2010-2011

CO-CHAIR
Jamie S. Gorelick
WilmerHale
1875 Pennsylvania Ave., N.W.
Washington, DC 20006

CO-CHAIR
Michael Traynor
3131 Eton Ave.
Berkeley, CA 94705

MEMBERS
Professor Stephen Gillers
New York, NY

Jeffrey B. Golden
London, United Kingdom

George W. Jones, Jr.
Washington, DC

Hon. Elizabeth B. Lacy
Richmond, VA

Judith A. Miller
San Francisco, CA

Hon. Kathryn A. Oberly
Washington, DC

Roberta Cooper Ramo
Albuquerque, NM

Herman Joseph Russomanno
Miami, FL

Professor Theodore Schneyer
Tucson, AZ

Professor Carole Silver
Bloomington, IN

Kenneth W. Starr
Waco, TX

Frederic S. Ury
Fairfield, CT

Hon. Gerald W. VandeWalle
Bismarck, ND

LIAISONS
ABA Board of Governors
Carolyn B. Lamm
Washington, DC

Kenneth G. Standard
New York, NY

ABA Center for Professional Responsibility
Donald B. Hilliker
Chicago, IL

ABA Task Force on International Trade in Legal Services
Professor Robert E. Lutz, II
Los Angeles, CA

ABA Standing Committee on Ethics and Professional Responsibility
Philip H. Schaeffer
New York, NY

ABA Young Lawyers Division
Youshea A. Berry

COMMISSION REPORTERS
Keith R. Fisher
Chicago, IL

Andrew M. Perlman
Boston, MA

CENTER FOR PROFESSIONAL RESPONSIBILITY
Jeanne P. Gray, Director

Ellyn S. Rosen, Commission Counsel
(312) 988-5311

Marcia Kladder, Policy & Program Director
(312) 988-5326

Natalia Vera, Senior Paralegal
(312) 988-5328

Kimley Grant, Regulation Paralegal
(312) 988-5319

AMERICAN BAR ASSOCIATION

ABA Commission on Ethics 20/20
321 N. Clark Street
Chicago, IL 60654-7598
Phone: (312) 988-5311
Fax: (312) 988-5280
Website: www.abanet.org/ethics2020

To: ABA Entities, Courts, Bar Associations (state, local, specialty and international), Law Schools, Individuals, and Entities

From: ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies[1]

Re: For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology

Date: September 20, 2010

I. Introduction

The American Bar Association's Commission on Ethics 20/20 is examining technology's impact on the legal profession, including confidentiality-related concerns that arise from lawyers' increasing transmission and storage of electronic information.[2] One of the Commission's objectives is to determine what guidance to offer to lawyers who want to ensure that their use of technology complies with their ethical obligations to protect clients' confidential information. The goal of this paper is to invite comments on the Commission's efforts to date and, specifically, to the questions posed at the end of this paper. Comments may be posted to the Commission's website and should be sent to the Commission as requested below by **December 15, 2010.**

The Commission has taken no positions about the matters addressed in this paper. Rather, the Commission expects to use any comments that it receives to supplement the research that the Commission has completed and to facilitate the development of various reports and proposals that the Commission plans to draft during the next two years.

II. A Brief Overview of Law Practice Technology

The Working Group and Commission have focused on two related types of technology that lawyers commonly employ. The first type has become known as "cloud computing,"[3] a term that usually refers to services that are controlled by third-parties and accessed over the Internet.

---

[1] Members of the Working Group are: Fred S. Ury and Carole Silver (Co-Chairs), Robert E. Lutz, Herman J. Russomanno, Judith A. Miller, Carl Pierce (ABA Standing Committee on Delivery of Legal Services), Michael P. Downey (ABA Law Practice Management Section), Paula Frederick (ABA Standing Committee on Ethics and Professional Responsibility), Stephen J. Curley (ABA Litigation Section), Youshea A. Berry (ABA Young Lawyers' Division). Andrew M. Perlman serves as Reporter, and Will Hornsby, Martin Whittaker, and Sue Michmerhuizen provide counsel.

[2] The Commission is considering other technology-related ethical concerns, but the goal of this paper is to solicit feedback only on issues relating to confidentiality.

