E – Ethics:
Ethical Issues for Lawyers in the Electronic Age

April 2008

Table of Contents

David Nuffer
United States Magistrate Judge, District of Utah

Note: An electronic copy of this outline is at http://www.utd.uscourts.gov/judges/nuffer_resources.htm#Continuing. That version includes working hyperlinks. Send any corrections or suggestions to mj.nuffer@utd.uscourts.gov.

This page is intentionally blank for two-sided printing.

Scope of Responsibility[1]

Rule 5.1 Responsibilities Of Partners, Managers, And Supervisory Lawyers
(a) **A partner** in a law firm, **and a lawyer who** individually or together with other lawyers **possesses comparable managerial authority** in a law firm, shall **make reasonable efforts** to ensure that the firm has in effect measures giving **reasonable assurance** that **all lawyers in the firm conform** to the Rules of Professional Conduct.
(b) **A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts** to ensure that the other lawyer conforms to the Rules of Professional Conduct.[2]

Rule 5.3 Responsibilities Regarding Nonlawyer Assistants
With respect to a nonlawyer employed or retained by or associated with a lawyer:
(a) a **partner**, **and a lawyer who** individually or together with other lawyers **possesses comparable managerial authority** in a law firm shall make **reasonable effort**s to ensure that the firm has in effect measures giving **reasonable assurance** that **the person's conduct is compatible** with the professional obligations of the lawyer;
(b) **a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts** to ensure that the person's conduct is compatible with the professional obligations of the lawyer . . . .[3]

Specific Obligations

Entrustment

Rule 1.15 Safekeeping Property
(a) A lawyer shall hold **property of clients or third persons** that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property **shall be identified as such and appropriately safeguarded**. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.[4]

Privilege & Confidentiality

Rule 1.6 Confidentiality Of Information
(a) **A lawyer shall not reveal information relating to the representation of a client** unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).[5]

---

[1] The ethical rules cited are from the ABA Model Rules of Professional Conduct.
[2] Model Rules of Professional Conduct Rule 5.19(a) and (b).
[3] Model Rules of Professional Conduct Rule 5.3(a) and (b).
[4] Model Rules of Professional Conduct Rule 1.15.
[5] Model Rules of Professional Conduct Rule 1.6.

A lawyer must act competently to safeguard information relating to the representation of a client **against inadvertent or unauthorized disclosure by the lawyer or other persons** *who are participating* in the representation of the client or *who are subject* to the lawyer's supervision.[6]

Competence

Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal **knowledge**, **skill**, **thoroughness** and **preparation** reasonably necessary for the representation.[7]

This provision was specifically applied to technology education in a Florida ethics opinion: "The foregoing obligations [regarding metadata] may necessitate a **lawyer's continuing training and education in the use of technology** . . . ."[8]

Rights of Others

Rule 4.4 Respect For Rights Of Third Persons

(b) **A lawyer who receives a document** relating to the representation of the lawyer's client and knows or reasonably should know that the document was **inadvertently sent shall promptly notify the sender**.[9]

Consider Statutory Obligations

A business in this State [Nevada] shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.[10]

E-Activities with Ethical Implications

Email

Email between attorneys and clients

A client's use of an employer's computer or email system may waive privilege. Under ECPA, the business and consent exceptions may entitle the employer to review all communications on the company system and uses of employer-owned computers or resources (e.g., thumbdrives). Communication in this insecure environment may constitute waiver of privilege. "[A] prudent attorney should consider implementing some precautionary measures to protect his client from losing the privilege and confidentiality of e-mail correspondence that the client may read or send

[6] Comment 16 to Model Rules of Professional Conduct Rule 1.6.
[7] Model Rules of Professional Conduct Rule 1.1.
[8] Professional Ethics of the Florida Bar Ethics Opinion 06-2 (September 15, 2006).
[9] Model Rules of Professional Conduct Rule 4.4.
[10] N.R.S. 597.970 (effective October 1, 2008).

in the workplace and to protect himself in any subsequent malpractice suit in which his correspondence with his client has lost its privilege due to workplace monitoring."[11]

Similarly, **a client may waive privilege by forwarding or sending a copy of an email containing privileged information** to someone outside the privilege. An email Martha Stewart sent to counsel contained attorney-client communication – but when she forwarded a copy to her daughter, she waived that privilege.[12]

A client may forward an email containing an opinion or assessment to a third party, creating the possibility of that person's reliance on the attorney's email and an impression of an attorney-client relationship.

