ELECTRONIC DUMPSTER DIVING:

THE LEGAL ETHICS OF "TMI"

MODERATOR:
William A. Herbert, Deputy Chair and Counsel
New York State Public Employment Relations Board

SPEAKERS:
Nancy L. Cohen, Esquire
MiletichCohen PC, Denver, Colorado

Louis P. Malone, III, Esquire
O'Donoghue & O'Donoghue, Washington, D.C.

Cynthia N. Sass, Esquire
Sass Law Firm, Tampa, Florida

American Bar Association
Section of Labor and Employment Law
Sixth Annual Labor and Employment Law Conference
Atlanta, Georgia
Ethics Track - November 1, 2012

ELECTRONIC DUMPSTER DIVING: THE LEGAL ETHICS OF "TMI"[1]

Moderator:
William A. Herbert, Esquire

Speakers:
Nancy L. Cohen, Esquire
Louis P. Malone, III, Esquire
Cynthia N. Sass, Esquire

Ethics Track
American Bar Association
Sixth Annual Labor and Employment Law Conference

What must the resourceful, yet ethical, lawyer do in an age of too much information ("TMI"), where the boundaries between what is "yours" and what is "mine" are not always clear? Along with other questions ethical lawyers should be asking themselves about the ever-increasing electronic TMI syndrome, this panel will discuss issues like:

- Receipt by a lawyer of unexpected electronically purloined information (from whistleblowers or as after-acquired information in employment cases).

- Providing evidence of a client's financial wrongdoing within the regulatory framework of Sarbanes-Oxley and Dodd-Frank.

- Can a lawyer ethically engage in surveillance of a client?

- What a lawyer who stumbles onto evidence of client perjury or potentially privileged information on the Internet is supposed to do.

- What happens if a lawyer teleworks and brings home client information, or whose computer screen displays confidential client information at an ABA conference?

[1] The material included in this paper is distributed as a service to interested individuals. The information contained herein is provided for informal use only. This material should not be considered legal advice and should not be used as such. Also, a special thanks goes out to Joshua R. Kersey, Esquire of the Sass Law Firm for his assistance in the preparation of these materials.

QUESTION 1: What are the ethical responsibilities of a lawyer who receives electronically purloined information, e.g., from whistleblowers or as after-acquired information in employment cases?

A. AS COUNSEL FOR EMPLOYER:

1. Ethical Opinions:

American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 11-460 August 4, 2011: "Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel"

- "When an employer's lawyer receives copies of an employee's private communications with counsel, which the employer located in the employee's business e-mail file on the employee's workplace computer or other device, neither Rule 4.4(b) nor any other Rule requires the employer's lawyer to notify opposing counsel of the receipt of the communications. However, court decisions, civil procedure rules, or other law may impose such a notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer's lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision."

- "When the law governing potential disclosure is unclear, the lawyer need not risk violating a legal or ethical obligation."

- "The fact that the employer-client has obtained copies of the employee's e-mails is 'information relating to the representation of [the] client' that must be kept confidential under Rule 1.6(a) unless there is an applicable exception to the confidentiality obligation or the client gives 'informed consent' to disclosure."

- "Even when there is no clear notification obligation, it often will be in the employer-client's best interest to give notice and obtain a judicial ruling as to the admissibility of the employee's attorney-client communication before attempting to use them and, if possible, before the employer's lawyer reviews them."

- "The employer's lawyer must explain these and other implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision."

2. Practical Advice for Employer Counsel:

- Determine **where** the information was found.

- Determine whether court decisions, rules of procedure, or other laws create a duty to disclose possession of the information to the other side.

- Explain the implications of making or declining to make the disclosure to the employer-client so that it may make an informed decision.

- For an employer, the **safest** approach to dealing with information from current or former employees is to segregate and preserve the information at the earliest stage possible and, if and when necessary, seek a judicial order as to whether the information is discoverable.

- Remember, at least one court has held there is no "good-faith" exception to a failure to comply with your ethical duty to disclose your possession of communications and/or documents you have reasonable cause to believe may have been inadvertently disclosed. Even if you feel you will ultimately be entitled to the information, the safest approach is to:

  - Refrain from reviewing the information;
  - Segregate the information; and
  - Seek adjudication by the court as to whether you are entitled to the information.

3. Analysis:

a. The most often cited case with respect to clients e-mailing their attorneys is *In re Asia Global Crossing*. There are two important characteristics of the facts in *Asia Global*:

   i. The case involved e-mails sent on a company computer and through a company e-mail address; and

   ii. The documents were segregated early on, so no ethical issues as to disclosure arose.

   Said issue of confidentiality of employee's e-mails in terms of attorney-client privilege is an **"analogous question"** to the employee's expectation of privacy in his office computer and the company e-mail system.

"To determine if a particular communication is confidential and protected by the attorney-client privilege, the privilege holder must prove the communication was (1) intended to remain confidential *and* (2) under the circumstances, was *reasonably* expected and understood to be confidential." *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003)

- The reasonableness of the employee's expectation of privacy usually turns on whether the employee was provided notice that the employer could search or monitor the computer. *United States v. Simons*, 206 F.3d 392, 398 & n.8 (4th Cir. 2000); *Muick v. Glenayre Elecs*, 280 F.3d 741, 743 (7th Cir. 2002); *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004); *Kelleher v. City of Reading*, 2002 U.S. Dist. LEXIS 9408 (E.D. Pa. May 29, 2002); *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002); *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001); *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir.), vacated on other grounds, 537 U.S. 802, 154 L. Ed. 2d 3, 123 S. Ct. 69 (2002); *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996)

The *Asia Global* court developed what is now the most widely used test for determining whether an employee has waived attorney-client privilege with respect to communications made on employer electronics:

- Does the company maintain a policy banning personal or other objectionable use?
- Does the company monitor the use of the employee's computer or e-mail?
- Do third parties have a right of access to the computer or e-mails?
- Did the company notify the employee, or was the employee aware, of the use and monitoring policies?

The crux of the *Asia Global* court's decision was: if the employee has reason to know that his or her e-mails are subject to being read by the employer, and the employee sends those e-mails despite that knowledge, the employee has implicitly consented to the employer reading those e-mails and the attorney-client privilege has been waived.

Other courts faced with those same conditions, reached the same conclusion. See *Kaufman* below.

b. <u>The New Jersey Supreme Court Departs from *Asia Global*.</u> However, in 2009, the New Jersey Supreme Court departed from the *Asia Global* analysis in *Stengart v. Loving Care Agency, Inc.*, 973 A.2d 390 (N.J. 2009). Importantly, unlike *Asia Global* and *Kaufman*, in *Stengart*:

- The case involved e-mails sent on a company computer, but through a private, password-protected e-mail account, such as Gmail or Yahoo; and

- The documents were not segregated, but were retrieved and reviewed by opposing counsel, who did not inform the plaintiff for months that he was in possession of the documents.

