faster, easier, and more accurately.

D. Litigation analysis.

1. There is an amazing amount of data in the U.S. court system's public records.

2. AI tools can analyze vast amounts of historical legal data, including case outcomes, judges' rulings, and legal precedents, to provide predictive insights.

3. AI can compare the facts of your case to other cases already decided by a court (or courts) to give you a prediction of how your case will fare.

4. AI provides much-needed analytics behind what traditionally has been a gut call by lawyers.

E. Contract management.

1. AI-driven contract management tools are valuable to lawyers, especially inside counsel, who quickly need to identify important information in contracts.

2. AI tools can flag termination dates and alert the lawyer about deadlines for sending a notice of renewal.

3. The AI tools also can identify important provisions in contracts, such as indemnification obligations and choice of law provisions, among others.

F. Detecting wrongdoing.

1. AI is being used to detect wrongdoing within an organization.

2. It is possible to utilize AI to search company records, such as emails, to detect bad behavior before it can bubble to the surface.

3. AI is being used to sniff out bribery, fraud, compliance issues, even potential litigation – all based on the content of the company's own documents and data.

4. AI can summarize conversations and the ideas discussed, identify code words, note the frequency of the communications, and even identify the mood of the speakers.

G. Legal spend analysis.

1. AI is being used by in-house law departments for legal spend analysis.

2. The AI provides the capability to:

a. analyze what work was done by a firm,

b. how it aligns with other work done by a firm,

c. how the work and efficiency compares with work provided by other firms engaged by the company or organization, and

d. how the work and efficiency compares to the market generally.

II. Overview of Ethical Obligations in Using AI in the Practice of Law.

A. Duty of competence.

1. One of the basic duties that lawyers owe to their clients is the duty of competence, which is embodied in Rule 1.1 of the ABA Model Rules of Professional Conduct.

    a. Under ABA Model Rule 1.1, a lawyer must provide competent representation to his or her client.

    b. Rule 1.1 states that "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

2. The duty of competence also includes the duty of *technological* competence.

    a. Comment 8 to Rule 1.1 makes clear that the duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."

3. Lawyers and their staff must have a general understanding of the technology that is available to serve clients.

    a. This includes understanding the risks and benefits of technology relevant to one's practice.

    b. AI is becomingly increasingly mainstream, so the duty of competence increasingly will include understanding the capabilities and potential drawbacks of using AI.

    c. This does not mean that lawyers are expected to know all the technical intricacies of AI systems, but a lawyer's duty of competence does include having a basic understanding of how AI technology produces results.

B. Duty of supervision.

1. Lawyers also have a continuing duty to maintain controls and oversight of AI, including AI vendors.

2. Under ABA Model Rules 5.1 and 5.3, lawyers have an ethical obligation to supervise nonlawyers who are assisting them in the provision of legal services to ensure that their conduct complies with the Rules of Professional Conduct.

    a. As the Comments to Rule 5.3 make clear, the duty of supervision encompasses nonlawyers, not only within the law firm, but also outside the law firm, including, as an example, hiring a document management company to create and maintain a database for complex litigation.

3. Thus, just as lawyers are required to supervise the work of their paralegals, secretaries, and other staff members, lawyers must maintain oversight of AI vendors and the AI used in client matters to ensure compliance with the ethics rules.

    a. Lawyers, for example, must supervise the inputs that go into AI and take responsibility for the outputs that are generated.

    b. Again, this does not mean that lawyers need to become computer programmers, but they do need to be educated on how AI technology works.

C. Duty of confidentiality.

1. ABA Model Rule 1.6 requires that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

2. The use of some AI tools may require client confidences to be shared with third-party vendors; thus, lawyers must take appropriate steps to ensure that their clients' information appropriately is safeguarded.

3. A lawyer should communicate with third-party providers about confidentiality concerns such as:

    a. the type of confidential client information provided,

    b. how the information will be stored,

    c. who or what has access to the information, and

    d. what safeguards the third-party provider has in place to preserve confidentiality.

4. The bottom line is that AI should not be used unless the lawyer is reasonably confident that the client's confidential information will be secure.

D. Duty of communication.

1. Lawyers have an ethical duty of communication, which is embodied in ABA Model Rule 1.4.

2. Rule 1.4 requires a lawyer "to reasonably consult with the client about the means by which the client's objectives are to be accomplished."