The **attorney should adequately archive** email concerning the client to preserve a record of actions taken, communications and advice given, and of decisions made.

Unencrypted email should not be used for sensitive communications. A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.[13]

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions.[14]

Consider a warning/disclaimer on your emails[15]

---

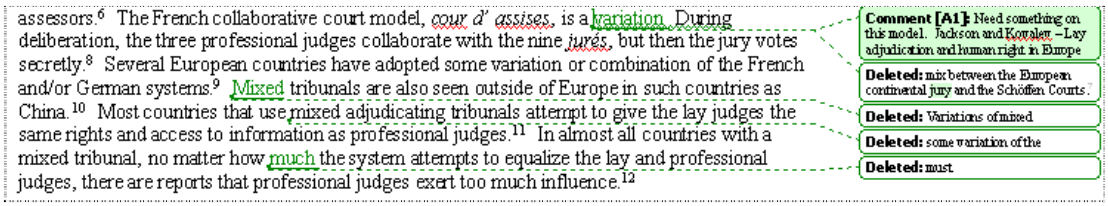
[11] Dion Messer, *To: client@workplace.com: Privilege at Risk?*, 23 J. Marshall J. Computer & Info. L. 75, 99 (2004).
[12] *U.S. v. Stewart*, 287 F. Supp. 2d 461, 464 (S.D.N.Y. 2003). The court did find work product protection existed and was not waived.
[13] ABA Summary of Formal Opinion 99-413 (March 10, 1999). Full opinion at http://www.abanet.org/cpr/pubs/fo99-413.html. See Helen W. Gunnarson, *Should Lawyers Use Email to Communicate with Clients*, 92 Ill. B.J. 572 (2004) and Kurt Metzmeier, *How to Avoid Losing your License on the Information Superhighway: Ethical Issues Raised by the Use of the Internet in The Practice of Law*, 62 Ky. Bar Assn. Bench & Bar 14 (1998) (also found at http://www.legalethics.com/articles.law?auth=metzmeier.txt) for a history of development of ethics opinions on this topic. For a brief look at some international implications, see Lance Johnson, *E-Mail Communication for Client Matters -- A Multinational Survey*, (June 4, 2000).
[14] Comment 17 to Model Rules of Professional Conduct Rule 1.6.
[15] David F. Gallagher, *When E-Mail Messages Come With a Tail of Legalese*, New York Times March 17, 2000; Ronald F. Pol, *Email Disclaimers: Fictional Wizardry*, 24 No. 9 ACC Docket (October 2006).

Email in the office

Consider restrictions on forwarding internal email outside the office. Baker & McKenzie suffered the indignity of public disclosure of an exchange of emails between a senior associate and a secretary over his request that she pay a $10 cleaning bill because she spilled ketchup on him at lunch.[16] Lotus Notes lets you set security restrictions on copying, printing and forwarding email.

Circulating documents outside the firm

Exchanging documents in electronic format with clients, or opposing counsel or providing them to the court may reveal more than you want. Concealed data – metadata – may be contained in your electronic document. The most critical metadata could be revision history which will show all revisions and by whom they were made.



Microsoft Word stores the following metadata:

- Author name
- Author initials
- Author company or organization name
- Author's computer name
- The name of the network server or hard disk where the document is saved
- Other file properties and summary information
- Non-visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions and attributions
- Document versions
- Template and style information
- Hidden text or cells
- Personalized views
- Comments

Microsoft resource: Control metadata in your legal documents
Corel resource: How can I remove metadata from WordPerfect documents?
Background**:** http://www.hricik.com/eethics/Metadata1103.doc

[16] http://www.snopes.com/embarrass/email/ketchup.asp.

