PROGRAM MATERIALS
Program #3053
March 26, 2020

Ethics Rules and Internet Law

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Internet legal ethics

Introduction

Internet use by attorneys is subject to traditional ethical rules

The Internet may be a source of just three transactions, namely publishing, broadcasting and telecommunications

Highlighted topics

1. Competitive keyword advertising

    Passive

    Active

2. Internet professional responsibility and client privacy

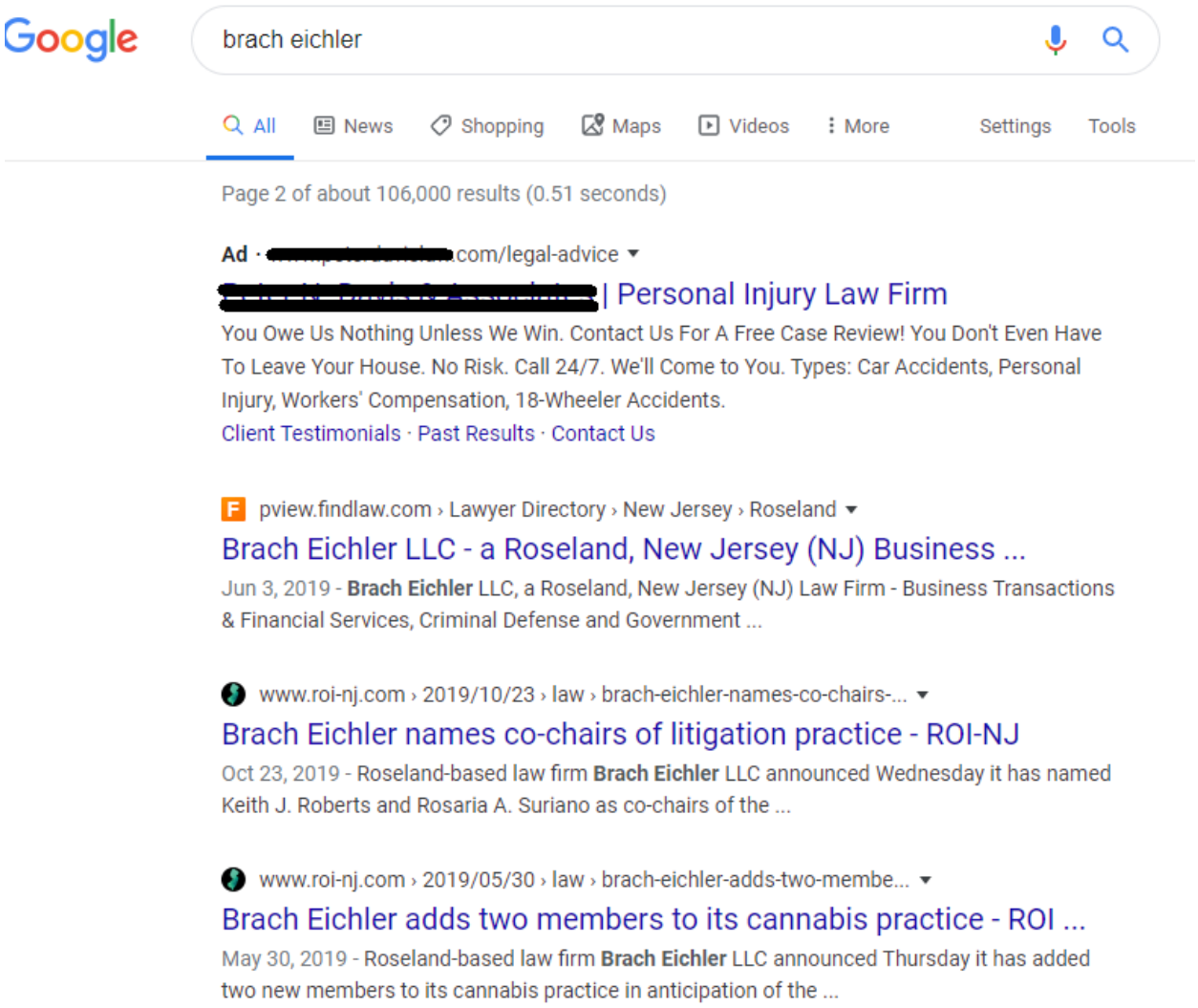
3. Using rules governing attorney ethics to protect Internet intellectual property

Passive competitive keyword advertising – description and benefit

Targeting competitor's keywords mean simply:

- Identifying and listing the names of your competitors who offer similar products and services;
- sending bids to the Internet sites which host their branded terms, and
- showcasing why your company is the better choice, by triggering your ads without displaying the name/brand in the ad copy, upon wining a bid.