3. Rule 1.4 also requires a lawyer to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

    a. Reasonableness under Model Rule 1.4 may be measured by the standard of competent representation under ABA Model Rule 1.1, which includes the duty of technological competence.

4. If a lawyer intends to use AI in providing legal services to clients, the lawyer may have an obligation under Rule 1.4 to discuss that decision with clients.

a. The discussion should include the risks of AI.

b. The client should also be informed about the potential limitations of AI.

5. Furthermore, if a lawyer chooses not to use AI tools in a manner where it may be beneficial to the client to do so, the lawyer may arguably have an obligation under the duty of communication to discuss that with the client as well.

a. This is especially true if not using the technology will increase the costs to the client.

b. As AI becomes more mainstream, more and more clients will expect their lawyers to use AI, so communication with the client may increasingly be necessary to explain why efficient AI tools are not being used for a particular client matter.

E. Reasonableness of Fees.

1. ABA Model Rule 1.5 prohibits a lawyer from charging or collecting unreasonable fees or unreasonable amounts for expenses.

2. If using AI can significantly reduce the time it takes to perform legal services, then failing to use the technology may result in charging the client an unreasonable fee in violation of Rule 1.5.

3. And of course, the failure to use AI technology also could run afoul of the duty of competence under Rule 1.1.

a. This is not to say that an attorney should substitute AI for his or her own judgment.

b. Rather, the lawyer should consider AI as a way to potentially reduce legal spend with the client's approval.

4. In-house lawyers at major companies have already begun using cost-saving AI tools.

a. One major company's legal department implemented an AI-based contract drafting tool that has reduced the drafting time on some matters from 10 hours to about 15 minutes.

b. One major bank implemented an AI tool that reviews commercial loan agreements, saving an estimated 360,000 hours of manual work by lawyers and loan officers each year.

c. Other companies have taken different approaches:

i. Some have expressly banned the use of their data going into an AI program.

ii. Others require outside counsel to obtain written consent prior to using AI.

5. Using AI as a cost-saving measure may become the expected norm in the legal world.

    a. One Canadian judge held that costs and fees can be excessive if attorneys fail to use AI tools.

    b. In examining the reasonableness of legal research fees sought to be recovered by defendant's counsel, the judge observed that "if artificial intelligence sources were employed, no doubt counsel's preparation time would have been significantly reduced." *Cass v. 1410088 Ontario Inc.*, 2018 ONSC 6959.

III. Ethical Issues in the Use of Generative AI in the Practice of Law.

A. Generative AI is an advanced AI tool that can produce human-like responses to questions posed by users.

1. Generative AI tools have dominated the news headlines recently.

2. Examples include ChatGPT and Google Bard.

B. The use of generative AI in the practice of law raises several ethical issues.

1. Using generative AI tools could violate a lawyer's duty of confidentiality under ABA Model Rule 1.6.

a. To use a generative AI tool, a user must input data to generate a response, but it is not clear that the inputted data remains confidential.

b. ChatGPT, for example, has expressly warned that user input may be reviewed by AI trainers to improve the system.

c. More generally, AI tools like ChatGPT may add information inputted by users to their collective data sets to improve their AI systems and even may share that inputted data with allied partners.

d. What this means is that lawyers who input confidential client information into a generative AI tool risk breaching their ethical duty of confidentiality.

e. Lawyers also potentially risk waiving the attorney-client privilege.

2. The problem of AI hallucination is another ethical issue raised by generative AI.

a. AI hallucinations occur when AI tools such as ChatGPT fabricate information, but confidently behave as if they are spouting true facts.

b. It has been well-documented that AI tools sometimes present facts in a misleading way or even present "facts" that are fabricated, such as made-up court cases, holdings, and legal concepts.

c. AI tools are only as good as the information they are trained on, and the information is not always correct.

d. What this means is that using ChatGPT or similar AI in the practice of law may lead to false or misleading advice and work product.

e. Earlier in 2023, a New York lawyer found himself in hot water for filing a brief that contained case citations generated by ChatGPT that were made up.

i. Six of the cases that the lawyer cited were "bogus judicial decisions with bogus quotes and bogus internal citations"—a circumstance that the judge in that case called "unprecedented."

ii. The New York lawyer at issue claimed that ChatGPT not only provided the legal sources, but also assured him of the reliability of the opinions and citations.

iii. The New York lawyer alleged that he falsely assumed ChatGPT was "a super search engine" and had no idea that it could fabricate cases and knowledge.

iv. The judge imposed joint and several sanctions of $5,000 on the lawyers involved (one who wrote the motion, and the other, his partner, whose name was on it). *See Mata v. Avianca, Inc*., Case No. 1:2022cv01461 (S.D.N.Y. 2023).