New York: Lawyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.[17]

Florida: A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata.[18]

Maryland: An attorney has a duty to remove metadata from electronic discovery before sending it.[19]

When you receive electronic documents with metadata

ABA: The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party.[20]

New York: A lawyer may not make use of computer software applications to surreptitiously "get behind" visible documents or to trace e-mail.[21]

Florida: A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt. The opinion is not intended to address metadata in the context of discovery documents.[22]

Maryland: Maryland does not have new Rule 4.4(b) and therefore a Maryland attorney receiving metadata in a state court matter, in the absence of an agreement to the contrary, need not notify the sending attorney. Federal Rule of Civil Procedure 26(b)(5) creates a different result in federal court proceedings.[23]

Privilege review in e-discovery

It is increasingly common to deliver large quantities of electronic information in response to a discovery request, without filtering it for responsiveness or privilege, under an agreement that there is no privilege waiver.

How can this be reconciled with the lawyer's duties

- to preserve confidences?
- to act with diligence?

There is a substantial risk of waiver of the privilege as to third parties who are not bound by the agreement.[24]

---

[17] New York State Bar Association Ethics Opinion 782 (December 8, 2004).
[18] Professional Ethics of the Florida Bar Ethics Opinion 06-2 (September 15, 2006).
[19] Maryland State Bar Association Committee on Ethics Ethics Docket no. 2007-09.
[20] ABA Formal Ethics Opinion 06-442 (August 6, 2006).
[21] New York State Bar Association Ethics Opinion 749 (December 14, 2001).
[22] Professional Ethics of the Florida Bar Ethics Opinion 06-2 (September 15, 2006).
[23] Maryland State Bar Association Committee on Ethics Ethics Docket no. 2007-09.
[24] Laura Catherine Daniel, *The Dubious Origins and Dangers of Clawback and Quick-Peek Agreements: An Argument Against Their Codification in the Federal Rules of Civil Procedure*, 47 Wm. & Mary L. Rev. 663 (2005); *Koch Materials Co. v. Shore Slurry Seal, Inc.*, 208 F.R.D. 109, 118 (D.N.J. 2002) "Courts generally frown upon "blanket" disclosure provisions as contrary to relevant jurisprudence. In particular, the court observes that such blanket provisions, essentially immunizing attorneys from negligent handling of documents, could lead to sloppy

E-filing in federal court

Privacy policy

The federal courts' privacy policy will be stated in new Rule 5.2 of the Federal Rules of Civil Procedure.[25] The rule became effective December 1, 2007.

> Rule 5.2. Privacy Protection For Filings Made with the Court
> (a) Redacted Filings. Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:
> (1) the last four digits of the social-security number and taxpayer-identification number;
> (2) the year of the individual's birth;
> (3) the minor's initials; and
> (4) the last four digits of the financial-account number.

The policy is most often violated in exhibits and attachments, but quite often counsel seem entirely unaware and unable to comply.

What obligations will accrue to counsel who fail to protect client identifying information – leading to identity theft? What liabilities will accrue to *opposing counsel* who fails to protect identifying information?

At least one court has indicated contempt sanctions would be available against counsel who fail to redact.[26] In response to the order to show cause, counsel stated "the undersigned has instituted procedures in his office whereby both he and his staff are to thoroughly review each and every exhibit, line by line, to further prevent a reoccurrence of the violation."[27]

Redaction

Since all documents filed in CM/ECF (the federal court filing system) must be in PDF format, it is essential to understand redaction of PDF documents. Placing graphics over text is not effective redaction in Acrobat. Acrobat Standard and Professional 8 include redaction tools.

---

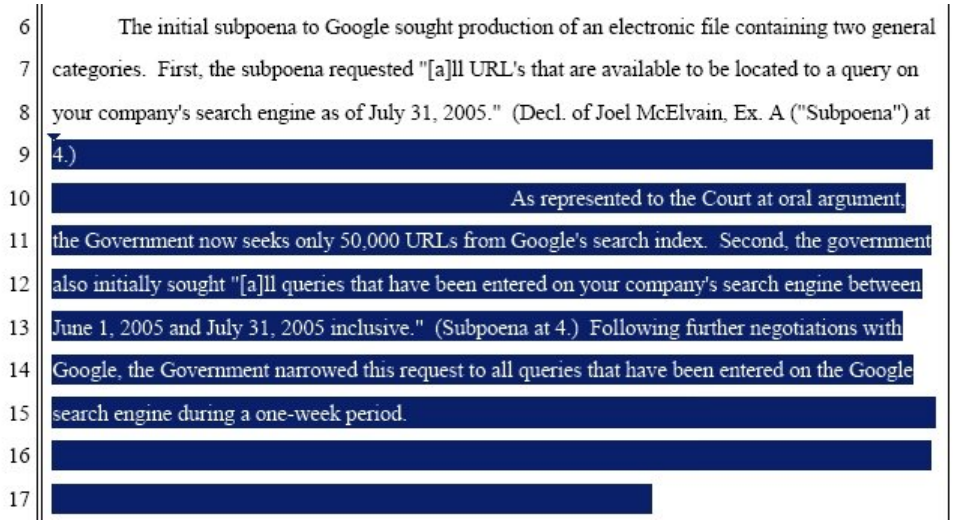
attorney review and improper disclosure which could jeopardize clients' cases." *See also* Colin P. Marks, *Corporate Investigations, Attorney-Client Privilege, and Selective Waiver: Is a Half-Privilege Worth Having at All*?, 30 Seattle U. L. Rev. 155 (2006).

