Amendments to the Pennsylvania Rules of Professional Conduct

From Parchment Files to Digital Document Management:

The Latest Changes to the Pennsylvania Rules of Professional Conduct Reflect the Technological Transformation of the Practice of Law

Jonathan W. Hugg
Stephanie K. Rawitt
Karolien M. Vandenberghe

Philadelphia, March 18, 2014

CLARK HILL

CYBERSECURITY FOR LAWYERS

The New York Times

Spying by N.S.A. Ally Entangled U.S. Law Firm

By JAMES RISEN and LAURA POITRAS FEB. 15, 2014

The list of those caught up in the global surveillance net cast by the National Security Agency and its overseas partners, from social media users to foreign heads of state, now includes another entry: American lawyers.

A top-secret document, obtained by the former N.S.A. contractor Edward J. Snowden, shows that an American law firm was monitored while representing a foreign government in trade disputes with the United States. The disclosure offers a rare glimpse of a specific instance in which Americans were ensnared by the eavesdroppers, and is of particular interest because lawyers in the United States with clients overseas have expressed growing concern that their confidential communications could be compromised by such surveillance.

CYBERSECURITY MATTERS

Bloomberg News

China-Based Hackers Target Law Firms to Get Secret Deal Data

By Michael A. Riley and Sophia Pearson | February 08, 2012

SEND TO kindle

(Updates with IT officer's comment in 16th paragraph.)

Jan. 31 (Bloomberg) -- China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.

LAW360
A LexisNexis® Company

Law360, San Francisco (August 09, 2013, 9:47 PM ET)

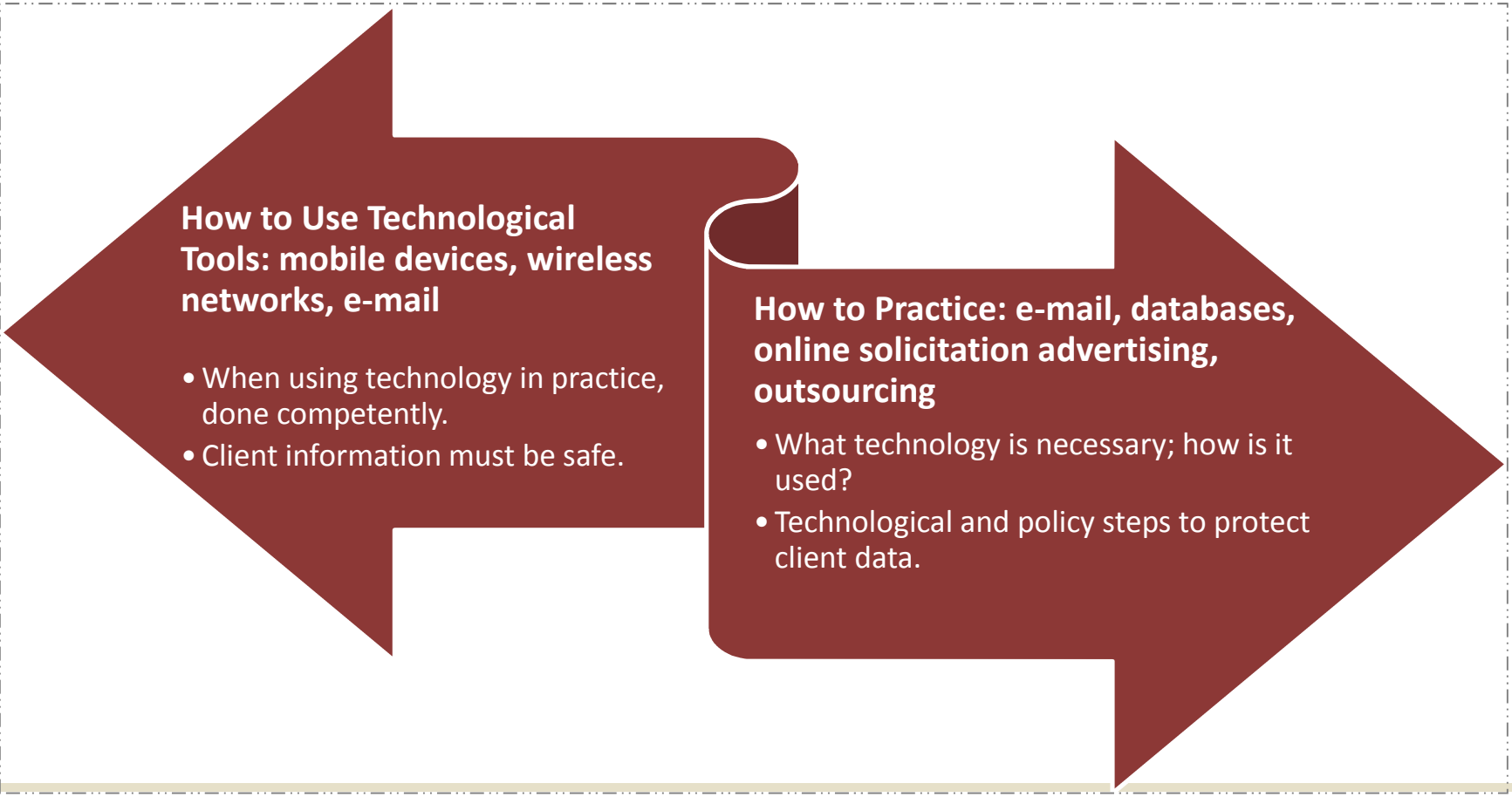
Big Law Firms Are Most Vulnerable To Hackers: ABA Panel