3. The problem of bias in the use of generative AI is another well-documented problem that raises significant ethical concerns.

a. A known problem with ChatGPT and all machine learning models is that the information and past transactions used to train AI systems may introduce racial, economic, or sexual bias in the AI system's output.

i. Even a carefully created AI system can reflect the biases and prejudices of its developers and/or the information that is inputted.

ii. For example, ChatGPT is trained on 300 billion words, or 570 GB of data—all sources of data scraped from the Internet that could be biased.

b. Bias associated with the use of AI has ethical implications for lawyers.

i. ABA Model Rule 8.4(g) prohibits harassment and discrimination by lawyers against eleven protected classes.

ii. Rule 8.4(g) states that it is professional misconduct for a lawyer to "engage in conduct that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, marital status or socioeconomic status in conduct related to the practice of law."

iii. About 20 states have adopted some variation of ABA Model Rule 8.4.

iv. If a lawyer's use of ChatGPT leads to discriminatory outputs, or involves biased inputs, even unknowingly, the lawyer not only risks violating his or her duty of competence, but also unwittingly may violate applicable ethical rules prohibiting discrimination.

v. The ABA has urged courts and lawyers to address the emerging ethical and legal issues related to the usage of AI

in the practice of law, including (1) bias, explainability, and transparency of automated decisions made by AI, (2) ethical and beneficial usage of AI, and (3) controls and oversight of AI and the vendors that provide AI. *See* Resolution No. 112 of the American Bar Association House of Delegates adopted August 12-13, 2019.

IV. Preventing or Minimizing Bias in the Use of AI in the Practice of Law.

A. To comply with their ethical obligations while avoiding bias, lawyers should embrace AI technology that can explain its decision-making process in understandable terms.

B. Lawyers need AI systems that work as expected and produce transparent explanations for the decisions that they make.

C. Lawyers, in particular, should be cautious about using "black box" AI that cannot explain how an output was generated based on the input.

1. How AI produces results can be quite an enigma.

2. This is because many AI tools, like ChatGPT, are "black box" models that arrive at conclusions or decisions without providing any explanation on how they were reached.

3. As one technical dictionary explains: "In black box models, deep networks of artificial neurons disperse data and decision-making across tens of thousands of neurons, resulting in a complexity that may be just as difficult to understand as that of the human brain. In short, the internal mechanisms and contributing factors of black box AI remain unknown." Yasar Kinza, Black Box AI, TechTarget, https://www.techtarget.com/whatis/definition/black-box-AI.

D. To prevent or minimize bias, lawyers should consider the following:

1. whether the AI tools were developed by diverse teams,

2. the nature of the data used to train the AI, including the volume, source, testing, and scientific acceptance of the data used,

3. whether the AI was tested for bias,

4. whether the AI is built with bias-detection systems, and

5. whether the decisions of the AI can be clearly traced or explained.

E. Real-life example of Amazon.

1. Several years ago, Amazon adopted an AI tool to automatically review job applicant resumes.
2. Amazon had to stop using the AI tool because it discovered that it was biased against women.

a. This happened because the AI tool had been trained to review potential job applicants by looking at patterns in resumes submitted in the past 10 years.

b. As it turned out, most of the resumes from the past 10 years were from men.

c. Thus, the AI tool learned that men were the desired job candidate.

F. Lawyers should strive to embrace AI technology that can explain its decision-making process in understandable terms—known as explainable AI.

1. With respect to black box AI tools such as ChatGPT, lawyers should be mindful of how outputs are generated and in which instances it is appropriate to make use of these outputs.