[25] Fed. R. Civ. 5.2. A similar rule is in effect for criminal cases. Fed. R. Crim. P. 49.1.

[26] *Luster v. City of Lebanon*, No. 04-663-MJR, 2007 WL 61859 (S. D. Ill. January 8, 2007).

[27] Response to Order to Show Cause at 3, docket no. 173, filed January 22, 2007, *Luster v. City of Lebanon*, No. 04-663-MJR, S. D. Ill.

This document appears redacted:



But the text behind the graphics is entirely available for copying, searching, etc.

> 4.) In negotiations with Google, this request was later narrowed to a "multi-stage random" sampling of one million URLs in Google's indexed database. As represented to the Court at oral argument, the Government now seeks only 50,000 URLs from Google's search index. Second, the government also initially sought "[a]ll queries that have been entered on your company's search engine between June 1, 2005 and July 31, 2005 inclusive." (Subpoena at 4.) Following further negotiations with Google, the Government narrowed this request to all queries that have been entered on the Google search engine during a one-week period. During the course of the present Miscellaneous Action, the Government further restricted the scope of its request, and now represents that it only requires 5,000 entries from Google's query log in order to meet its discovery needs.

Managing a litigation hold

> *In re Prudential Ins. Co. Sales Practices Litig.*, 169 F.R.D. 598 (D.N.J. 1997).
> While there is no proof that Prudential, through its employees, engaged in conduct intended to thwart discovery through the purposeful destruction of documents, its haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute. Because the destroyed records in Cambridge are permanently lost, the Court will draw the inference that the destroyed materials are relevant and if available would lead to the proof of a claim. . . .
> When the September 15, 1995 Court Order to preserve documents was entered, it became the obligation of senior management to initiate a comprehensive document preservation plan and to distribute it to all employees. . . .
> The Court finds that the document destruction, particularly in the Cambridge, Massachusetts office, caused harm to party opponents. Over 9,000 files were cleansed. . . .
> Within ten (10) days after the issuance of this Opinion, Prudential shall pay to the Clerk of the United States District Court for the District of New Jersey, the sum of One Million Dollars ($1,000,000).

General Technology Issues with Ethical Implications

Employee practices

- Screen employees before hiring – check references
- Train all employees on confidentiality, proper email use, and security for network, mobile devices and storage
- Make all employees aware of court privacy policy, redaction issues, and metadata
- Evaluate each employee periodically for compliance with procedures and understanding
- Have written agreements with non-lawyers to bind them to confidentiality obligations
- Establish no expectation of privacy in portable data devices, email, computer and network storage and internet use[28]
- Place policy and technical limits on user installed software and violation of copyright and licenses
- Make sure that passwords are protected; terminated on change of employment
- Password lists must be secure

  Standard password advice:
  - Require a password for any computer or network access;
  - People who share jobs do not share passwords;
  - Require that passwords be used to be difficult to decipher. Passwords should be at least seven characters long; should contain letters *and* numbers or characters (@, *, and so on); should never contain a person's name; and should never be written down near the computer;
  - Prohibit use of guest ("Temp1") or default passwords or logons;
  - Require passwords to be updated or changed every four to six months; and
  - Have a central secure location for the firm to record all passwords in use.[29]

Mobile devices

Laptops require a sign-on to access any data or programs and are equipped with updated security tools (consider biometric)
Any remote wireless access is to a trusted service, not to a free host
Any VPN software is accompanied by firewall
Thumbdrives require a password *and* encrypt data
Password protection on PDAs and phones with contact / calendar information
Scheduled inventory day when all equipment must be in the office

Office hardware

Limit the number of recordable CD and DVD drives
Dispose of hardware responsibly

---

[28] The Electronic Communications Privacy Act of 1986 "prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication" but is subject to business provider and consent exceptions. Sarah DiLuzio, Comment, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 Del. J. Corp. L. 741, 745 (2000).