For instance, upon conducting a branded search for Brach Eichler (your speaker Jonathan Bick's law firm) you can see that another law firm (whose name has been covered) has won the bidding on the Brach Eichler search term:



Passive competitive keyword advertising, also known as AdWords seems like a no-brainer. An easy way to redirect your competitor's traffic, leads, and sales.

Passive competitive keyword advertising – authorized in some jurisdiction and perhaps with limitations

North Carolina ethic opinions bans competitive keyword advertising.

Florida ethics opinion (2015) authorized competitive keyword advertising, then in 2017 implemented regulations to limit but not ban, competitive keyword advertising.

Texas Bar ethics opinion (2016) specifically authorized competitive keyword advertising by lawyers.

New Jersey ethics opinion (2017) specifically authorized competitive keyword advertising by lawyers.

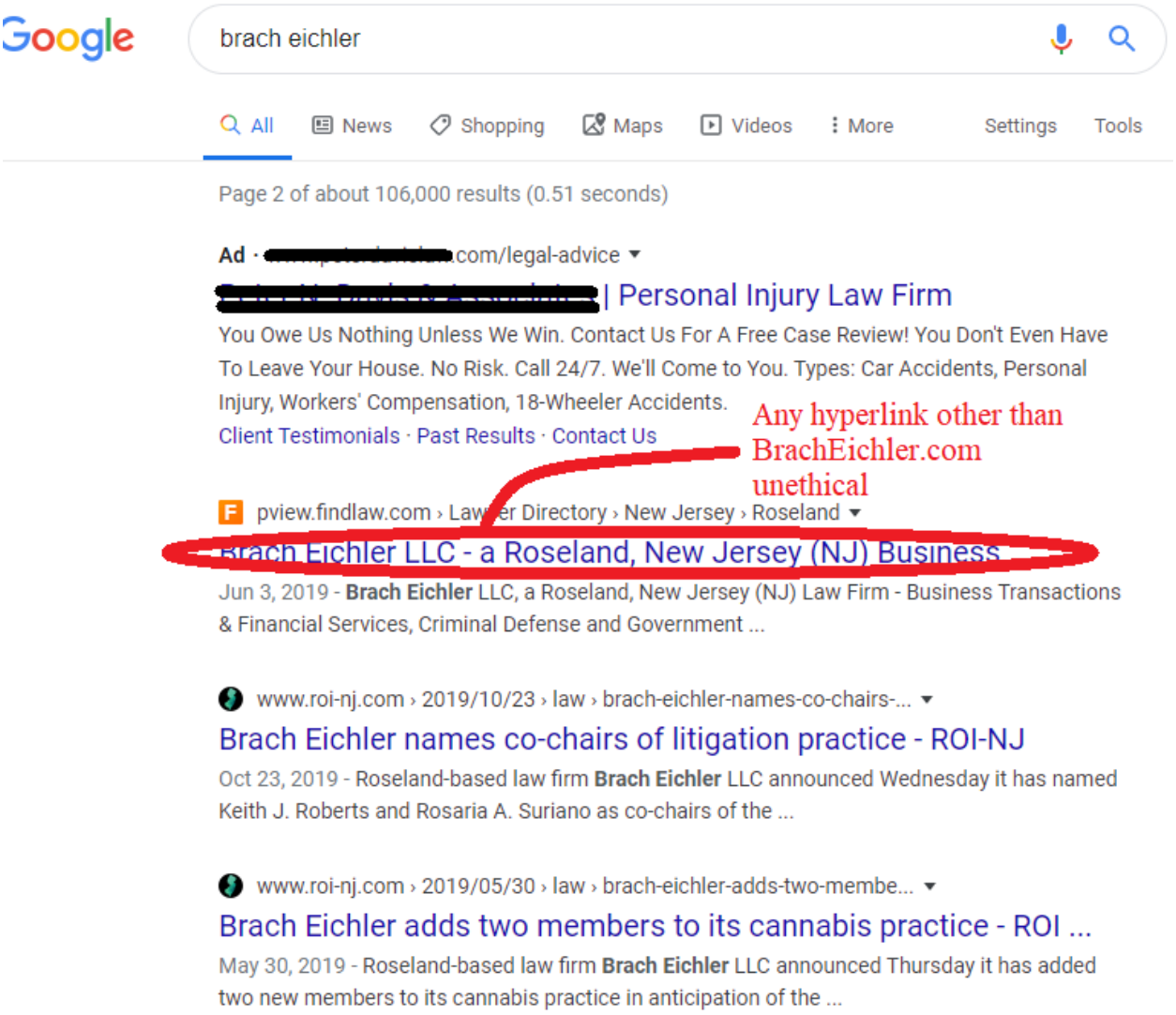
- it also endorses the Habush v. Cannon opinion from Wisconsin).

