



**26 Law. Man. Prof. Conduct 586 (September 29, 2010)**

*Model Rules*

**Ethics 20/20 Commission Invites Comments  
On Issues Raised by Growing Use of Internet**

The ABA's Commission on Ethics 20/20 Sept. 20 released two "issues papers" soliciting comments on confidentiality concerns that arise when lawyers transmit and store electronic information and the related professional responsibility issues that crop up when lawyers take advantage of online technology to market and advertise their services.

The papers, drafted by the commission's Working Group on the Implications of New Technologies, outline a number of ethical concerns identified by the group, and they ask for input on the approaches that commission members are contemplating. The commission set a Dec. 15 deadline for comments, which it said may be posted on its website.

"Evolving technology will continue to be a game changer for lawyers, bar associations, clients, and an information-hungry public," said commission co-chairs Jamie S. Gorelick and Michael Traynor in a joint e-mail to BNA. They explained that responses will be used to supplement the commission's ongoing research in these areas.

Gorelick and Traynor made clear that the commission has not yet taken a position on any of these issues. "The papers merely identify areas where questions exist and solicit responses," they pointed out.

Although Ethics 20/20 will continue to conduct public hearings, the co-chairs said the commission will distribute additional issues papers "as a way to reach a broader and more diverse audience."

The commission was launched in August 2009 by incoming ABA President Carolyn B. Lamm to recommend updates to the ABA Model Rules of Professional Conduct in light of evolving technology and globalization of legal practice. See 25 Law. Man. Prof. Conduct 418.

**Cloudy Forecast**

Confidentiality concerns are implicated in two related types of technology, the working group said. The first involves "cloud computing," which typically refers to computer applications and data storage facilities controlled by third parties. In the working group's view, potential threats to security in this scenario include:

- unauthorized access to confidential client information;
- the location of servers in countries with fewer legal protections for electronically stored information;
- a vendor's failure to back up data adequately;
- unclear policies on ownership of stored data;
- the provider's procedures for responding to (or, when appropriate, resisting) government requests for

access to information;

- policies for notifying customers of security breaches;
- policies for data destruction when a lawyer no longer wants the relevant information available or for transferring the data if a client switches law firms; and
- insufficient data encryption.

“Evolving technology will continue to be a game changer for lawyers, bar associations, clients, and an information-hungry public.”

ABA Commission on Ethics 20/20

Because cloud computing is arguably a form of outsourcing, the working group also speculated that the procedures outlined in ABA Formal Ethics Op. 08-451, 24 Law. Man. Prof. Conduct 466 (2008), which describe a lawyer's obligations when outsourcing work to lawyers and nonlawyers, may need to be applied to the cloud computing context. The commission also asked for input on so-called “cyberinsurance and cyberliability insurance.”

### **Dude, Where's My Laptop?**

The second confidentiality issue raised by the Working Group on the Implications of New Technologies is the threat posed by lost or stolen electronic devices such as portable computers, flash drives, and cell phones. These items are capable of storing an enormous amount of confidential information, the working group observed, and ethics regulations say very little about the specific safety measures that are warranted.

To that end, the working group asked for more input on suggested internal security precautions that lawyers and law firms could take, including:

- providing adequate physical protection or having methods for deleting data remotely in the event that a device is lost or stolen;
- encouraging the use of strong passwords;
- purging data from devices before they are replaced;
- installing safeguards such as programs to combat viruses, malware, and spyware;
- erecting adequate firewalls;
- ensuring frequent backups of data;
- updating computer operating systems to ensure that they contain the latest security protections;
- configuring software and network settings to minimize security risks;
- encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them; and
- avoiding “wifi hotspots” in public places when transmitting confidential information.

The working group said it is weighing three options to address these concerns: (1) develop a “white paper” or some other form of practice guidance document; (2) create an online resource describing existing practices and emerging standards; and/or (3) propose amendments to Model Rule 1.1 (competence), Model Rule 1.6 (confidentiality), and Model Rule 1.15 (safeguarding client property).

## **Blogging and Friending**

The second paper, issued by the same working group, addresses the ethics concerns surrounding lawyers' use of internet tools such as blogs, websites, and social and professional networking services, for purposes of interacting with clients and marketing legal services.

The group said it seeks input on questions surrounding the propriety of:

- blending personal communications and lawyer advertising;
- lawyers' using online social networks to “friend” judges;
- using networking sites to gather information about adverse witnesses and parties;
- participating in blogging and discussion forums; and
- online referral programs.

On the question of lawyer websites, the commission's working group asked for feedback on whether it should recommend updating the Model Rules to reflect the way internet technology has altered the advertising landscape. It specifically mentioned Model Rule 4.1(a) (false statements of material facts or law to third parties), Model Rule 7.1 (material misrepresentation of law in advertisements), and Model Rule 8.4(c) (misrepresentations), as well as Comment [2] to Model Rule 7.2, which describes the types of information that lawyers are allowed to disseminate about their services.

The working group also seeks feedback on the question whether it makes sense to amend Model Rule 1.18 (duties to prospective clients) or the accompanying comments to clarify when communications received through a website might create an inadvertent lawyer-client relationship.

The paper notes that ABA Formal Ethics Op. 10-457 (2010), which was released in late September, addresses these issues in more detail. See 26 Law. Man. Prof. Conduct 577.

Finally, the working group asked for input on how the First Amendment limits application of the ethics rules to these areas of lawyer conduct.

The commission's next public hearing is scheduled for Oct. 14 at the ABA headquarters in Chicago.

By Lance J. Rogers

The Ethics 20/20 Commission's issues paper on client confidentiality and lawyers' use of technology is posted at <http://www.legalethicsforum.com/files/letterhead-client-confidentiality-issues-paper-final-9.20.10-1.pdf>.

The commission's issues paper on lawyers' use of internet-based client development tools may be viewed at <http://www.legalethicsforum.com/files/letterhead-client-development-issues-paper-final-9.20.10.pdf>.

The *ABA/BNA Lawyers' Manual on Professional Conduct*, a multivolume reference and notification service, is available by subscription through the ABA Web Store at <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=2170002MOPC> or by contacting BNA at 1-800-372-1033 or [customer care@BNA.com](mailto:customer care@BNA.com). For a free trial subscription go to [www.bna.com/products/lit/mopc.htm](http://www.bna.com/products/lit/mopc.htm)