Stengart raised new ethical questions with respect to electronic information found by employers in searches of their own electronic equipment which involved use of company equipment, but only to access information in the "cloud." Under which circumstances has an employee waived attorney-client privilege with respect to such information and what are the employer's attorney's ethical responsibilities in dealing with such information?

The *Stengart* decision itself was unclear. The court begins with an *Asia Global*-like analysis, poking holes in the language of the employer's electronic communications policy and finding that employees were not given reasonable notice that all of their personal electronic communications were subject to employer review. The court referred to these policy-related disputes as "threshold" issues. *Id*. at 402.

However, the court later writes that, **regardless of any company policy, "the company policy is of insufficient weight when compared to the important societal considerations that undergird the attorney-client privilege."** *Id*. at 402.

Reconciling the two statements is difficult. If the court holds that the "important societal considerations that undergird the attorney-client privilege" simply outweigh a company's policy regarding electronic considerations, then policy-related disputes would be irrelevant and, therefore, would not be "threshold" issues.

Other notable positions taken by the *Stengart* court:

- **Something does not become company property solely because it was done during working hours.** The *Stengart* court states, "We thus reject the philosophy . . . that, because the employer buys the employee's energies and talents during a certain portion of each workday, anything that the employee does during those hours becomes company property." *Id*. at 401.

- **Something does not become company property solely because it was done on company property.** The *Stengart* court states, "A policy imposed by an employer, purporting to transform all private communications into company property—merely because the company owned the computer used to make private communications or used to access such private information during work hours—furthers no legitimate business interest." *Id*. at 401.

- **The court will not define the extent to which an employer may go in searching information on an employee's computer.** The *Stengart* court states "Here, we make no attempt to define the extent to which an employer may reach into an empoyee's private life or confidential records through an employment rule or regulation. Ultimately, these matters may be a subject best left for the Legislature."

- **There is no "good faith" exception to an attorney's duty to notify the other side when it receives a document it has reasonable cause to believe was inadvertently produced.** The *Stengart* court states that notwithstanding an attorney's good-faith belief that he or she will ultimately be entitled to the document, "attorneys are obligated, as suggested by [the rules of professional conduct] to cease reading or examining the document, protect it from further revelations, and notify the adverse party of its possession so that the attorney's right to retain or make use of the document may thereafter be adjudicated by the court."

c. Post-*Stengart* decisions still use *Asia Global* for work e-mail. *Alamar Ranch, LLC. v.County of Boise*, 2009 U.S. Dist. LEXIS 101866 (D. Idaho Nov. 2, 2009)

The post-*Stengart* decision in *Alamar Ranch* cites to *Stengart*, but distinguishes it because, like *Asia Global* and *Kaufman*, plaintiff used her **work** e-mail on her work computer, not her **private** e-mail on her work computer.

In **determining whether privilege has been waived**, court goes back to *Asia Global* factors.

(1) Three types of e-mails:

- **E-mails sent from plaintiff to her attorney**. Says plaintiff knew that her e-mails were monitored and was explicitly told she had no expectation of privacy in her e-mails, therefore plaintiff waived attorney-client privilege.

- **E-mails sent from her attorney to plaintiff**. As for e-mails sent *from* plaintiff's attorney *to* her work e-mail, the court said that plaintiff's e-mail ("JeriK@IHFA.org") clearly put her attorney on notice that it was her work e-mail and, because employer monitoring of employee e-mail is so common these days, her attorney should have known that the IHFA would be monitoring, accessing and retrieving the e-mails he sent to that address.

- **E-mails sent from co-plaintiffs to attorney and copied to plaintiff, or to plaintiff and copied to attorney**. The court said there had been no waiver of privilege as to these documents because

> "laypersons are simply not on 'high-alert' for such things as attorneys must be" and therefore are not reasonably expected to know that their e-mails sent directly to, or copied to plaintiff's work e-mail account would be viewed by Defendant IHFA.

The court does not address a good-faith exception or any ethical duty on the part of defense counsel to have brought the documents to plaintiff counsel's attention. This is noteworthy because the *Alamar Ranch* court was aware of the decision in *Stengart* and that court's discussion of the attorney's ethical duty. One might read the *Alamar Ranch* court's decision as accepting a good-faith exception to that duty, although they never addressed it.

By referring back to the *Asia Global* factors and excluding any discussion with respect to the ethical obligations of the attorney (and arguably accepting a good-faith defense), the *Alamar Ranch* decision serves to isolate the applicability of the holding in *Stengart*.

d. The U.S. Supreme Court Addresses the Extent of a Reasonable Expectation of Privacy with Respect to Government Employers and the Fourth Amendment

In *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), a case involving a search of government employer-provided pagers, the Supreme Court analyzed the reasonableness of the employees' expectation of privacy under the Fourth Amendment. The additional issue involved with respect to government searches is whether the search itself was reasonable. The search must be "motivated by a legitimate work-related purpose" and "not excessive in scope". In making this determination the Court, in dicta, discussed not only whether Quon's expectation of privacy was reasonable, but also the *extent* of that expectation, i.e., just *how* private can Quon reasonably expect the contents of his pager to be. To that point the Court states:

> "Furthermore, and again on the assumption that Quon had a reasonable expectation of privacy in the contents of his messages, the extent of an expectation is relevant to assessing whether the search was too intrusive. See Von Raab, supra, at 671, 109 S. Ct. 1384, 103 L. Ed. 2d 685; cf. Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 654-657, 115 S. Ct. 2386, 132 L. Ed. 2d 564 (1995). Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing. As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to

> determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises--and given that Quon had received no assurances of privacy--Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations."

The Court's language suggests a two-part analysis of privacy expectation with respect to communications on employer-owned systems. First, whether the employee had *any* reasonable expectation of privacy and second, assuming there was a reasonable expectation of privacy, what is the *extent* of that reasonable expectation.

B. AS COUNSEL FOR EMPLOYEE:

1. Ethical Opinions:

a. American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 06-440 May 13, 2006: "Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382 (July 5, 1994)"

Rule 4.4(b) does not apply to the factual situation where an attorney has received documents that he knows or reasonably should know have been wrongfully obtained, therefore, a lawyer receiving materials under such circumstances is not required to notify another party or that party's lawyer of receipt as a matter of compliance with the Model Rules.

b. Professional Ethics of the Florida Bar Opinion 07-1, September 7, 2007: Documents that were wrongfully obtained.

