LEGAL ETHICS AND TECHNOLOGY

By William Freivogel
www.freivogel.com

Introduction

This paper deals with how technology intersects with the legal ethics rules. The relevant areas are competence, confidentiality, and conflicts of interest.

A. Competence and Technology

The first rule in legal ethics is that a lawyer must be competent.[1] Failure of a lawyer to use technology properly can lead to client harm and thus the claim that the lawyer has acted incompetently.

1. *Backup*

The failure of a lawyer to back up her computer system could result in the loss of crucial client data.

2. *Viruses*

Failure of a lawyer to use standard antivirus software can cause the loss of crucial client data.

3. *Bulletin Boards, Listservs, and Chat Rooms*

Taking positions on legal issues online could undermine the position a lawyer is taking, or may have to take, on behalf of a client. In the context of a law firm, one partner or associate may undermine the position being taken by another. For example, the author is aware of a situation in which a lawyer in a firm posted on the Internet opinions that were highly critical of a law firm that was representing a tobacco company. It turned out the lawyer's firm was co-counsel with the law firm being criticized.

4. *Electronic Filings*

Some tribunals and government agencies require electronic filing.[2] Some prohibit electronic filing.[3] Thus, failure to know the difference can cause harm to a client.

---

[1] American Bar Association Model Rules of Professional Conduct, Rule 1.1. The ABA Model Code of Professional Responsibility has no analogue to Rule 1.1, but references to competence appear throughout the Code. See, for example, EC 1-1, EC 1-2, EC 6-1, EC 6-2, EC 6-3, EC 6-4, EC 6-5, and DR 6-101(A). In the following footnotes and in the text, further references to the ABA Model Rules will be simply "Rule 1.1," and so forth, and references to the ABA Model Code will be simply "EC 1-1," "DR 6-101(A)," and so forth.

[2] See, for example, the SEC's EDGAR filing requirements at 17 C.F.R. pt. 230, et seq.

5. Litigator Competence - Discovery

Much valuable information resides on the hard drives of the parties to the litigation. A client whose lawyer does not know how to discover that information is at a distinct disadvantage.[4]

All the above situations are those in which a perfectly competent lawyer can act incompetently and violate Rule 1.1.

B. Confidentiality and Technology

Rule 1.6 and DR 4-101 are the principal provisions requiring lawyers to protect client information. The ways in which a lawyer can violate her duties of confidentiality to her client through the misuse of technology are virtually endless. This subpart of this chapter will attempt to list the most prominent, and, hopefully, the most dangerous.

1. Backup

Subpart A above referred to how crucial client data can be lost through failure to back up a computer system. There is another side to this. There may be instances where the lawyer would have preferred to destroy data – in situations, of course, where destruction would have been perfectly legal. But, the lawyer did not know how the firm's backup system worked and discovered to her chagrin that the data remained on a tape in a warehouse.

2. *Misdirected Facsimiles or E-mails*

It is, of course, possible to send a fax or an E-mail to the wrong person, thereby disclosing client confidences to someone who should not have them. Speed dialing and the ability to send documents to multiple locations with the press of one or two buttons only increase the danger. The author is not aware of a case or ethics opinion holding that misdirecting a fax or E-mail violates the ethics rules on confidentiality.[5] There is, however, no question in the author's mind that lawyer carelessness in this regard could lead to such a finding.

---

[3] In Georgia Department of Transportation v. Norris, 222 Ga. App. 361, 474 S.E.2d 216 (1996), *rev'd on other grounds*, 268 Ga. 192, 486 S.E.2d 826 (1997), a lawyer's filing was deemed late because he had used a fax machine to transmit a crucial filing on the last day it was due. The Georgia Supreme Court reversed because the lawyer had put the document in the mail the day before it was due.

[4] A good discussion of electronic discovery is at Douglas A. Cawley, "Deleted but not Removed," Legal Times, July 21, 1997, at S34.

[5] Formal Opinion 92-368 (1992) of the American Bar Association Standing Committee on Ethics and Professional Responsibility discusses when the recipient of an inadvertently transmitted document containing the opposing parties confidences can be used by the recipient. The focus of the opinion was on whether the attorney-client privilege was waived, not whether Rule 1.6 or DR 4-101 was violated. Both misdirected faxes and E-mails were mentioned in passing. In following footnotes and text the ABA Committee's opinions will be referred to simply as "ABA Op. 92-368 (1992)."

3. *Hardware Abuses*

Lawyers increasingly send documents as E-mail attachments. However, some still use floppy disks. Failure to use new, or "fresh," floppies could result in a breach of client confidentiality. For example, it may be possible for the recipient to detect earlier drafts of the subject document. Or the floppy could contain confidential information of other clients.

Steps should be taken to ensure that hardware that is scrapped, traded in, or sold does not contain client information. Likewise, hardware that is rented or leased should be checked for client information before being returned to its owner.

4. Deleting Documents

Most lawyers now know that hitting the delete button does not remove the document from the hard drive. The document remains retrievable until it is "written over." Even documents written-over can sometimes be recovered if the expertise and software are available. Thus, the lawyer who thinks she has eliminated client data may not have done so.

5. Internet E-mail and Encryption

A debate persists about whether lawyers should communicate with or about clients using Internet E-mail without encryption. Three issues emerge in this debate: (1) Is it a violation of ethics rules on confidentiality? (2) Could it cause a waiver of the attorney-client privilege? and (3) Does it expose the lawyer to a malpractice claim?

Several factors are germane to all three issues. First, no one has been able to show that intercepting Internet E-mail is easier than tapping a landline telephone. Telephone conversations can be scrambled. No one suggests that talking with or about a client in an unscrambled telephone conversation triggers any of the above-listed three concerns.