By Beth Winegarner

"Expanded Duty of Competence
Previously, the duty of competence focused primarily on the lawyer's knowledge of the areas of substantive law and the experience necessary to represent the client in the particular engagement. This technology shift has now made that insufficient."

San Diego County Bar Association, Legal Ethics Opinion 2012-1

ABA'S COMMISSION ON ETHICS 20/20: HOW GLOBALIZATION AND TECHNOLOGY ARE TRANSFORMING THE PRACTICE OF LAW



TECHNOLOGY TRANSLATED INTO ETHICS

Use of Technology / Tools Outside of the Office

- Work / Personal
- Don't use unsecured wireless for work related e-mails
- Don't connect remotely over unsecured, public networks
- Be careful with USB ports (malware or spyware)

Use of Technology in the Office/ in Representation

- Minimum of knowledge of technology in order to provide services competently while using these tools
- Duty of confidentiality to the client implies cybersecurity measures and firm policies

Ethical Rules

Competence
Confidentiality

PBA'S RECOMMENDATIONS

- **PBA Legal Ethics and Professional Responsibility Committee, September 2012:**
  - recommend proposed amendment to PA Rules of Professional Conduct
  - adoption of ABA Model Rules amendments of August 2012
    - promote consistency, unless controlling PA precedent or important policy

OVERVIEW: RULES

Rule 1.1 Competence: Comments were changed

- digital competence
- outsourcing

Rule 1.6 Confidentiality: Black letter and comments were changed

- prevent inadvertent disclosure / unauthorized access
- conflict checks during merger talks

Rule 4.4 Respect for Rights of Third Parties: Black letter and comments were changed

- notification obligation when receiving inadvertently sent information, also ESI

Rule 5.3 Use of Nonlawyers Outside the Firm: Comments were changed

- outsourcing

RULE: COMPETENCE INCLUDES DIGITAL COMPETENCE

PA Rule1.1 Competence

- A lawyer shall provide competent representation to a client.
- Legal knowledge, skill, thoroughness and preparation reasonably necessary.

Comment 8

- "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 (emphasis supplied)."

ABA COMMISSION'S REPORT ON DIGITAL COMPETENCE, ADOPTED BY PBA

In order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology.

E.g., a lawyer will have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.

Comment 8 already encompasses an obligation to remain aware of changes in technology that affect law practice.

- Making obligation explicit offers greater clarity, *emphasizes importance of technology to modern law practice*.
- Not new; reminder: remain aware of technology, including benefits and risks, as part of a lawyer's ethical duty to remain competent.

RULE: CONFIDENTIALITY OF INFORMATION

PA Rule1.6 Confidentiality of Information

- "(d): 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 (emphasis supplied)."

COMMENT: REASONABLE EFFORTS TO PREVENT ACCESS OR DISCLOSURE

Comment 25 to PA Rule 1.6 Confidentiality of Information

- Act competently to preserve confidentiality
- Reasonable efforts to prevent access or disclosure?
- Some factors:
  - Sensitivity of the information
  - Likelihood of disclosure if no additional safeguards
  - Cost of additional safeguards
  - Difficulty of implementing additional safeguards
  - Extent to which safeguards adversely affect ability to represent client
    - e.g., by making device or software excessively difficult to use
- Client's requirements - special security / Client's consent - forgo reasonable security measures

Conclusion

- What is reasonable depends on the circumstances
- Client may override; follow instructions
- Other laws may impose additional requirements (data privacy) or obligations:
  - e.g., HIPAA (privacy and security of health information)

PREVIOUS ETHICS OPINIONS: NEW YORK STATE BAR OPINION 782 (2004)

- Exercise reasonable care: ensure that confidential information is not inadvertently disclosed by e-mail.
- Act reasonably: assess risks involved in using technology to determine if the mode of transmission is appropriate under circumstances.
- May require to stay abreast of technological advances, learn about risks.
- With regard to necessary degree of care, consider:
  - subject matter of document,
  - whether document was based on template used in other matter for other client,
  - whether there have been multiple drafts with comments from multiple sources,
  - whether client has commented on document, and
  - identity of intended recipients.