While Rule 4.4(b) does not require the receiving lawyer to notify the adverse party, there are other rules that apply to the situation:

- 1.6 Ethical Duty of Confidentiality—A lawyer **shall**[2] reveal such information to prevent:
  - (b)(2)—client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services.

[2] Note that this differs from the ABA Model Rules which state a lawyer **may** disclose such information.

- (b)(3)—mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services.

- 4-3.4(a)—A lawyer shall not unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person so do any such act.

- 4-4.4(a)—A lawyer shall not use methods of obtaining evidence that violate the legal rights of third persons.[3]

- 1.2(d)—A lawyer shall not assist a client in conduct that the lawyer knows or reasonably should know is criminal or fraudulent.

- 4-8.4(a)—A lawyer shall not violate the rules through the acts of another.

- 4-8.4(d)—A lawyer shall not engage in conduct that is prejudicial to the administration of justice.

Therefore, a lawyer whose client has provided the lawyer with documents that were wrongfully obtained by the client:

- May need to consult with a criminal defense lawyer to determine if the client has committed a crime;

- Must advise the client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue; and

- If the client refuses to consent to disclosure, the inquiring attorney must withdraw from the representation.

c. <u>American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 11-459 August 4, 2011: "Duty to Protect the Confidentiality of E-mail Communications with One's Client"</u>

[3] The ABA recently amended Rule 4.4 to include that a receiving attorney is required to notify the sending attorney of inadvertent disclosure of electronically stored information and/or metadata. However, with respect to metadata, the commentary suggests that an obligation is only created if the "receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer."

"A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communication will be read by the employer or another third party."

2. Practical Advice:

- Do not communicate with your client through employer-provided means such as work e-mail addresses or work cell phones.

- Advise your client not to access their private electronic communications accounts, (e.g. Yahoo, Gmail) on employer-provided equipment.

- Even if you do not disclose to opposing counsel that you have employer documents in your possession initially upon receipt, you are still required to produce those documents in response to any relevant discovery request.

- Be aware of criminal laws pertaining to electronically stored and/or accessed information as you may be inadvertently concealing evidence of a crime committed by your client.

- Be aware of laws pertaining to trade secret and/or confidential information as you may be assisting your client in furtherance of a criminal act.

- Be aware of your own state bar's opinion, case law and rules as to wrongfully obtained documents as they may differ from the ABA Model Rules.

3. Analysis:

a. <u>Has your client committed or is your client currently committing a crime?</u>

- **The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030**. A number of cases have involved employers alleging violations of the Computer Fraud and Abuse Act. The CFAA prohibits the unauthorized access of a computer (or exceeding authorized access of a computer) and obtaining information. The problem often arises when departing employees attempt to gain an advantage by stealing information from the employer prior to their departure. The statute focuses

on whether the employee's accessing the company computer was without authorization or exceeded any authorization which was granted. There is disagreement among the circuits as to when an employee acts with the requisite authorization. The CFAA provides both criminal penalties including fines and imprisonment for up to 10 years (18 U.S.C. §1030(c)) and a civil cause of action for certain violations of the CFAA where compensatory damages and other injunctive or equitable relief may be granted. 18 U.S.C. §1030(g).

- **The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2510, *et seq*. (a/k/a the Federal Wiretap Act)**. Title I of the ECPA regulates the search and seizure of electronic communications while they are in transit. It provides civil and criminal penalties for the unlawful interception, disclosure or use of electronic communications, and it most often arises in the labor context where employers monitor and intercept communications between employees. Importantly, under the ECPA, consent to the interception by one party to the communication—such as signing an electronic monitoring policy—is a defense to a violation. However, employees can be guilty of offenses under the act in the employment context as well.

  - *United States v. Szymuszkiewicz,* 622 F.3d 701 (7th Cir. 2010) (Szymuszkiewicz' license had been suspended for driving while drunk. He was worried this would lead to his termination because his job required him to drive to people's homes. The jury found that Szymuszkiewicz had gone on his supervisor's computer while she was away and activated a "rule" on her e-mail account so that any e-mail that was sent to Szymuszkiewicz' supervisor was also forwarded to him. Szymuszkiewicz was convicted of intentionally intercepting an electronic communication in violation of the ECPA.) The ECPA provides for separate causes of action both by private individuals and by the government.

  In a private cause of action under the ECPA, a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520. Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5). Finally, the ECPA provides for criminal penalties including a fine and up to up five years of imprisonment. 18 U.S.C. §2511(4).

- **State Wiretap Statutes**. Some state statutes prohibit an individual from intercepting any "wire, oral or electronic communication." In Florida, for instance, any person who has their wire, oral, or electronic communication intercepted in

violation of the statute has a private cause of action where they may seek preliminary or equitable or declaratory relief as may be appropriate, actual damages but not less than liquidated damages computed at a rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages and a reasonable attorney's fee and other litigation costs reasonably incurred. Fla. Stat. §934.10. In contrast to the Federal Wiretap Act, Florida's wiretap statute provides that consent to the interception is a defense only if all parties consent. Additionally, violation of the statute may result in a first degree misdemeanor charge resulting in up to one year in jail.

b. Has your client taken information that may reasonably constitute a "trade secret"?

- **Common Law**. "Any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." Restatement (Third) of Unfair Competition §39 (1995)

- **State Law**. "Trade secret" means the whole or any portion or phase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage, or an opportunity to obtain an advantage, over those who do not know or use it. "Trade secret" includes any scientific, technical, or commercial information, including any design, process, procedure, list of suppliers, list of customers, business code, or improvement thereof. Irrespective of novelty, invention, patentability, the state of the prior art, and the level of skill in the business, art, or field to which the subject matter pertains, a trade secret is considered to be:

  (1) Secret;
  (2) Of value;
  (3) For use or in use by the business; and
  (4) Of advantage to the business, or providing an opportunity to obtain an advantage, over those who do not know or use it

  when the owner thereof takes measures to prevent it from becoming available to persons other than those selected by the owner to have access thereto for limited purposes. Uniform Trade Secrets Act—adopted by 46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Not adopted by Massachusetts, New York, North Carolina and Texas.

- **Federal Law**. "Trade secret" means all forms and types of financial business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or

intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(1) The owner thereof has taken reasonable measures to keep such information secret; and
(2) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

Economic Espionage Act of 1996 ("EEA")—18 U.S.C. §1831, *et seq.*

c. Factors Used in Evaluating Whether Information Constitutes a Trade Secret:

(1) The extent to which the information is known outside the claimant's business.