- In a brief opinion dated June 25, 2019 (ACPE #735), the NJ Advisory Committee on Professional Ethics explains why competitive keyword advertising doesn't violate MRPC Rules 7.1 (the purchased keywords do not constitute a "communication"), 1.4 or 8.4 (labeled keyword ads aren't deceptive, fraudulent, dishonest, egregious or flagrant).

Thus, for competitive keyword advertising jurisdictions an attorney may, consistent with the jurisdiction's rules governing attorney ethics, purchase an internet search engine advertising keyword that is a competitor lawyer's name, in order to display the lawyer's own law firm website in the search results when a person searches for the competitor lawyer by name

Active competitive keyword advertising – description

Active competitive keyword advertising consists of an attorney inserting or paying another, such as an internet search engine company or a hosting site to insert, a hyperlink on the name or website URL of a competitor lawyer that will divert the user from the searched-for website to the lawyer's own law firm website.



Inserting or paying an internet search engine company to insert, a hyperlink on the name or website URL of a competitor lawyer that will divert the user from the searched-for website to the lawyer's own law firm website is not passive competitive keyword advertising.

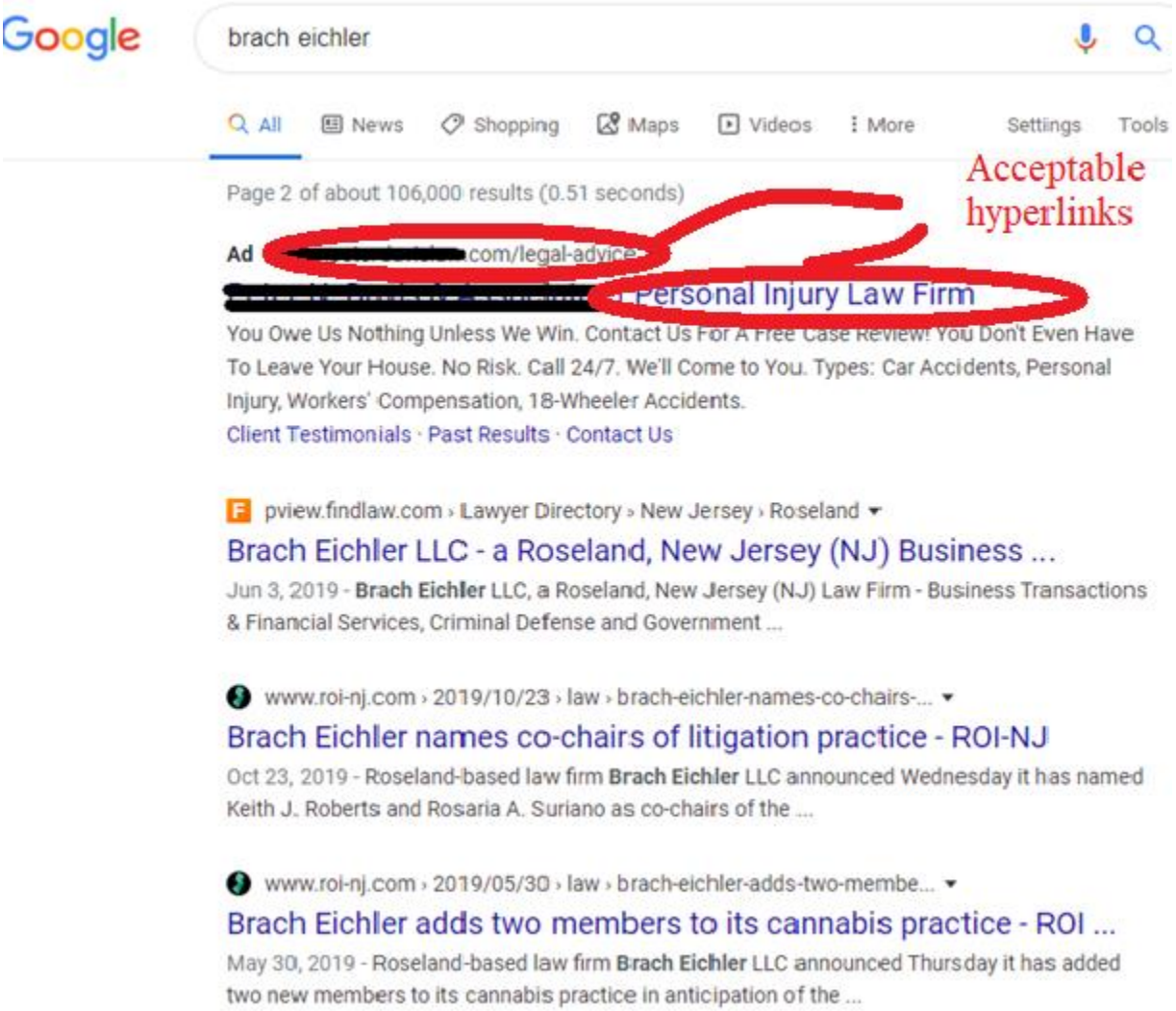
Rather, active competitive keyword advertising involve URL-swapping resulting in a clickjacking transaction where an advertiser could pay to surreptitiously swap URLs to redirect consumers from their intended destination to the advertiser.