G. There is debate and discussion over whether AI tools can promote diversity, equity, and inclusion efforts.

1. Some supporters of AI tools argue that they can be used to circumnavigate the inherent bias and unpredictability of humans.

a. AI might be used to identify candidates from underrepresented groups without the limitations of human recruiting representatives.

b. AI also might be used to make language of job postings more inclusive.

i. For one company, AI analysis revealed that the phrase “prior experience” drew more male applicants, while the phrase “demonstrated ability” was more likely to attract female candidates.

c. AI is also relevant for current employees.

i. Law firms, for example, might use AI to evaluate compensation policies or to design targeted retention programs for diverse employees.

2. Lawyers, however, must be mindful that AI tools can be biased and therefore can undermine diversity, equity, and inclusion efforts.

H. Lawyers are responsible for the quality, accuracy, and absence of prohibited discrimination in their ultimate legal advice to clients and communications to courts and other third parties.

V. Overview of Ethics of Cloud Computing.

A. There is a clear consensus among ethics authorities: Lawyers may ethically use cloud computing to transmit, store, and process client confidential data from reasonably reliable cloud service providers if the lawyers exercise "reasonable care" to prevent unauthorized access to or disclosure of such data.

1. ABA Formal Opinion 477R summarizes a lawyer's duty of reasonable care as follows:

a. "[A] lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."

2. In addition to the ABA, about 30 states in the U.S. have issued ethics opinions addressing the ethics of cloud computing.

a. The opinions generally emphasize a reasonable care standard necessary for lawyers to use cloud services ethically.

B. What the "reasonable care" standard means in practice.

1. Reasonable care requires that lawyers have a basic understanding of the cloud technology they are using.

2. Lawyers also must continually monitor and reassess the protections of their cloud service provider as the technology evolves.

C. There are several practices that lawyers should follow to satisfy the reasonable care standard as it relates to cloud computing.

1. Ensure that the cloud service provider has an enforceable obligation to preserve confidentiality.

2. Ensure that the cloud provider employs available technology to guard against reasonably foreseeable attempts to infiltrate the stored data.

3. Gain a basic understanding of cloud computing technology in order to ensure that a client's data will be protected.

a. Attending a CLE program on cloud computing is one way to gain such knowledge.

D. A critical part of a lawyer's ethical duty when it comes to the use of cloud computing is ensuring the protection of a client's confidential information.

1. ABA Model Rule 1.6(c) specifically states "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

2. Comment 18 to ABA Model Rule 1.6 describes some of the factors to be considered in determining whether a lawyer made “reasonable efforts” to prevent disclosure.

    a. the sensitivity of the information,

    b. the likelihood of disclosure if additional safeguards are not employed,

    c. the cost of employing additional safeguards,

    d. the difficulty of implementing the safeguards, and

    e. the extent to which the safeguards adversely affect the lawyer’s ability to represent clients.

3. Lawyers should conduct due diligence of third-party cloud service providers to ensure that the providers are reputable and employ adequate safeguards to protect client confidential information. Below are some questions to ask:

    a. Is the cloud service provider a solid reputable company with a good operating record?

    b. In what country and state are the cloud services located and do business

    c. What does the end user’s licensing agreement contain?

    d. Is the third-party cloud service attempting to contract away potential liability?

    e. What is the cost of the service?

    f. In the event of a financial default, will the lawyer lose access to their client’s data?

    g. How would the lawyer terminate the relationship with the cloud service provider?

4. There are special considerations when lawyers are dealing with highly confidential or especially sensitive client confidential information.

    a. Several ethics opinions suggest that when especially sensitive client information is involved, a lawyer should consider whether to employ additional security measures, including encryption, or even deciding to not use cloud services at all.

        i. Some opinions suggest that lawyers must inform the client of the lawyer’s use of cloud computing and to obtain the client’s informed consent.

    b. ABA Formal Opinion 477R suggests that a lawyer must take extra precautions when sensitive client information is at issue.

i. “[A] lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by agreement with the client or by law, or when the nature of the information requires a higher degree of security.”

c. In some cases, the client information may be so sensitive that it may not be appropriate to use a cloud provider at all.

i. For example, Florida Ethics Opinion 12-3 states that “the lawyer should consider whether the lawyer should use the outside service provider . . . in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information.”

d. If the lawyer ultimately decides to use the cloud service provider, additional security steps should be considered.

i. One option is encrypting the sensitive information on premises before uploading it to the cloud provider.

(1). This can help ensure the security of the information if the cloud provider is somehow compromised or hacked.