(2) The extent to which it is known by employees and others involved in the business.

(3) The extent of measures taken by the claimant to guard the secrecy of the information.

(4) The value of the information to the business and its competitors.

(5) The amount of effort or money expended by the business in developing the information.

(6) The ease or difficulty with which the information could be properly acquired or duplicated by others.

Restatement of Torts §757, comment b; *Harvard Apparatus, Inc. v. Cohen*, 130 F. Supp. 2d 161 (D. Mass. 2001); *Basic Am, Inc. v. Shatila*, 992 P.2d 175 (Idaho 1999)

QUESTION 2: What are the ethical responsibilities of a lawyer who provides evidence of a client's financial wrongdoing within the regulatory framework of Sarbanes-Oxley and Dodd-Frank?

A. 17 C.F.R. PART 205:

1. **Standards of Professional Conduct for Attorneys Appearing and Practicing Before the Commission in the Representation of an Issuer**

   With regards to Sarbanes-Oxley in particular, there are specific regulations controlling the professional conduct of attorneys with respect to the regulatory framework of the act. SOX specifically states that the regulations are to be the minimum required and that states are not prevented from requiring even more stringent standards. It also states that where the regulations conflict with state ethics requirements, the SOX regulations control.

   The regulations generally require:

   - If an attorney becomes aware of evidence of a material violation by the issuer or by an officer, director, employee, or agent of the issuer, the attorney must report such evidence to the company's chief legal officer or to both the chief legal officer and the chief executive officer.

   - If the attorney then feels that the chief legal officer or chief executive officer have not provided an appropriate response within a reasonable amount of time (or if the attorney feels it would be futile to report it to the chief legal officer or chief executive officer), the attorney shall report the evidence of a material violation to:

     - The audit committee of the issuer's board of directors;

     - Another audit committee of the issuer's board of directors who are not, in the case of a registered investment company, "interested persons;" or

     - The issuers board of directors.

   (For more detailed requirements, see 17 C.F.R. 205.3 Issuer as client.)

2. **Notably, the Regulations Permit an Attorney to Reveal Confidential Information in Order to Carry Out the Purpose of the Act**:

(d) *Issuer confidences.*
(1) Any report under this section (or the contemporaneous record thereof) or any response thereto (or the contemporaneous record thereof) may be used by an attorney in connection with any investigation, proceeding, or litigation in which the attorney's compliance with this part is in issue.
(2) An attorney appearing and practicing before the Commission in the representation of an issuer may reveal to the Commission, without the issuer's consent, confidential information related to the representation to the extent the attorney reasonably believes necessary:
(i) To prevent the issuer from committing a material violation that is likely to cause substantial injury to the financial interest or property of the issuer or investors;
(ii) To prevent the issuer, in a Commission investigation or administrative proceeding from committing perjury, proscribed in 18 U.S.C. 1621; suborning perjury, proscribed in 18 U.S.C. 1622; or committing any act proscribed in 18 U.S.C. 1001 that is likely to perpetrate a fraud upon the Commission; or
(iii) To rectify the consequences of a material violation by the issuer that caused, or may cause, substantial injury to the financial interest or property of the issuer or investors in the furtherance of which the attorney's services were used

QUESTIONS 3: What are the ethical responsibilities of a lawyer who wants to engage in surveillance of a client? Why might employment attorneys wish to monitor employees and/or applicants?

A. EVIDENCE TO SUPPORT EMPLOYMENT DECISIONS

Perhaps most significantly, employment attorneys may monitor employees' e-mails, telephone conversations and even their movement to develop evidence to support adverse employment decisions. An employer may view an employee's Facebook page and discover that the employee was really at an amusement park on a day they called in sick or find in a comment or a post that the employee is violating one of the employer's policies while at work (e.g., a tweet saying "took a one hour nap in the supply room again today"). Employers may also discover potential breaches of contract such as current or ex-employees engaging in competition or violating non-solicitation agreements. Further, employers may find after-acquired evidence of a legitimate, non-discriminatory reason to take an adverse action against an employee once the employee has threatened or commenced litigation.

1. **Recruiting**. According to the New York Times, 75% of recruiters are required by their companies to perform online research on potential candidates, including sites like Facebook, MySpace, LinkedIn and Twitter.[4] An employer may observe problematic behavior by applicants such as pictures of the individual engaged in illegal acts.

2. **Monitoring**. Employers may use surveillance to monitor the job satisfaction of its workforce, perhaps in order to try to prevent attempts at unionization.

B. HOW MIGHT EMPLOYMENT ATTORNEYS WISH TO PERFORM SURVEILLANCE OF EMPLOYEES?

1. **Monitoring E-mail and Servers**. One of the most common ways employers perform surveillance on their employees is through monitoring the employees' e-mail (intra-office instant messages, etc.). Quite simply, this allows employers to see what their employees are talking about and with whom.

2. **Monitoring Cell Phones**. Technologies exist that allow employers to monitor their employees' locations over the Internet using employer-provided cell phones. As technologies such as these become more affordable, they will be more widely used by

[4] Preston, Jennifer. "Social Media History Becomes a New Job Hurdle" The New York Times. July 20, 2011. http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?pagewanted=1&_r=2&ref=technology.

employers. Further, monitoring voicemail messages, telephone numbers to which calls were made and from which calls were received, and text messages, allows employers to see what type of activity their employees are engaged in.

3. **Monitoring Internet Usage**. Employers may monitor *how* employees use their computers, the websites they visit, the amount of time they spend on those sites and the images they view. Monitoring Internet usage may inform an employer than an employee is spending large portions of their day playing online games instead of working or even when an employee is committing criminal acts on company property such as viewing child pornography.

4. **Monitoring Employees' Social Media**. In 2009, the city of Bozeman, Montana made news by requiring applicants to "Please list any and all, current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc." The form also asked for the applicant's user names, log-in information and passwords. While no lawsuits were filed, after much public criticism of the policy, the city eliminated the requirement.

5. **Keystroke Logging Monitoring**. Keystroke logging software can be used to record the actual key strokes on an employee's computer in order to surreptitiously determine what communications employees are having. Additionally, certain key logging programs will also take periodic screen shots and save them to a server or remote hard drive so that employers can monitor which websites employees are using. Such devices, while used by some employers, are legally questionable to say the least. Some courts have held that keylogging software violates the ECPA by intentionally intercepting electronic communications without authorization.