[3] There are many different types of cloud computing. This paper uses the term generically to refer to any service provided online and operated by a third party.

Examples include online data storage (e.g., Mozy.com, Carbonite.com), Internet-based email (e.g., AOL, Yahoo, or Gmail), and software as a service ("SaaS").[4] SaaS includes a variety of services that lawyers now use, such as law practice management applications that can help lawyers with conflicts checking, document management and storage, trust account management, timekeeping, and billing.

The second type of technology – technology controlled by lawyers or their employees – has received less recent media attention than cloud computing, but it is more ubiquitous and raises similar confidentiality-related concerns as cloud computing. This category includes many devices that can store or transmit confidential electronic information, such as laptops, cell phones, flash drives, and even photocopiers (e.g., copiers that scan and retain information).

I. Confidentiality-Related Issues of Interest to the Commission

The Commission is studying how lawyers use these forms of technology as well as the current state of data security measures for each form of technology. The Commission's efforts have been guided by the reality that information, whether in electronic or physical form, is susceptible to theft, loss, or inadvertent disclosure. The Commission's goal is to offer recommendations and proposals regarding how lawyers should address these risks. To that end, the Commission invites comments on several confidentiality-related issues arising from lawyers' use of technology.

A. The Form of the Commission's Recommendations

As an initial matter, the Commission recognizes that there may be a gap between technology-related security measures that are ethically required and security measures that are merely consistent with "best practices." For example, it may be consistent with best practices to install sophisticated firewalls and various protections against malware (such as viruses and spyware), but lawyers who fail to do so or who install a more basic level of protection are not necessarily engaged in unethical conduct. Similarly, it might be inadvisable to use a cloud computing provider that does not comply with industry standards regarding encryption, but it is not necessarily unethical if a lawyer decides to do so.

In light of these distinctions, the Commission is currently considering three options, which are not mutually exclusive. First, the Commission could produce a white paper or some other form of practice guidance with regard to lawyers' use of technology. The Commission invites comments on whether the Commission should offer such guidance, and if so, how specific the guidance should (or could) be given the rapid pace

[4] In the past, software had to be installed on a computer to take advantage of certain applications, such as word processing. Today, it is possible to access similar applications online without installing the software on a computer or storing the data (such as word processing files) locally. These online applications are known as "software as a service" and, depending on how they are configured, enable multiple users to access information from different locations. *See* ABA Legal Technology Resource Center, FYI: Software as a Service (SaaS) for Lawyers (2010), http://www.abanet.org/tech/ltrc/fyidocs/saas.html.

of technological change. Moreover, the Commission is interested in learning how lawyers currently determine their ethical obligations in these areas. For example, do lawyers hire technology experts or consultants? Do lawyers review bar association materials, including ethics opinions and best practices guidelines, and if so, which materials do they review and find to be helpful? The Commission is also interested in learning whether any guidance it offers should vary depending on a law office's size, its resources, its practice areas, and the type of clients it serves.

A second option is to create an online resource that describes existing practices and emerging standards regarding lawyers' use of technology. This resource could be operated and continuously updated by the American Bar Association in coordination with various entities, such as the ABA Center for Professional Responsibility, the ABA Legal Technology Resource Center, the ABA's Division for Legal Services, and outside experts on legal technology and legal ethics. This approach has the benefit of ensuring that lawyers have access to regularly updated information about security standards as new technology-related ethical concerns arise.

Finally, a third option (either instead of or in addition to offering a white paper or an interactive online practice guide) is for the Commission to propose amendments to the Model Rules of Professional Conduct, such as Model Rules 1.1 (competency), 1.6 (duty of confidentiality), 1.15 (safeguarding client property), or the comments to those Rules. These amendments could emphasize that lawyers have particular ethical duties to protect clients' electronic information beyond mere practice norms. The Commission invites comments on which Rules or comments should be amended and what issues those amendments should address.

The Commission recognizes that any guidance or rule amendments that it offers would have to operate within an increasingly large body of law that governs data privacy, some of which already applies to lawyers. For example, Massachusetts recently adopted a rigorous law on data privacy, http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf, which applies to many lawyers and law firms (including those outside of Massachusetts) that have confidential information about Massachusetts residents. The Commission invites comments on whether any existing state or federal regulations, or any guidance offered in non-legal industries, would serve as a good model for the legal profession.