Active competitive keyword advertising – inconsistent with rules governing attorney ethics

In short, an attorney may not insert, or paying an internet search engine company to insert, a hyperlink on the name or website URL of a competitor lawyer that will divert the user from the searched-for website to the lawyer's own law firm website and still be incompliance with the rules governing attorney ethics.

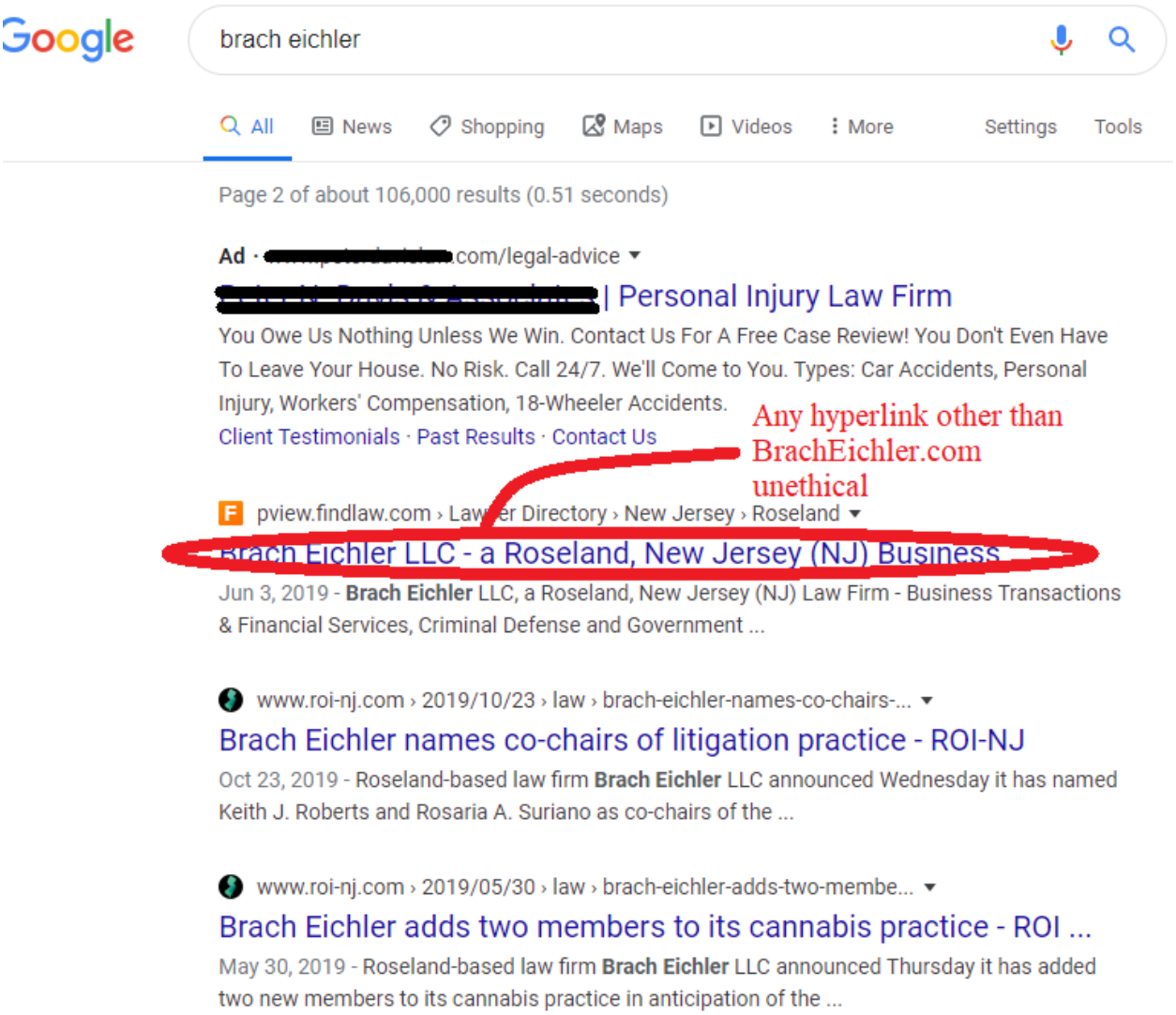
The use of hyper link for passive competitive keywork advertising is acceptable in jurisdictions which permit passive competitive keyword advertising. For example:

These permitted hyperlinks will redirect an Internet site user from a competitor's band name or offering to said competitor's Internet site. It will not redirect an Internet site user from Brach Eichler's band name to a competitor's Internet site



Ethic opinions, such as one issued by New Jersey clearly object to active competitive keyword advertising because it "surreptitiously redirecting a user from the competitor's website to the lawyer's own website."