(2). Only the lawyer will have access to the decryption keys.

ii. A further option is to encrypt the data encryption keys themselves.

iii. Regardless of the ultimate method used, the key takeaway is that lawyers may need to employ additional safeguards when the client information stored in the cloud is especially sensitive.

e. Ultimately, it is in a lawyer’s best interests to make sure that all proper procedures are in place to protect client confidential information.

VI. Duty to Protect Client Information Stored on a Lawyer's Smartphone.

A. Overview of Opinion 1240 from the New York State Bar Association Committee, dated April 11, 2022.

1. Opinion 1240 addresses the common problem of what lawyers should do when they download an app on their smartphone and the app asks for consent to access the phone's contacts (among other things).

    a. These contacts may include a lawyer's clients, including current, former, or prospective clients.

2. According to the New York State Bar Association Committee, there are circumstances where a lawyer giving access to such confidential contacts through an app could be an ethics violation.

3. The relevant rule analyzed by the New York opinion is New York Rule 1.6.

    a. New York Rule 1.6(a) states that confidential information "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

    b. New York Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), and 1.18(b)."

    c. Note that New York's version of Rule 1.6 is narrower than ABA Model Rule 1.6.

        i. Under the ABA Model Rule, the confidential client information that must be protected from disclosure extends to anything "relating to a representation." It is not limited to the three categories listed in New York Rule 1.6(a).

4. In Opinion 1240, the New York State Bar Association Committee reviewed several prior New York ethics opinions.

    a. The prior ethics opinions made clear that lawyers must exercise "reasonable care" to protect clients' confidential information.

    b. Exercising "reasonable care" includes doing so in the following situations:

        i. When carrying electronic devices containing confidential information across the border. *See* N.Y. City 2017-5 (2017).

        ii. When using an online storage provider to store clients' confidential information. *See* N.Y. State 842 (2010).

iii. When sending emails containing confidential information. *See* N.Y. State 709 (1998).

c. In Opinion 1240, the New York State Bar Association Committee referenced its prior ethics opinion from 2008, which addressed a lawyer's use of an email service provider that would scan emails for keywords and then send computer-generated ads targeted at the lawyer based on the words in the emails.

i. The Committee concluded that using such a service was permissible if under the email provider's privacy policies, no individuals other than e-mail senders and recipients read or had access to the emails, and no other individuals received targeted ads from the service provider.

d. In its new opinion, the New York State Bar Association Committee also addressed one of its prior ethics opinions from 2016, which is New York Opinion 1088.

i. This 2016 opinion addressed whether an attorney could disclose to a potential client the names of actual clients the attorney had represented in the same practice area.

ii. The answer depended on whether the names of current or past clients could be confidential information under Rule 1.6(a).

iii. It would clearly be a client confidence if the client asked to keep its name confidential.

iv. It also could be confidential if the fact of representation was not generally known and if disclosing the identity of the client and the fact of representation could be embarrassing or detrimental to the client.

v. New York Opinion 1088 from 2016 noted that the fact of representation is more likely to be embarrassing or detrimental where the representation involves or involved criminal law, bankruptcy, debt collection, or family law.

5. Turning back to smartphone contacts, the New York State Bar Association Committee pointed out that such contacts include both "directory information" and "non-directory information."

a. Directory information includes such things as email addresses, work or residence addresses, and phone numbers.

b. But smartphone contacts also may include non-directory information, such as birth dates or the lawyer's relationship to a contact.

c. The Bar Committee noted there are many reasons why apps seek both types of information.

i. A social media app may want this information to attract more users to its platform or to establish links between users.

ii. Apps that sell products or services may seek such access to promote more sales.

iii. Apps that espouse political or social beliefs may seek such access to disseminate their views.

iv. In short, there are many ways that a lawyer's contacts could be exploited by an app.

6. In its opinion, the New York State Bar Association Committee stated that to the extent that clients' names are confidential information, a lawyer must make reasonable efforts to prevent the unauthorized access of others to those names.