6. **Radio Frequency Identification ("RFID")**. Use of RFID technology is increasing in the workplace. RFID allows employers to place incredibly small "tags" on items or people, or even implant them. RFID tags are most commonly attached to ID badges and security cards to grant access to secure areas. However, the tags can also be monitored wirelessly to track employee behavior. For instance, employers may track how long it takes an employee to perform a certain task, when the employee arrives to and departs from work, or where in the building (or the city) an employee is located. The RFID tags can also be tied to databases containing information about the individual such as name, age, address, phone number, eye color, fingerprints, blood type, full medical history, etc.

7. **Global Positioning Systems ("GPS")**. Many employers with employees who drive as part of their duties use GPS to track such employees' movements. GPS data can be key evidence as it can establish the whereabouts of a party which may be determinative of factual disputes regarding a person's whereabouts.

C. WHAT ARE THE ETHICAL ISSUES ASSOCIATED WITH AN ATTORNEY PERFORMING SURVEILLANCE OF A CLIENT?

1. **On the Job**. With respect to client surveillance in the workplace or on employer-provided property, the large majority of jurisdictions hold that surveillance is allowed when the employee is provided full notice that the employer reserves the right to engage in the surveillance, e.g., a written electronic communications policy.

2. **Off the Job**. With respect to client surveillance through electronic means *outside* the workplace:

   a. Surreptitious or Deceptive "Friending." In 2009, the Philadelphia Bar Association's Professional Guidance Committee (the "Committee") issued an opinion regarding an attorney's proposed method of gaining access to a witness's Facebook and MySpace accounts. The attorney deposed the witness and found out the witness maintained Facebook and MySpace accounts. Believing that the witness might be posting useful information relevant to her deposition on these websites, the attorney visited her Facebook and MySpace accounts and attempted to gain access. However, the attorney discovered that he would have to "friend" the witness who could then decide whether to grant him access or not. The attorney believed that if he identified himself and asked the witness to "friend" him, she would deny his request. Therefore, the attorney sought the Committee's opinion as to whether the following proposed course of action would violate any ethical rules. The attorney proposed that he would ask a third person, a person whose name the witness would not recognize, to go to her Facebook and MySpace pages and ask her to "friend" him. The person would state only truthful information to the witness, i.e., his real name, but would not reveal that he is affiliated with the attorney. If the witness "friended" the third person, the third person would provide the attorney with the information the witness was posting on her Facebook and MySpace pages.

      The Committee found that the attorney's proposed course of action could violate various state ethics rules. For example, the Committee found that that proposal could violate Rule 8.4 (Misconduct) because it is inherently deceptive as the plan purposely omits the key fact to the witness that the third party is only seeking to "friend" her so that he can obtain information for the attorney. The Committee found that the proposal could also violate Rule 4.2 (Communication with Person Represented by Counsel), 4.3 (Dealing with Unrepresented Person), Rule 4.1 (Truthfulness in Statements to Others); and 5.3 (Responsibilities Regarding Nonlawyer Assistants). The Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (March 2009).

      The New York State Bar is in agreement with the Philadelphia Bar Association's opinion. New York State Bar Ass'n, Formal Op. 843 (Sept. 10, 2010)(echoing the opinion of the Philadelphia Bar). *See also* Carole J. Buckner, *Ethical Informal Discovery of Social Media*, Los Angeles County Bar Association County Bar Update,

Vol. 31, No. 5 (May 2011). (Citing Philadelphia opinion and advising "Lawyers must proceed with caution when conducting informal discovery of social networking sites, restricting such efforts to truthful requests to nonparties to avoid ethical perils."); Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, Minnesota State Bar Association Bench & Bar of Minnesota, Vol. 66, No. 10 (November 2009). (Citing Philadelphia opinion and advising that, while attorneys can and should engage in informal social media discovery, they should be mindful of the ethical limitations imposed by duty to avoid deception.)

Similarly, in *Pietrylo v. Hillstone Rest. Group*, 2008 U.S. Dist. LEXIS 108834 (D. N.J. July 25, 2008), motion for new trial denied by *Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS 88702 (D. N.J., Sept. 25, 2009), an employee of Houston's Steakhouse created a MySpace page and stated that its purpose was to operate as a place to "vent about any BS we deal with [at] work without any outside eyes spying in on us." The page touted, "This group is entirely private, and can only be joined by invitation" and "[l]et the s**t talking begin." At some point a Houston's manager asked one of the members of the group to provide her MySpace password so that he could access the group. The employee stated that she gave him the password because she feared she would get in trouble if she did not. The plaintiffs claimed that Hillstone violated the SCA when it accessed the group without authorization and the jury agreed.

b. Oregon State Legal Ethics Comm., Formal Ops. 2005-164 (August 2005) and 2005-173 (August 2005). However, the Oregon State Bar seemingly takes a different view on the permissibility of "misrepresentation and subterfuge" by attorneys.

In an August 2005 opinion addressing ethically permissible conduct by an attorney with respect to an adversary's website, the Oregon Bar states that information on publicly available websites, or even websites for which a membership or subscription is required, is fair game because it is no different than "reading a magazine article or purchasing a book written by the adversary." The opinion warns, however, that you may not communicate through the Internet with a represented adversary, as doing so would violate a lawyer's ethical duty.

Significantly, in footnote 1 of the opinion, the Bar writes, "[w]e express no opinion concerning access to Web sites involving or obtained through the use of deception. *Cf.* OSB Formal Ethics Op No 2005-173."

A review of the opinion referenced in footnote 1 shows that the Oregon Bar rules, like the Model Rules, prohibit an attorney from engaging in "conduct involving dishonesty, fraud, deceit or misrepresentation that reflects adversely on the lawyer's fitness to practice law[.]" However, unlike the Model Rules, the Oregon Bar rules further state:

> [Notwithstanding certain provisions of the Oregon Code] it shall not be professional misconduct for a lawyer to advise clients or others about or

> to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer's conduct is otherwise in compliance with these Rules of Professional Conduct. **"Covert activity," as used in this rule, means an effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge. "Covert activity" may be commenced by a lawyer or involve a lawyer as an advisor or supervisor only when the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future.**

The Oregon Bar interprets this to mean that the lawyer must have some rational basis for his belief that an "unlawful activity" has, is or will take place. An "unlawful activity" is defined as "violations of civil law, criminal law, or constitutional rights." Further, it states that civil law "clearly encompasses both statutory and common-law duties, including duties imposed by tort or contract law. 'Civil law' duties regulate both intentional violations and reckless or negligent breaches of civil standards. It is not, however, reasonable to conclude that a 'violation' of 'civil law' refers to a situation in which no breach of any recognized duty is evident or alleged."

The opinion suggests that, so long as the attorney has a rational basis to believe the investigation relates to unlawful conduct and so long as they do not otherwise violate the Rules of Professional Conduct (for example, by friending a represented party and thereby "communicating" with them in violation of the rules), he or she may use "misrepresentations and subterfuge" to try to obtain informal discovery.