B. Confidentiality-Related Concerns from Cloud Computing

Lawyers in different practice settings have taken advantage of cloud computing's many benefits, but cloud computing also raises several specific issues and possible concerns relating to the potential theft, loss, or disclosure of confidential information. They include:

● unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet

● the storage of information on servers in countries with fewer legal protections for electronically stored information

● a vendor's failure to back up data adequately

● unclear policies regarding ownership of stored data

● the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business

● 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 data available or transferring the data if a client switches law firms

● insufficient data encryption

● the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information

The Commission invites comments on how it should approach each of these issues as well as information about other confidentiality-related concerns that the Commission should be addressing with regard to cloud computing.

1. Cloud Computing and Outsourcing

Because cloud computing is arguably a form of outsourcing, the Commission welcomes feedback on the extent to which the procedures outlined in ABA Formal Ethics Opinion 08-451 (describing a lawyer's obligations when outsourcing work to lawyers and non-lawyers) should apply in the cloud computing context.

Similarly, the Commission seeks input into whether cloud computing should affect the Commission's ongoing examination of possible amendments to Model Rule of Professional Conduct 5.3 and the comments to that Rule. In particular, Model Rule 5.3 currently describes a lawyer's ethical obligations when supervising non-lawyer assistants, and a comment to that Rule clarifies that the duty extends to non-lawyers who serve as independent contractors. The Commission is considering possible amendments that would clarify the extent to which lawyers have a duty to supervise non-lawyer assistants who perform their work outside of the law firm. The Commission invites comments on whether Model Rule 5.3 or its comments should be revised to reflect that cloud computing falls under the Rule and, if so, what a lawyer's ethical obligations should be when using cloud computing services.

2. Cloud Computing Industry Standards and Terms and Conditions

The Commission seeks more information about existing cloud computing industry standards with regard to data privacy and security. The Commission also seeks to determine which terms and conditions (if any) are essential for lawyers. Such terms and conditions could address:

- the ownership and physical location of stored data
- the provider's backup policies
- the accessibility of stored data by the provider's employees or sub-contractors
- the provider's compliance with particular state and federal laws governing data privacy (including notifications regarding security breaches)
- the format of the stored data (and whether it is compatible with software available through other providers)
- the type of data encryption
- policies regarding the retrieval of data upon the termination of services

The Commission invites comments on whether lawyers have an obligation to negotiate particular terms and conditions before incorporating cloud computing services into their law practices. And if lawyers should have such an obligation, the Commission seeks input into what the terms and conditions should state and what the Commission's recommendations in this area should be.

C. Confidentiality-Related Concerns from "Local" Technology

Forms of technology other than cloud computing can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen. Because these forms of technology can store vast amounts of confidential information, the Commission is considering whether to recommend that lawyers take certain precautions, such as:

- providing adequate physical protection for devices (e.g., laptops) 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 (e.g., computers, smart phones, and copiers with scanners)

● installing appropriate safeguards against malware (e.g., virus protection, spyware protection)

● installing adequate firewalls to prevent unauthorized access to locally stored data

● 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[5]

● avoiding "wifi hotspots" in public places as a means of transmitting confidential information (e.g., sending an email to a client)

The Commission invites comments on how it should approach each of these issues as well as information about other confidentiality-related concerns that the Commission should be addressing.

D. Cyberinsurance and Cyberliability Insurance

The Commission has learned of the increasing availability of cyberinsurance and cyberliability insurance. Cyberinsurance provides coverage for some technology-related losses, such as the cost to replace lost information due to cyberattacks or the expense of post-cyberattack compliance obligations. A related insurance product is cyberliability insurance, which provides coverage for lawsuits that might not be covered by some professional liability policies, such as claims by third parties arising out of a lawyer's failure to protect confidential electronic information.