Tapping a telephone and intercepting an Internet E-mail message are both felonies under the same federal law.[6]

Malpractice Liability. Take the last question first. The author worked at Attorneys' Liability Assurance Society (ALAS) for 12 years studying claims, among other things. Not once during that period, and not since leaving ALAS, has the author ever heard of a claim against a lawyer resulting from the theft of information.

Waiver of Attorney-Client Privilege. The ECPA provides as follows:

[6] Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq. (ECPA).

> No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.[7]

That certainly takes care of federal courts. What about state courts? The author is not aware of any different result in a state court case.

Duty of Confidentiality under Ethics Rules. The ABA and all of the major states' ethics committees have opined that communicating with or about clients using unencrypted Internet E-mail is appropriate except in the most extreme circumstances.[8]

The T.J. Hooper Case. A handful of encryption proponents continue to cite the 1932 Learned Hand opinion in a Second Circuit case, *The T.J. Hooper.*[9] A barge sank in a storm. The issue was whether the tugboat tethered to the barge was seaworthy. The tugboat did not have a wireless radio, with which to monitor the weather. Few vessels had radios then. Nevertheless, the court ruled that the tug could have had a radio. That would have enabled to crew to anticipate the storm and seek shelter. Failure to have the radio made the tug not seaworthy. The problem with using the *T.J. Hooper* case is that it would require lawyers using the telephone to using scrambling technology, which has been around for years.

An excellent summary of these issues appears at David Hricik, *E-Mail and Client Confidentiality: Lawyers Worry too Much about Transmitting Client Confidences by Internet E-Mail.*[10] The author of this chapter wrote one of the early articles advancing the view of the above; it can be found online.[11]

6. Use of Cellular and Cordless Telephones

Use of portable phones should not raise privilege or confidentiality issues. This is because unauthorized interception and use of portable phone conversations violate the same federal law that prohibits unauthorized interception of E-mail messages.[12] Most commentators agree with this view.[13] Caution is advised, however. There have been a

---

[7] 18 U.S.C. § 2517(4).

[8] ABA Op. 99-413 (1999); D.C. Op. 281 (1998); Ill. Op. 96-10 (1997); Mass. Op. 00-1 (2000); and N.Y. Op. 709 (1998).

[9] 60 F.2d 737 (2d Cir. 1932).

[10] 11 GEO. J. LEGAL ETHICS 459 (1999).

[11] http://www.legalethics.com/articles.law?auth=freivogel.txt.

[12] Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq. (ECPA).

[13] David Hricik, *Confidentiality and Privilege in High-Tech Communications*, THE PROFESSIONAL LAWYER, February 1997, at 1; Albert Gidari, Jr., *Proprietary Rights: Privilege and Confidentiality in Cyberspace*, THE COMPUTER LAWYER, February 1996; and Peter R. Jarvis & Bradley F. Tellam, *High-Tech Ethics and Malpractice Issues*, THE PROFESSIONAL LAWYER, 1996 Symposium Issue, at page 51. Another source on these issues is *Electronic Communications*, ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT , at 55:401-55:424 (October 30, 1996). That material is based upon two excellent articles in the Current Reports of that Manual by Joan C. Rogers, dated February 21, 1996, at 37, and March 6, 1996, at 59.

number of ethics opinions and court decisions to the effect that there is no reasonable expectation of privacy on cellular or cordless phones.[14]

C. Conflicts of Interest and Technology

1. Web Site Missteps

Many law firm Web sites contain instructions to viewers of the site on how to contact the firm. This might even include an E-mail template that enables the viewer to insert his or her name and address and append a message. *Caution*. The author is aware of several instances in which a stranger to a law firm E-mailed confidential information to the firm, and then the firm discovered that it represented the party against which the stranger wanted to bring an action. There was a very real danger that receipt of the confidences of the other side would have conflicted the firm out of the matter. For this reason, any invitation for a viewer to contact the firm should contain language similar to the following:

> We will not have an attorney-client relationship with you until you have spoken to a lawyer in the firm and have been sent an engagement letter. Do not put any confidential information in a message to us, until a lawyer in the firm asks you for it.

It would also be advisable to assign one staff member to review all such E-mails and do a conflict-of-interest check. If the matter appears to be a conflict, the staff member would immediately notify the sender that the firm cannot be involved. The staff member would then delete the sender's message and not reveal its contents to anyone else in the firm. The procedure should be put in writing and made part of the firm's office manual. While the author knows of no case or opinion that approves such a screening procedure, by having it and following it, the firm should have a fighting chance to avoid disqualification.

2. Corporate Family Conflict Issues

All lawyers and law firms recognize the need to do conflict-of-interest checks at the outset of any new matter. This might include a computerized check, but it need not be. The author has observed manual checking procedures using file-room cards and/or accounting records that are quite satisfactory. One area that is neglected by most firms is the checking of corporate affiliations. A lawyer who wants to take on a matter adverse to a corporation needs to know whether her firm already represents the corporation's parent, subsidiary, or other affiliate.[15]

---

[14] Complete listings of these opinions and cases can be found at the Hricik and Jarvis & Tellam articles cited in Footnote 13.

[15] Such a relationship may, or may not, create a conflict of interest. A thorough discussion of this appears at http://www.freivogelonconflicts.com. Go to the Table of Conflicts and click on "Corporate Families."

The biggest law firms check corporate relationships with each new matter. They use computers to do conflicts checks and include in those checks data on corporate relationships of the new client *as well as* other parties to the matter. This data is available online and on CD-ROMS. Some law firms use books, but the search results are then entered into the firm's conflicts database. A good law or business librarian can help identify the easiest-to-use and most economical sources of corporate family information.