3. Other Potential Dangers With Electronic Surveillance.

a. Potential Violation of State and Federal Laws:

- **Fair Credit Reporting Act**. The Fair Credit Reporting Act ("FCRA") requires that employers notify applicants if consumer reports will be used in an employment decision. The statute provides that in general, "a person may not procure a consumer report, or cause a consumer report to be procured, for employment purposes with respect to any consumer," unless

  (1) a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and
  (2) the consumer has authorized in writing (which authorization may be made on the document referred to in clause (i)) the procurement of the report by that person.

A "consumer report" means any written, oral, or other communication of **any** information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, **character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for … employment purposes.**

"Employment purposes" means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

The FCRA is typically inapplicable because employers tend to do their own searches of social media sites. However, if an employer were to employ an outside firm, or a "consumer reporting agency" such as Info Check USA, to research the candidate's social networking profiles, the FCRA may require that the candidate is first given notice.

Noncompliance with the FCRA can result in civil penalties including a $1,000 fine, punitive damages and the award of attorney's fees and costs.

- **The Stored Communications Act**. The Stored Communications Act or "SCA," 18 U.S.C. §2701, *et seq*., prohibits intentionally accessing stored communications without authorization or in excess of authorization which, again, is why a well-drafted communications policy is so important. The SCA provides for a cause of action to remedy conduct constituting a violation. Those remedies include preliminary and other equitable and declaratory relief as may be appropriate, actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages where appropriate (for willful or intentional violations), a reasonable attorney's fee and other litigation costs reasonably incurred. The SCA also states that in no case shall a person entitled to recover receive less than the sum of $1,000. 18 U.S.C. §2707. In addition, there are possible criminal penalties including a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b).

- **Other Laws Discussed *Supra***:

  - The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030

  - The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §2510, *et seq*. (a/k/a the Federal Wiretap Act)

  - State Wiretap Statutes

b. If Used for Hiring or Employment Decisions There is the Potential for Discrimination. A potential employer can discover a wealth of information about an applicant, which they would not normally have, from various social media profiles including:

- Age
- Religious Beliefs
- Sexual Orientation
- Memberships/Affiliations
- Political Associations
- Marital Status
- Whether They Have Children

An employer could use this information to discriminate against an applicant for an unlawful purpose, or, even if the employer does not use the information, an applicant who was denied a position could still allege that they *did* use it. See the case of *C. Martin Gaskell v. University of Kentucky*, No. 5:09-cv-00244-KSF (E.D. Ky. 2009)(no decision, settled out of court in January 2011) (Gaskell was the most qualified applicant for an astronomy position with the university. However, after one of the members of the hiring committee performed an Internet search on Gaskell and discovered certain of his religious beliefs, the university decided not to hire Gaskell, despite his superior qualifications, because of his religious beliefs. Gaskell brought suit and received a $125,000 settlement.)

c. Information Learned May Be False. An employer cannot be guaranteed that the information it receives from Internet sources is accurate. Potential candidates' profiles could contain undeserved glowing recommendations or harsh criticisms from friends and foes alike. Further, the person they describe themselves as online may not be an accurate portrayal of their true character; giving employers a false sense of familiarity with the candidate's true nature.

Note: The New York City Bar Association, Committee on Professional Ethics recently released a Formal Opinion 2012-2 addressing lawyers' research of jurors. The panel concluded that even *inadvertent* communication with a juror or prospective juror (e.g., viewing a juror's LinkedIn page, causing the juror to receive a notification that "John Attorney viewed your profile") may violate ethics rules prohibiting communication with jurors.

QUESTION 4: What are the ethical responsibilities of a lawyer who stumbles onto evidence of client perjury on the Internet?

A. PERJURY

1. **When A Lawyer May, Must, or Must Not Disclose Perjury to a Tribunal.** ABA Model Rules 1.6, 3.3(a)(1), (a)(3), (b), and (c) are pertinent to this question.

   a. Rule 3.3:

> (a) A lawyer shall not knowingly:
> (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
> • • •
> (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
> (b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.
> (c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply **even if compliance requires disclosure of information otherwise protected by Rule 1.6.**

Under this rule, followed by 44 states, a lawyer who "comes to know of" the falsity of the client's testimony "shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal." See *Feld's Case*, 815 A.2d 383 (N.H. 2002)(where the New Hampshire Supreme Court suspended a lawyer for one year for failing to advise his client to correct false deposition testimony.)

There is some variation even among the states that follow the Model Rules. For instance, in Texas, the attorney is required to first try to convince the client to correct the perjury his or herself. If the client refuses, the attorney is then required to disclose the perjury to the tribunal. Rule 3.03(2). In Virginia, not only is the lawyer required

to disclose the perjury to the tribunal, but he is also required to seek to withdraw as counsel. Rule 1.6(c)(1). In Pennsylvania, the obligation to disclose matters applies only to that information the lawyer learns while the matter is ongoing, and not to that information learned after the matter is closed. Philadelphia Bar Ass'n Professional Guidance Committee, Opinion 2001-2 (March 2001). For a comprehensive analysis of the general guiding principles and "reasonable remedial measures" in those states that follow the Model Rules, see the Colorado Bar Association Ethics Opinion 123: Candor to the Tribunal and Remedial Measures in Civil Proceedings. A copy of the opinion can be found at http://www.cobar.org.

There are however a handful of jurisdictions that do not follow the Model Rules. Tennessee stands alone as the only jurisdiction that requires the attorney to first consult the client on the consequences of engaging in or failing to correct the perjury, and then to seek withdrawal of representation, telling the court only that their withdrawal is required by the Rules of Professional Conduct and disclosing no information protected by Rule 1.6.

Five other states—California, New York, North Dakota, Oregon, and Washington—and the District of Columbia depart from the Model Rules. Of those jurisdictions, California, New York, Oregon and Washington rules require plainly that an attorney must not disclose perjury by his client if doing so would involve disclosing information protected by Rule 1.6. The District of Columbia allows that a lawyer *may* make such a disclosure, but only if the client's perjury is reasonably certain to result in substantial injury to the financial interests or property of another or to mitigate or rectify the same. Finally, North Dakota rules require that in the case of perjury by a client, the lawyer must try to convince the client to consent to disclosure. If the client will not consent, the lawyer needs to seek withdrawal from representation. If withdrawal is not allowed, the lawyer should continue representation, but not use or argue the client's false testimony.