The Commission seeks more information about cyberinsurance and cyberliability insurance, including the underwriting requirements for such insurance and whether typical professional liability policies provide inadequate coverage for technology-related claims and losses. The Commission invites comments on the prevalence of cyberinsurance and cyberliability insurance among lawyers, how lawyers currently manage the risks associated with technology (including whether lawyers believe their

[5] The Commission is considering two other issues that relate to the subject of metadata but are outside the scope of this paper. In particular, the Commission is considering whether any guidance is needed beyond ABA Formal Opinion 06-442 concerning a lawyer's surreptitious review of another party's metadata. The Commission is also considering whether any guidance is needed regarding a lawyer's receipt of materials from a third party that the lawyer knows or has reason to believe were unlawfully obtained, such as through a cyberattack.

current professional liability policies provide adequate coverage), and whether the advisability of such policies should vary depending on a law office's size, its resources, its practice areas, and the type of clients it serves. The Commission also seeks to learn whether smaller law firms and solo practitioners have had difficulty obtaining cyberinsurance or cyberliability insurance because of the underwriting requirements involved.

II. Conclusion

Lawyers must take reasonable precautions to ensure that their clients' confidential information remains secure. When data was strictly in hard copy form, lawyers could easily discern how to satisfy their professional obligations and did not need elaborate ethical guidance. Now that data is predominantly in electronic form, however, the necessary precautions are more difficult to identify. One of the Commission's goals is to identify the precautions that are either ethically necessary or professionally advisable. To that end, the Commission invites comments on the questions and issues posed above, including the following:

1. Should the Commission offer some form of white paper that offers practice guidance with regard to lawyers' use of technology? (See Part III.A above.)

    a. If so, which issues should the document address and what advice should it offer? Should the guidance vary depending on a law office's size, its resources, its practice areas, and the type of clients it serves?

    b. How do lawyers currently determine their ethical obligations when using technology? For example, do they rely on information technology experts (either full or part-time)? Do they consult bar association materials, including ethics opinions and best practices guidelines, and if so, which materials do they consult? Are there resources other than the materials listed in the bibliography at the end of this paper that the Commission should review?

2. Should the Commission recommend that the ABA create an online and continuously updated resource that describes existing practices and emerging standards regarding lawyers' use of technology? (See Part III.A above.)

3. Should the Commission propose any amendments to the Model Rules of Professional Conduct, such as Model Rules 1.1 (competency), 1.6 (duty of confidentiality), or 1.15 (safeguarding client property), or the comments to those Rules? If so, which Rules or comments should be amended and what issues should those amendments address? (See Part III.A above.)

4. Do any existing state or federal regulations, or any best practices documents offered in non-legal industries, serve as a good model for the legal profession regarding the use of technology? For example, for law firms that have had to

comply with the new Massachusetts statute on data security, have those law firms found the new requirements to be consistent with existing practices, and if not, are the new requirements useful? Do the requirements impose any unnecessary burdens on law practices? (See Part III.A. above.)

5. With regard to cloud computing, which confidentiality-related issues require the Commission's attention, and what particular guidance should the Commission offer regarding those issues? (See Part III.B above).

    a. Is cloud computing a form of outsourcing that should be analyzed under ABA Formal Ethics Opinion 08-451 or governed by Model Rule 5.3 and its comments? (See III.B.1 above.)

    b. Should lawyers have an obligation to negotiate particular terms and conditions before incorporating cloud computing services into their law practices? If so, which terms and conditions are essential, and what should the Commission's recommendations be regarding these terms and conditions? (See III.B.2 above.)

    c. What are the cloud computing industry's standards regarding data security? Does the industry have standard terms and conditions? To what extent are they negotiable? (See III.B.2 above.)

6. Should the Commission offer guidance on various precautions that lawyers should take regarding the use of various devices that are capable of storing or transmitting confidential information, such as laptops, flash drives, smart phones, and photocopiers? If so, which precautions should the Commission recommend? And should those recommendations take the form of practice guidance or proposed amendments to the Model Rules of Professional Conduct? (See III.C above.)

7. Do professional liability policies typically cover claims arising out of technology-related thefts, losses, or inadvertent disclosures of confidential digital information? If not, should lawyers consider purchasing cyberinsurance or cyberliability insurance? Should the decision to buy such coverage depend on a law office's size, its resources, its practice areas, and the type of clients it serves? What are the underwriting requirements for such insurance? Have lawyers and law firms had difficulty satisfying the underwriting requirements for such policies? (See III.D above.)