If the ad copy contains the rival lawyer's name or URL, and people can click on that name/URL but are linked to the advertiser's website, then perhaps that would constitute the referenced "diversion." For Example:



As another example, if the keyword advertisement content is the clickable (linked to a hyperlink) and said hyperlink is anything other than an Internet site which would be normally anticipated by an Internet user then it is unethical. Thus, if an AdWord uses one law firm's name but the hyperlink redirects an Internet user to a rival's Internet site, then such activity will be deemed inconsistent with rules governing attorney ethical behavior.

In short, competitive keyword ads are ethical so long as the rival isn't referenced in the ad copy– or at least not in the ad title.

Internet professional responsibility and client privacy

Internet professional responsibility and client privacy difficulties are intimately associated with the services offered by lawyers. Electronic attorney services result in data gathering, information exchange, document transfers, enhanced communications and novel opportunities for marketing and promotion. These services, in turn, provide an array of complicated ethical issues that can present pitfalls for the uninitiated and unwary.

Since the Internet interpenetrates every aspect of the law, Internet activity can result in a grievance filed against attorneys for professional and ethical misconduct when such use results in: communication failure, conflicts of interest, misrepresentation, fraud, dishonesty, missed deadlines or court appearances, advertising violations, improper billing and funds misuse. While specific Internet privacy violation rules and regulations are rarely applied to attorney transactions, attorneys are regularly implicated in unfair and deceptive trade practices and industry specific violations which are often interspersed with privacy violation facts.

Attorneys have a professional-responsibility duty to use the Internet, and it is that professional responsibility which results in difficulties for doing so. More specifically, the Model Rules of Professional Conduct Rule 1.1 (competence) paragraph 8 (maintenance) has been interpreted to require the use of the Internet, and Rules 7.1 – 7.5 (communications, advertising and soliciting) specifically charge attorneys with malfeasance for using the Internet improperly.

Internet professional conduct standards and model rules/commentary cross the full range of Internet-related concerns, including: expert self-identification and specialty description; the correct way to structure Internet personal profiles; social media privacy settings; the importance and use of disclaimers; what constitutes “communication”; and the establishment of an attorney-client relationship. Additionally, ethics rules address “liking,” “friending” and “tagging” practices.

The application of codes of professional conduct is faced with a two-fold difficulty. First, what is the nature of the attorney Internet activity? Is the activity publishing, broadcasting or telecommunications? Determining the nature of the attorney Internet activity is important because different privacy and ethic cannons apply. Additionally, the determination of the nature of the attorney activity allows practitioners to apply analogies. For example, guidance with respect to attorney Internet-advertising professional conduct is likely to be judged by the same standards as traditional attorney advertising.

The second difficulty is the location where activity occurs. Jurisdictions have enacted contrary laws and professional-responsibility duties.

Options for protecting client privacy and promoting professional responsibility include technical, business and legal options. Consider the following specific legal transactions.

A lawyer seeking to use the Internet to attract new clients across multiple jurisdictions frequently is confronted with inconsistent rules and regulations. A number of jurisdictions have taken the position that Internet communications are a form of advertising and thus subject to a particular state bar’s ethical restrictions. Such restrictions related to Internet content include: banning

testimonials; prohibitions on self-laudatory statements; disclaimers; and labeling the materials presented as advertising.

Other restrictions relate to content processing, such as requiring that advance copies of any advertising materials be submitted for review by designated bar entities prior to dissemination, and requiring that attorneys keep a copy of their website and any changes made to it for three years, along with a record of when and where the website was used. Still other restrictions relate to distribution techniques, such as unsolicited commercial emailing (spam). Spam is considered by some states as overreaching, on the same grounds as ethical bans on in-person or telephone solicitation.

To overcome these difficulties and thus permit responsible use of the Internet for attorney marketing, both technical and business solutions are available. The technical solution employs selectively serving advertisements to appropriate locations. For this solution, software can be deployed to detect the origin of an Internet transaction. This software will serve up advertising based on the location of the recipient. Thus, attorneys can ameliorate or eliminate the difficulties associated with advertising and marketing restrictions without applying the most restrictive rule to every state.

Alternatively, a business solution may be used. Such a business solution would apply the most restrictive rules of each state to every Internet advertising and marketing communication.

Another legal difficulty associated with attorney Internet advertising and marketing is the unauthorized practice of law. All states have statutes or ethical rules that make it unlawful for persons to hold themselves out as attorneys or to provide legal services unless admitted and licensed to practice in that jurisdiction.

There are no reported decisions on this issue, but a handful of ethics opinions and court decisions take a restrictive view of unauthorized practice issues. For example, the court in Birbower, Montalbano, Condon & Frank v. Superior, 949 P.2d 1(1998), relied on unauthorized practice concerns in refusing to honor a fee agreement between a New York law firm and a California client for legal services provided in California, because the New York firm did not retain local counsel and its attorneys were not admitted in California.