Even among the states that "agree", there are minor variations in the language of the rules. Certain jurisdictions rely on the language prohibiting a lawyer from failing to disclose "a material fact to a tribunal when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client." Others rely on language stating, "if a lawyer has offered material evidence and thereafter comes to know of its falsity, the lawyer shall take reasonable remedial measures." Finally, the clearest language states, "[i]f a lawyer, the lawyer's client, or a witness called by the lawyer has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable and timely remedial measures, including, if necessary, disclosure to the tribunal."

If a lawyer "stumbles onto" evidence of client perjury, it would be difficult to argue that the lawyer has not "come to know of" the falsity of his client's statement. In states deciding "[i]f a lawyer, the lawyer's client, or a witness called by the lawyer has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take

reasonable and timely remedial measures, including, if necessary, disclosure to the tribunal," the lawyer would undoubtedly have an obligation to take remedial measures and, if necessary, disclose the perjury to the court.

Similarly, in states prohibiting a lawyer from failing to disclose "a material fact to a tribunal when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client," the lawyer has a duty not only to disclose perjury by the client, but perhaps even by those with a sufficient relationship to the client.

- *United States v. Shaffer Equip. Co.*, 11 F.3d 450, 461 (4th Cir. 1993)("Since Caron was involved in the case as an important agent of the EPA and his misrepresentation was made in the course of his employment with the EPA with the effect of disguising a weakness in the EPA's case, his action is fairly characterized as an act of the EPA.")

B. IS INFORMATION AVAILABLE ON THE INTERNET "CONFIDENTIAL" OR "SECRET"?

Ironically enough, the lawyers who need to be the *most* careful about their ethical responsibilities when stumbling upon evidence of client perjury may be those who seem to have the *least* duty.

1. Take the District of Columbia for example, whose pertinent rule states:

> Rule 3.3
> (a) A lawyer shall not knowingly:
> (1) Make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer, unless correction would require disclosure of information that is prohibited by Rule 1.6.

Rule 1.6 generally protects "confidences" and "secrets" which are defined by the D.C. Bar as:

> "Confidence" refers to information protected by the attorney-client privilege under applicable law, and "secret" refers to other information gained in the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing, or would be likely to be detrimental, to the client.

- Let's say the D.C. lawyer's client testified that he stayed home from work on May 5, 2012 because the harassment at the office was so severe he was too depressed to get out of bed. Subsequent to his client's testimony, the lawyer is viewing the <u>public</u> portions of his client's Facebook page and sees a photo of his client wearing a sombrero

and drinking a Mexican beer, smiling from ear to ear, with his arms around two of his best friends, on the outside patio of a local Mexican restaurant in the middle of the day. The photo is time and date stamped 05/05/12 2:30 PM. One of the client's friends has commented on the photo, "this year's cinco de mayo party was better than last year's, or any of the 10 before that, it was great to see you."

- What is the D.C. lawyer's ethical responsibility in this situation? Is the picture on Facebook and the attendant's comment a "confidence" or "secret"?

  a. The information ***is not*** protected by the attorney-client privilege and therefore **is not** a "confidence."
  b. The information **was** gained in the professional relationship and the disclosure of the information **would be** embarrassing or likely detrimental to the client and therefore the information could be classified as "secret".

- However, can the lawyer argue in good faith that the information—which is posted on the Internet and available for anyone in the world with an Internet connection to view—is truly "secret"? Can the lawyer argue in good faith that correcting the false testimony would involve "disclosure"? Can the lawyer "disclose" something that is readily known to the world?

2. Oregon rules present an even greater complexity. Rule 3.3(a)(3) states, "If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if permitted, disclosure to the tribunal." That is straightforward enough.

   - Further, Rule 3.3(b) states, "A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if permitted, disclosure to the tribunal." Again, the rule seems clear.

   - However, Rule 3.3(c) states, notwithstanding sections (a) and (b), "in no event" may a lawyer disclose information otherwise protected by Rule 1.6. Turning to Rule 1.6 the lawyer finds "(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)."

   - Using the same factual scenario with D.C. lawyer above, is the cinco de mayo photo "information relating to the representation of a client"? Assuming that it is, in complying with his duties under 3.3(a) and (b), would the Oregon lawyer be "revealing" the information? Can you "reveal" something that is readily known to the world?

- In addition, under 1.6(b)(5), the Oregon lawyer may reveal information relating to the representation of a client "to comply with other law, court order, or as permitted by these Rules." So assuming that the information is related to the representation and assuming the disclosure to the court *would* be "revealing" the information, is the Oregon lawyer nonetheless permitted to disclose the information to avoid becoming an "accessory to perjury" (if such a thing even exists)?

3. Practical Advice:

- The reality is, even in states where you arguably do not have a duty to correct the perjury or inform the tribunal, in the best-case scenario your failure to do so will force you to fashion an argument based on linguistic maneuvering as to why you did not have a duty to inform the tribunal that you knew a fraud had been committed upon it. That is a tough position to be in.

- State bar ethics rules aside, courts understandably frown upon lawyers knowingly allowing their clients to present false evidence.

    - *Shockley v. Kearney*, 1996 U.S. Dist. LEXIS 10939 (D. Del. July 25, 1996)(quoting *Nix v. Whiteside*, 475 U.S. 157, 168-169 (1986)("The legal profession has accepted that an attorney's ethical duty to advance the interests of his client is limited by an equally solemn duty to comply with the law and standards of professional conduct; it specifically ensures that the client may not use false evidence. This special duty of an attorney to prevent and disclose frauds upon the court derives from the recognition that perjury is as much a crime as tampering with witnesses or jurors by way of promises and threats, and undermines the administration of justice.") *Lafler v. Cooper*, 132 S. Ct. 1376, 1387 (2012)(same).

- Read your own state's rules carefully though. In California for instance, you almost certainly will be in violation of the rules of professional conduct if you disclose your client's perjury to the court.

QUESTION 5: What is a lawyer's duty not to violate client confidentiality in the electronic era?

A. MODEL RULES OF PROFESSIONAL CONDUCT APPLICABLE TO KEEPING CLIENT CONFIDENTIALITY

1. **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."

   - On August 7, 2012, the ABA House of Delegates amended the commentary of Rule 1.1 as follows: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

   - The reason for the amendment to the rule was to make clear that a lawyer's obligation to keep up on changes in law and practice includes changes to technology and the pros and cons of same. "The [] amendment emphasizes that a lawyer should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent in a digital age."

2. **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).