Responses to these questions or comments on any related issues should be directed by **December 15, 2010**, to:

Natalia Vera
Senior Research Paralegal, Commission on Ethics 20/20
ABA Center for Professional Responsibility
321 North Clark Street
15th Floor
Chicago, IL 60654-7598
Phone: 312/988-5328
Fax: 312/988-5280
veran@staff.abanet.org

Comments received may be posted to the Commission's website.

Select Bibliography

The Commission has had the benefit of reviewing numerous materials, a select number of which are included in this sample bibliography. The Working Group and Commission welcome recommendations for additional resources that address the issues in this paper.

Ethics Opinions and Related Materials

1. ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008).
2. ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).
3. ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995).
4. State Bar of Arizona Op. 09-04 (2009).
5. State Bar of Arizona Op. 05-04 (2005).
6. Florida Bar Op. 06-01 (2006).
7. Illinois State Bar Ass'n Op. 96-10 (1997).
8. Maine Prof'l Ethics Comm'n Op. no. 194 (2008).
9. Nevada State Bar Formal Op. 33 (2006).
10. New Jersey Advisory Comm. on Prof'l Ethics Op. 701 (2006).
11. New York State Bar Ass'n Op. 820 (2008).

12. New York State Bar Ass'n Op. 782 (2004).

13. North Carolina Bar Ass'n Proposed Op. 7 (2010).

14. State Bar Ass'n of N. Dakota Op. 99-03 (1999).

15. Pennsylvania Bar Ass'n Inquiry No. 2010-014 (2010).

16. Pennsylvania Bar Ass'n Op. 2005-105 (2005).

17. Technology Advisory Comm. of North Carolina Bar Ass'n, Comments to State Bar's Request for Comments on Ethics Opinion (May 10, 2010).

18. Memorandum from the ABA eLawyering Task Force of the Law Practice Management Section, to the North Carolina Ethics Committee, *"Cloud Computing", Solos and Small Law Firms, and Consumer Access Affordable Legal Services* (Oct. 15, 2009).

19. Letter from Carolyn Elefant, Attorney, Creator of MyShingle.com, to Alice Neece Mine, Assistant Executive Director, North Carolina State Bar, *Re: Ethics Inquiry on Cloud Computing*, (April 9, 2010).

Background on Cloud Computing

20. ABA Legal Technology Resource Center, FYI: Software as a Service (SaaS) for Lawyers (2010).

21. Roland L. Trope & Claudia Ray, *The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges* (2010).

22. David Bilinksky and Matt Kesner, *Introduction to Cloud Computing*, ABA Techshow (2010).

23. Nicole Black, *Lawyers Should Not Be Wary of Cloud Computing*, 72 Tex. B.J. 746 (2009).

24. Stephanie Kimbro, *Chapter 3: Choosing the Technology, Cloud Computing and Software as a Service (SaaS), in* Delivering Legal Services Online: How to Set Up and Operate a Virtual Law Practice (2010).

25. Edward A. Pisacreta, A Checklist for Cloud Computing Deals (2010).

26. Catherine Reach and Erik Mazzone, *Hey, You, Get ~~Off of~~ Onto My Cloud: Tools to Run Your Practice in the Cloud*, ABA Techshow (2010).

Background on Lawyers' Use of Technology

27. Erik Mazzone & David Ries, *A Techno-Ethics Checklist, Basics for Being Safe, Not Sorry*, ABA Law Practice Magazine, Vol. 35 No. 2 (2009).

28. Roland L. Trope & E. Michael Power, *Lessons in Data Governance: A Survey of Legal Developments in Data Management, Privacy and Security*, 61 Bus. Law. 471 (2005).

29. John D. Comerford, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 Geo. J. Legal Ethics 629 (2006).

30. Faith M. Heikkila, *Data Privacy in the Law Firm*, 88-JUL Mich. B.J. 33 (2009).

31. Tonya L. Johnson, *Is Your Copy Machine A Security Risk?*, ABA Site-tation Posts (May 18, 2010).

32. Ash Mayfield, *Decrypting the Code of Ethics: The Relationship Between an Attorney's Ethical Duties and Network Security*, 60 Okla. L. Rev. 547 (2007).

33. Dan Pinnington, Managing the Security and Privacy of Electronic Data in a Law Office- Part 1, Law Practice Today (Jan. 2005).