Software can detect the origin of an Internet transaction. Thus, attorneys can ameliorate or eliminate the unauthorized practice of law by identifying the location of a potential client and only interacting with potential clients located in state where an attorney is authorized to practice. Alternatively, an attorney could use a net nanny to prevent communications with potential clients located in state where the attorney is not authorized to practice.

Preserving clients' confidences is of critical importance in all aspects of an attorney's practice. An attorney using the Internet to communicate with a client must consider the confidentiality of such communications. Using the Internet to communicate with clients on confidential matters raises a number of issues, including whether such communications: might violate the obligation to maintain client confidentiality; result in a waiver of the attorney-client privilege if intercepted by an unauthorized party; and create possible malpractice liability.

Both legal and technological solutions are available. First, memorializing informed consent is a legal solution.

Some recent ethics opinions suggest a need for caution. Iowa Opinion 96-1 states that before sending client-sensitive information over the Internet, a lawyer should either encrypt the information or obtain the client's written acknowledgment of the risks of using this method of communication.

Substantial compliance may be a technological solution, because the changing nature of Internet difficulties makes complete compliance unfeasible. Some attorneys have adopted internal measures to protect electronic client communications, including: asking clients to consider alternative technologies; encrypting messages to increase security; obtaining written client authorization to use the Internet and acknowledgment of the possible risks in so doing; and exercising independent judgment about communications too sensitive to share using the Internet. While the use of such technology is not foolproof, if said use is demonstrably more significant than what is customary, judges and juries have found such efforts to be sufficient.

Finally, both legal and business options are available to surmount Internet-related client conflicts. Because of the business development potential of chat rooms, bulletin boards, and other electronic opportunities for client contact, many attorneys see the Internet as a powerful client development tool. What some fail to recognize, however, is that the very opportunity to attract new clients may be a source of unintended conflicts of interest.

Take, for example, one of the most common uses of Internet chat rooms: a request seeking advice from attorneys experienced in dealing with a particular legal problem. Attorneys have been known to prepare elaborate and highly detailed responses to such inquiries. Depending on the level and nature of the information received and the advice provided, however, attorneys may be dismayed to discover that they have inadvertently created an attorney-client relationship with the requesting party. At a minimum, given the anonymous nature of many such inquiries, they may face the embarrassment and potential client relations problem of taking a public position or providing advice contrary to the interests of an existing firm client.

An acceptable legal solution is the application of disclaimers and consents. Some operators of electronic bulletin boards and online discussion groups have tried to minimize the client conflict potential by providing disclaimers or including as part of the subscription agreement the acknowledgment that any participation in online discussions does not create an attorney-client relationship.

Alternatively, the use of limited answers would be a business solution. The Arizona State Bar recently cautioned that lawyers probably should not answer specific questions posed in chat rooms or news groups because of the inability to screen for potential conflicts with existing clients and the danger of disclosing confidential information.

Because the consequences of finding an attorney-client relationship are severe and may result in disqualification from representing other clients, the prudent lawyer should carefully scrutinize the nature and extent of any participation in online chat rooms and similar venues.

Using rules governing attorney ethics to protect Internet intellectual property

An Internet firm hires an attorney to review its Google Ads account registration responses to help it secure Internet advertising. The law firm uses the firm's confidential intellectual property information to do so. After the representation ends, the Internet firm is repeatedly outbid for Google Ads by an Internet competitor and thereby losing market share and revenue opportunities. The Internet competitor is using the same attorney to review its Google Ads account registration responses as the Internet firm. The Internet firm concerned the attorney is using its information to help a rival want to sue the attorney for malpractice but does not want to expose its confidential intellectual property information to do so. The use of Rule of Professional Conduct may provide an solution.

The use of ethics rules in malpractice proceeding is design to prevent the law from requiring former clients form revealing confidential intellectual property information while in the process of dealing with attorneys who have misused said confidential intellectual property information. The use of ethics rules provides an alternative for a former client to providing direct proof that attorneys misused their confidential information, by disclosing the confidential intellectual property information that ethic rules are intended to shield.

For the New Jersey and the Model Rule of Professional Conduct 1.9. Rule 1.9(a) prohibits an attorney "who has formerly represented a client in a matter" from subsequently "represent[ing] another person in the same or a substantially related matter in which that person's interests are materially adverse to the interests of the former client." The application of this Rule provides an options for the Internet firm to prove the element of breach within the broader claim of breach of confidentiality without specific disclosure of the firm's confidential intellectual property information.