   (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

   (1) to prevent reasonably certain death or substantial bodily harm;

   (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

- The ABA recently approved an amendment to Rule 1.6 to add a subpart (c), which reads as follows:

  "**(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."**

  The amendment makes it clear for lawyers that they have an ethical obligation to "take reasonable measures to protect" confidential client information and communications from inadvertent disclosure or unauthorized access without regard to the medium. It also provides factors for lawyers to consider in determining the reasonableness of their safeguards for electronically stored communications and/or confidential client information. These factors include the "sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients."

  Significantly, the commentary to the amended rule emphasizes that a lawyer does not violate Rule 1.6 merely for unauthorized access to such information by third parties or because of inadvertent disclosures.

3. **Rule 5.3 Responsibilities Regarding Non-Lawyer Assistants**. With respect to a non-lawyer 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

efforts 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 non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action."

- The ABA also amended the commentary of this rule as well on August 7, 2012. The purpose of the revised commentary was to explain that use of non-lawyers outside of the firm can have ethical issues, including breaches of confidentiality. This is important in the technology sense especially where lawyers use outside vendors for technological services, such as for printing, scanning or using Internet-based services to store information. The commentary emphasizes that a lawyer has an obligation to make reasonable efforts to ensure that those outside services are provided in a manner that is consistent with the lawyer's ethical and professional obligations. It goes further and provides that the lawyer "should communicate directions appropriate under the circumstances to give reasonable assurance that the non-lawyer's conduct is compatible with the professional obligations of the lawyer."

B. OPINIONS ON ETHICAL CONSIDERATIONS

1. **Using Public Wireless Connections**. An attorney runs the risk of violating his or her duty of confidentiality and competence when using a public wireless connection, such as in a coffee shop, unless the attorney takes appropriate precautions to protect confidential information and avoid inadvertent disclosure (i.e. firewalls, encryption). California Bar Opinion No. 2010-179.

2. **Using Public Devices or Other Storage Media**. Lawyers using shared devices or public devices, such as copiers, printers, scanners or fax machines (for example, at hotels), must take reasonable steps to protect confidential information and properly sanitize storage devices to prevent the inadvertent disclosure of confidential information. For an in-office copier and/or scanner, the lawyer must remove or delete all confidential information from the device's hard drive before disposition. However, when using public devices, the lawyer should determine whether the devices can preserve confidentiality. If it cannot, the

lawyer runs the risk of inadvertently disclosing attorney-client confidential information. Florida Bar Opinion, 10-2 (Sept. 24, 2010).

3. **Using E-mail to Communicate with Clients**. The primary focus is to caution employees not to use their employer's e-mail systems or business computers when engaging in confidential communications so as to prevent access to such information by third parties. If a lawyer learns that an employee is using an employer's e-mail system, the lawyer should inform the client about the potential risks of waiver of attorney-client privilege and inadvertent disclosure to third parties of confidential communications. The opinion even goes as far as to suggest that if a lawyer learns that the client is not heeding the lawyer's advice about refraining from using employer devices, the lawyer should discontinue electronic communication with the client. ABA Formal Opinion 11-459 (Aug. 4, 2011).

4. **Using Organization Listserv or Other Electronic Source Used to Consult with Other Attorneys**. Lawyers who consult with other lawyers through legal organization listservs or other electronic sources where the consulted lawyers are not members of the consulting lawyers firm must ensure not to breach Rule 1.6 on confidentiality. Inherently, Rule 1.6 allows an attorney to consult with other attorneys where the lawyer "reasonably believes the disclosure will further the representation by obtaining the consulted lawyer's experience or expertise for the benefit" of the client. The ABA cautions that such consultations can create unforeseen ethical issues. In order to avoid breaches of confidentiality, the ABA Opinion suggests that lawyers consulting with outside lawyers use hypothetical situations to avoid providing any identifiable real situations or real client information. The ABA also suggests getting client consent to share certain information with consulted lawyers. One way to get consent from clients is to expressly obtain consent in retainer agreements in which the clients are expected to sign for representation. It is wise to also ensure that lawyers avoid consulting with a lawyer who may represent the adverse party. Another way to protect confidentiality of client information when consulting with other lawyers is to get an express agreement from the consulted lawyer that they will keep the information confidential. When using listservs, organizations should draft the rules governing the listserv to include confidentiality and all members who participate in the listserv must acknowledge and agree to keep the information confidential.

   However, consulting with other lawyers can bring up ethical issues for the consulted lawyer. For example, the consulted lawyer must take caution not to give advice that may be adverse to the consulted lawyer's existing clients. Also, conflict of interest issues can arise for the consulted lawyer. The ABA recommends attempting to get the consulting lawyer to sign a conflicts waiver or screening to avoid disqualification of other members of the consulted lawyer's firm. Lastly, the consulted lawyer should confirm the confidentiality of the information, if not asked to keep the information confidential or it is not of the nature in which any reasonable lawyer would know that the information should be kept confidential. Otherwise, the consulted lawyer does not breach Rule 1.6 if the consulted lawyer subsequently uses or discloses the information. ABA Formal Opinion 98-411 (August 30, 1998).

5. **Digging out Metadata May Raise Ethical Concerns**. The ABA issued an opinion in 2006 indicating that there was no specific prohibition against lawyers vetting out metadata from electronic documents received from an adversary party, opposing counsel or other agent of the adverse party. ABA Formal Opinion 06-442 (August 5, 2006). However, there are numerous states that prohibit an attorney from drawing out metadata and using it. (Alabama, Arizona, Florida, Maine, New Hampshire, New York, North Carolina, Washington, D.C. and West Virginia). There are other states that find it acceptable to dig out metadata and use it. (Colorado, Maryland, Oregon, Vermont and Washington). The ABA has collected this information and provided it on its website, See Metadata Ethics Opinions Around the U.S., A.B.A. Law Practice Management Section. Leg. Tech. Resource Center, available at: www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

6. **Reading a Judge's Text Messages Could Land You in Ethics Classes**. Two lawyers (prosecutor and defense attorney) in Corpus Christi were ordered to attend ethics classes after they inappropriately read a text message on the judge's phone. The defense lawyer contended that he picked up the judge's phone, inadvertently mistaking it for his own. He commented that "almost all of us have phones that look identical." However, the court did not buy the argument and ordered both lawyers to complete a certain amount of hours of ethics courses before being allowed to appear in the judge's courtroom again.

DISCLAIMER

The information provided in these materials was accurate at the time written. The Sass Law Firm makes no assurance that the laws, statutes, rules, regulations or ordinances referenced herein have not been changed, amended or rescinded. Additionally, relevant new case law may have been recently published.

These materials are being made available for informational purposes only and are not to be relied upon as legal advice.

If you have an employment law question,
we urge you to seek legal counsel.

Thank you.

SASS LAW FIRM