[29] David Kricik, *Protecting Portable Confidences*, E-Ethics Vol. 1, No. VII (March 2002).

Outside services

If you use an outside technical consultant or service, obligate them to confidentiality. "A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer may be obligated to disclose it to the client."[30] This may apply to off-site backup, transcription and document preparation services,[31] data entry services, network administrators, copy services, and forensic consultants.

Law firm web site

Be sure you are licensed in any state in which you may attempt to collect fees. [32] Unsolicited email from prospective clients may create an attorney-client relationship or provide confidential information that disqualifies the firm from adverse representation.[33] Consider web site disclaimers that state, essentially, that any information sent by e-mail before the firm agrees to represent the transmitting party will not be held to be confidential by the firm.[34]

Office network

An office network holding sensitive personal information should comply with industry standards.[35]

Take special precautions with a wireless network.[36]

Assign responsibility to monitor network threats[37] and keep current in the industry:

Sniffer – traffic interceptor that can capture email, web site visits and passwords used. The sniffer may also be used for legitimate network monitoring.

Spoofer – imposter email server that copies all email intended for a legitimate server.

Keylogger – hidden software or hardware that records every keystroke on a computer, and thus captures all data input, including logins, passwords, and message traffic.

---

[30] Summary of ABA Formal Opinion 95-398 Access of Nonlawyers to a Lawyer's Data Base (October 27, 1995).

[31] Opinion No. 194, The Professional Ethics Commission of the Board Of Overseers Of The [Maine] Bar (December 11, 2007).

[32] *Birbrower, Montalbano, Condon & Frank v. Superior Court*, 949 P.2d 1 (Cal. 1998).

[33] Douglas K. Schnell, *Don't Just Hit Send: Unsolicited E-Mail and the Attorney-Client Relationship*, 17 Harv. J. L & Tech 533 (2004).

[34] David Hricik, *Whoops! I did it Again! What Britney Spears Can Teach Us About the Ethical Issues Arising From the Intentional Transmission of Confidences From Prospective Clients to Firms*, E- Ethics Vol. III, No. I, (2004) and David Hricik, *To Whom It May Concern: Using Disclaimers to Avoid Disqualification by Receipt of Unsolicited E-Mail from Prospective Clients*, 16 Professional Lawyer 1 (2005).

[35] *Protecting Personal Information: A Guide for Business*, available at http://www.ftc.gov/infosecurity.

[36] http://www.practicallynetworked.com/support/wireless_secure.htm ; http://www.pcmag.com/article2/0,4149,844020,00.asp; http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

[37] See wikipedia for basic information on any of these threats.

Screen grabber – takes periodic shots of whatever is on the computer screen.

Data miner – software that gathers and amalgamates data from the internet and information services.

Virus and worm – self replicating attack software with or without human intervention.

Intrusions – invasion of network for any purpose.

Zombie – takes possession of all or part of a server to run illicit programs. (Recently used to host child pornography sites and run related e-commerce.)

Capture computer resource such as a web cam or microphone for spy purposes.

According to the 2005 CSI/FBI Computer Security Survey,[38] we have a long way to go:

- Average annual expenditure per employee for computer security is $240 – 750. Legal industry average is $40.
- The legal industry self reports the least satisfaction (2.5 out of 7) with the amount spent on Security Awareness training. High tech reports 4.5 satisfaction.
- Over 50% of those responding to the survey had an incident of unauthorized use in last 12 months.
- Only 20% of computer crime is reported to law enforcement. Only 16% is reported to counsel.
- The range of attacks is broad – almost 100% of web sites are attacked.

[38] http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml.

Note: An electronic copy of this outline is at http://www.utd.uscourts.gov/judges/nuffer_resources.htm#Continuing. That version includes working hyperlinks. Send any corrections or suggestions to mj.nuffer@utd.uscourts.gov.