Rule 1.9 allows the Internet firm to bring a legal malpractice suit against its former attorney by alleging that the attorney breached of confidentiality of the Internet firm by showing the attorney misused its confidences (i.e. the Internet firm's intellectual property information). As in the case of traditional violation of confidentiality matters, the Internet firm would identify damages stemming from being out bid on Google Ads and associated lost market share and profits.

The elements of a breached of confidentiality action are : (1) the attorney had a duty not to misuse the confidential information of its former client; (2) the attorney breached that duty by misusing confidences; and (3) the breach caused the former client to suffer an injury (see Restatement (Second) of Torts § 652H (Am. Law Inst. 1977)). Traditionally, the Internet firm should have to present proof that the law firm actually misused the firm's confidential intellectual property information but by doing so the Internet firm may be required to disclose the information it want kept secret.

The concept of "substantial relationship between two matters" is common understood. In particular, two matters are substantially related when there is a "substantial risk" that the former client's confidential information would advance the new client's position. See In re American Airlines, Inc. 972 F.2d 605, 621-28 (5th Cir. 1992) (finding disqualification proper when law firm engaged in impermissible conflicts of interest in substantially related matters), cert. denied, Northwest Airlines, Inc. v. American Airlines, 113 S. Ct. 1262 (1993).

Rather, the Internet firm may convince a judge that a malpractice suit be allowed by merely showing that the exact matter for which the Internet firm hired the attorney in question is the "same or a substantially related matter in which that person's interests are materially adverse to the interests of the former client" (i.e. a violation of Rule 1.9). This finding may be in the form of a courts finding of a conclusive presumption that an attorney breach had occurred. See Damron v. Herzog, 67 F.3d 211, wherein the Court found that common law requires a continuing duty owed by attorneys to former clients not to represent an interest adverse to a former client on a matter substantially related to the matter of engagement. When such a duty is breached, the former client may bring a cause of action at law.

It should be noted that Rule 1.9 provides the basis for three kinds of action adverse to the conflicted attorney: professional discipline, disqualification, and civil damages. See Restatement (Third) of the Laws Governing Lawyers Section 132 (2000). Thus, Rule 1.9 is directly allows a malpractice action in the form of a suit arising out of an attorney's violation of a confidentiality duty.

Due to the importance of the attorney client confidence, courts are likely to allow rules which are favorable to the client to apply. Thus, a court may not require, proof of the actual misuse of confidential intellectual property information, but rather the possibility of the breach of confidential intellectual property information to be determinative. In short, the public policy of protecting attorney client confidence combined with the risk of breach may justify a conclusive presumption. Thus, the Internet firm in this matter need no disclosure confidential intellectual property information in order to result in a favorable malpractice result.

In short, the mere threat of disclosure may be enough to raise a presumption of breach. It should be noted "substantial relationship" standard is not meet every time an attorney has some knowledge of a former client's confidential information. However, it is most likely met when an attorney has access to information helpful to a client's rival while performing identical services for both a former client and a client's rival immediately after do so for a former client. The fact that mere substantial relationship" standard is not meet every time an attorney has some knowledge of a former client's confidential information protects attorneys from facing liability for a breach of confidentiality that never happened.

It should be noted that the application of the "substantial relationship" standard for malpractice proceeding is viewed by the court in light of the totality-of-the-circumstances test, wherein a court will consider all of the factual and legal issues relevant specific circumstances. See Black's Law Dictionary, Totality of circumstances test (Accessed December 3, 2019).

Thus, Rule 1.9 combined with the benefit of a conclusive presumption may make sense in a malpractice action because it may avoid disclosing confidential intellectual property information in open court. The application of Rule 1.9 in this instance is a practical option when confidential intellectual property information should not be disclosed.

Supplemental material E-Discovery Ethics: Let's Be Reasonable

E-discovery is likely to be as important as traditional discovery because relevant information is as likely to be found on phones, websites, Facebook, e-mail and voicemail messages, as it is in a file cabinet. Although attorneys are rapidly becoming familiar with structuring digital data requests and responding to those requests in a way that is thorough, but reasonable, most attorneys feel at sea in the e-discovery ethics arena. New Jersey and more than a dozen other states have addressed e-discovery ethics and have concluded that "reasonability" is the standard by which ethical digital behavior will be judged.

For example, the N.J. Advisory Committee on Professional Ethics Opinion 701 (2006) found that an attorney may use the Internet to communicate with clients and store client files, provided that the attorney uses reasonable care. This New Jersey ethics opinion also requires New Jersey attorneys to make a reasonable effort to provide security on the Internet against hacking and other forms of unauthorized use of digital information. Additionally, New Jersey attorneys are required to use reasonable care to prevent against unauthorized disclosure of digital documents with which the lawyer has been entrusted, as well as reasonable care to ensure that digital documents entrusted to a third party for analysis are preserved, confidential and secure according to the same ethics opinion.