7. Thus, the Committee concluded that before an attorney grants access to the attorney's contacts, the attorney must determine whether any contact – even one – is confidential within the meaning of Rule 1.6(a).

   a. A contact could be confidential because it reflects the existence of a client-attorney relationship which the client requested not be disclosed or which, based upon the facts and circumstances, would likely be embarrassing or detrimental to the client if disclosed. N.Y. State 1088 (2016).

   b. The New York Committee identified several factors a lawyer should consider in determining whether any contacts are confidential.

      i. Whether the contact information identifies the smartphone owner as an attorney.

      ii. Whether the contact information identifies the attorney's area of practice (such as criminal law, bankruptcy law, debt collection law, or family law) – these are areas of law where a client is more likely to find that disclosure of a representation by a lawyer is embarrassing or detrimental.

      iii. Whether people included in the smartphone contacts are identified as clients, as friends, as something else, or as nothing at all.

      iv. Whether the contact information also includes email addresses, residential addresses, telephone numbers, names of family members or business associates, financial data, or other personal or non-public information that is not generally known.

8. Bottom line conclusion from the New York State Bar Association Committee:

   "If the contacts on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with an app, unless the attorney, after reasonable due diligence, including a review of the app's policies and stated practices to protect user information and

user privacy, concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent."

B. Practical takeaways from New York Opinion 1240.

1. Lawyers (or at least New York lawyers) should not grant consent to a smartphone app absent a name-by-name review of the phone's contacts to ensure nothing confidential is involved.

2. The best course of action may be simply to say "no" when an app asks for consent to access contact data that may include information about firm's clients.

3. It may also make sense to consult with your firm's or organization's IT department to determine whether and/or how data could be used by an app in question.

VII. The Ethics of Surreptitious Recordings.

A. A number of ethics authorities, including the ABA, have concluded that a lawyer's surreptitious recording of another does not by itself violate ethics rules if the recording does not violate the law of the jurisdiction in which the recording takes place.

B. To address the ethics of secret recordings, it is first necessary to look generally at federal and state law on secret recordings.

1. The majority of states are *one-party* consent states, which means:

a. To secretly record a phone call in these states, one party to the conversation must consent.

b. This means that if the person recording the conversation is a party to the conversation, they can record the conversation without the other party's knowledge.

c. Federal law also follows the one-party consent approach.

2. A minority of states—11 states—are *all-party* consent states.

a. This means that to record a conversation or phone call, all parties to the conversation must consent before the conversation can be recorded.

C. The ethics of secret recordings may turn on the federal or state laws that apply, and it is not always clear which law applies.

1. Even if you know what state or federal law applies, you still need to know what ethics law applies.

2. And the answer is not always clear.

D. If you look at the ABA Model Rules, you will not find any specific rule or Comment expressly addressing secret recordings by attorneys.

1. On their face, the ABA Model Rules of Professional Conduct, and indeed the ethics rules of all the states, do not explicitly prohibit surreptitious recordings of conversations by lawyers.

2. The rule most often associated with secret recordings is ABA Model Rule 8.4(c), which states it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation."

a. Twenty-two years ago, in Formal Opinion 01-422, the ABA concluded that "the mere act of secretly but lawfully recording a conversation inherently is not deceitful."

b. A number of states have reached a similar conclusion.

c. At least 21 states take the position that secret recordings are generally permitted because they are not inherently unethical.

i. Of those 21 states, sixteen state the reason they are specifically not unethical is because they are not inherently deceitful.

E. Ultimately, there is a lot of grey area when it comes to the ethics of secret recordings.

1. There are some states that permit lawyers to make secret recordings of a third party, but they expressly prohibit secret recordings if the conversation is with a client.

2. There also are over a dozen states that have not yet addressed whether secret recordings by lawyers are ethical or not, so it is not clear whether they would follow the majority approach.

3. Even states that generally allow surreptitious recordings by lawyers recognize that lawyers can be disciplined for conduct involving such recordings.

a. One Ohio ethics opinion recognizes that an attorney could be subject to professional discipline if the attorney:

i. Lied about the fact of making the secret recording.

ii. Used deceitful tactics to become a party to the conversation.

iii. Uses the recording to commit a crime or fraud.

iv. Uses the recording when it has no substantial purpose other than to embarrass, harass, delay, or burden a third person.

v. Uses the recording as a means of obtaining evidence in violation of a third person's rights.

F. Bottom line: Lawyers should consult with an ethics attorney or their law firm's general counsel before secretly recording a conversation with a client or opposing counsel or even a third party.

Local Connections.
Global Influence.

SQUIRE
PATTON BOGGS

squirepattonboggs.com