Applying this standard to the discovery process suggests certain actions. While the evolution of the Internet will require some evolution in these actions, since nearly every case involves some form of evidence stored electronically—in databases, email servers, cellphones, social media networks and the cloud—attorneys are likely to adjust to such new technology by applying existing discovery ethics to e-discovery by analogy.

Furthermore, the New Jersey reasonability standard applies to a requirement that New Jersey attorneys be reasonably educated in Internet-related technology. As noted in Ethics Opinion 701, New Jersey attorneys are considered reasonably competent regarding e-discovery when they avoid being rendered useless, and can maintain the duty of confidentiality, as well as competently overseeing nonlawyers, including e-discovery experts.

Specifically, this ethical requirement means that New Jersey litigators must be able to assess e-discovery needs and issues, understand certain e-discovery terminology such as ESI ("electronically stored information," which refers to all information stored in computers and storage devices), implement appropriate ESI preservation procedures, and effectively advise the client on available options for collection and preservation of ESI and related custodians. Other reasonable e-discovery competencies include assessing the relevant ESI, ability to engage in competent and meaningful meetings and confer with opposing counsel concerning an e-discovery plan, direct digital data searches, harvest responsive ESI and prepare responsive nonprivileged ESI.

Initially, preserving ESI is the most important matter with respect to e-discovery. Among the first e-discovery activities with respect to digital data preservation is a litigation hold. A litigation hold is a demand issued by an attorney to entities associated with a matter who may

possess potentially relevant documents (including ESI) that directs those custodians to preserve such documents, pending further direction. Failure to issue an ESI litigation hold, as well as failure to enforce it, may subject a lawyer to ethical and litigation sanctions. In Scentsy v. B.R. Chase (D. Idaho Oct. 2, 2012), the court found that failure to execute an ESI litigation hold would result in the dismissal of the case if any ESI any destruction was revealed.

It would be unreasonable for an attorney to pass the responsibility to preserve documents on to a client upon the implementation of a litigation hold. Rather, an attorney must remain actively involved to ensure the hold is executed, or else both the lawyer and the client may suffer sanctions.

As a result, applying a "reasonability" standard, it would be reasonable for a New Jersey attorney to recommend to a litigation client to regularly monitor a legal hold to ensure compliance by requiring ongoing certifications from custodians. It may also be reasonable for a New Jersey attorney to monitor such certifications, as well as recommend that clients deploy legal hold automation software and dedicated "legal hold" servers to facilitate client compliance.

Since it is reasonable for an attorney to know that a computer is only one source of ESI, a New Jersey attorney is most likely responsible for counseling a client to refrain from Facebook comments, to honor an ethical duty to preserve evidence. The duty to preserve ESI includes text messages and other information stored on a party's cellphone. Thus, it is reasonable for a New Jersey attorney to educate a client on the importance of electronic evidence. Besides, to comply with a reasonable standard as related to ethical duties, a New Jersey attorney must make an active effort to understand his client's electronic storage, contact custodians of documents in order to mandate preservation and monitor compliance with such directions—and do all these things across all forms of ESI.

ESI may result in an ethical duty to preserve a massive amount of data. Nevertheless, it is reasonable that a New Jersey attorney has an ethical obligation to protect privileged documents.

To properly address this ethical obligation, it is reasonable for New Jersey attorneys to determine what search terms could result in harm to a client prior to discussing appropriate searches of a client's database with opposing counsel, or allowing a vendor unfettered access to his client's network. A failure to protect privileged data might also result from a New Jersey attorney's reasonable effort to monitor the vendor or reasonably review the data the vendor gathered. A litigator may ameliorate personal responsibility to comply with an ethical obligation to protect privileged documents by hiring an e-discovery expert to consult on the case. This option is particularly relevant to New Jersey attorneys who are not able to actively supervise searches due to a lack of time or expertise.

Delegation is not a panacea. E-discovery experts may be useful for expediting discovery and guiding a lawyer through an otherwise unmanageable maze of documents. However, the lawyer, not the expert, is ultimately responsible for a breach of ethics because the attorney must be certain never to certify the completeness of discovery responses without a "reasonable inquiry" under Federal Rule of Civil Procedure 26(g), or risk being liable for court-imposed sanctions.

The risk of accidentally producing privileged material is significant due to the nature and volume of ESI, as well as the involvement of third-party experts. Thus, in the event of an error, lawyers rely on claw-back provisions and Federal Rule of Evidence 502(b)—which allows certain inadvertent disclosures to not act as a waiver of privilege—for protection in the event of inadvertently disclosed documents. The relative novelty of ESI makes the execution of this option more palatable for both attorneys and the courts.

However, a claim of "inadvertent disclosure" is not enough to protect accidentally produced, privileged documents. Unless a New Jersey attorney has taken reasonable steps to prevent the inadvertent disclosure, he will be deemed to have waived the privilege, despite his reasonable efforts to correct the error on the back end.