- Sensitivity
- Templates
- Drafts
- In line comments
- Recipients

PREVIOUS ETHICS OPINIONS: CALIFORNIA STATE BAR OPINION 2010-179

Factors to consider before using technology

- a) The attorney's ability to assess the level of security afforded by the technology
- b) Legal ramifications to third parties of intercepting, accessing of another person's electronic information
- c) Degree of sensitivity of information
- d) Possible impact on client of inadvertent disclosure of privileged information or confidential information
- e) Urgency of the situation
- f) Client instructions or circumstances

consideration of how the technology differs from other media (e.g., regular mail/e-mail)

- whether reasonable precautions may be taken to increase level of security (e.g., encryption)
- limitations on who is permitted to monitor, to what extent and on what grounds (service providers)
- third party subject to criminal charges /civil claims (e.g., computer fraud)
- the greater the sensitivity, the less the risk one should take
- waiver

- Imminent situation
- e.g., email is checked by others

UNAUTHORIZED ACCESS BY "THIRD PARTIES": THE UNSEEN ONLOOKERS

Technology: Deception of Privacy	Risk: No Reasonable Expectation of Privacy
• e-mailing over public WiFi • accessing client files over hotel connection • clients-employees communicate with attorney from employer's accounts or employer's devices	• = speaking to your client in a crowded room • = reading client information with onlookers • = communicating with the employer present

DUTY TO WARN THE CLIENT

ABA Formal Opinion 11-459 (2011) on Duty to Protect the Confidentiality of E-mail Communications with One's Client

- "A lawyer sending or receiving *substantive* communications with a client via e-mail, text messages, or other electronic means 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 *significant risk* that a *third party* may gain access (emphasis supplied)."

NO DUTY TO NOTIFY EMPLOYEE'S COUNSEL

ABA Formal Opinion 11-460 (2011) on 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, … located in the employee's business e-mail file or 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."

AMERICAN BAR ASSOCIATION
Center for Professional Responsibility

CASES: PRIVACY EXPECTATIONS IN WORKPLACE COMMUNICATIONS

Privilege Maintained

- Nat. Eco. Research Ass., Inc. v. Evans (Super. Ct. Mass 2006)
- Stengart v. Loving Care Agency (Sup. Ct. N.J. 2010)
- Sims v. Lakeside School (W.D. Wash. 2007)
- United States v. Nagle (M.D. Pa. 2010)

Privilege Did Not Attach / Waived

- Kaufman v. Sungard (D.N.J. 2006)
- Long v. Marubeni America Corp. (S.D.N.Y. 2006)
- Sims v. Lakeside School (W.D. Wash. 2007)
- Scott v. Beth Israel Medical Center (N.Y. Sup. Ct. 2007)
- Holmes v. Petrovich (Cal. Ct. App. 2011)
- Chechele v. Sandridge Energy, Inc. (W.D. Okla. 2012)

CASES: LOSS OF THE ATTORNEY-CLIENT PRIVILEGE IN EMPLOYMENT CONTEXT

- Facts:
  - Employees who used employer's account or employer's device to communicate with attorney → loss of the attorney-client privilege
- Attorney-client privilege: "confidentiality anticipated and preserved"

> • "…This was akin to consulting her attorney in one of [employer's] conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard … would be privileged." Holmes v. Petrovich (Cal. Ct. App. 2011).

- Loss of confidentiality:
  - Impact of employer's policy is significant : notice
  - No reasonable expectation of privacy

FACTORS: COMMUNICATIONS IN EMPLOYMENT

Attorney-Client Privilege

attorney

client

communication

confidentiality anticipated and preserved

for the purpose of legal advice

UNITED STATES V. NAGLE (M.D. PA. 2010): REASONABLE EXPECTATION OF PRIVACY

FACTS

Employee made chronology of employment events giving rise to criminal charges at request of attorney on employer's laptop. Saved document in "personal" folder on laptop's drive, not server. Fired, device returned. Document found. CEO wanted to use document.

PRIVILEGE

Employee's counsel raised privilege.

CEO disputed "in *confidence*" prong of privilege: prepared on work computer, others with access, document not labeled 'confidential.'

TEST : FOUR FACTOR TEST

(1) does company maintain a policy banning personal or objectionable use;

(2) does company monitor the use of employee's computer or e-mail;

(3) do third parties have a right to access computer or e-mail; and

(4) did company notify employee, or was employee aware, of the use and monitoring policies?

Asia Global Crossing (Bankr. S.D.N.Y. 2005)

UNITED STATES V. NAGLE (M.D. PA. 2010): REASONABLE EXPECTATION OF PRIVACY CONT'D

FACTORS APPLIED	OUTCOME
1. No policy banning personal use 2. No evidence regarding monitoring 3. No general right of access by third parties 4. Policy existed but employees were not aware of it	The court concluded that employee's belief that in storing the employment chronology on the hard drive of his laptop, issued by his employer, it would remain private was reasonable.

DOMBROWSKI V. GOVERNOR MIFFLIN SCHOOL DIST. (E.D. PA. 2012): REASONABLE EXPECTATION OF PRIVACY

- Privacy claim (4th Amendment), e-mails between plaintiff and counsel, retrieved from laptop, using personal e-mail account but clear employer's policy (no privacy)
- Factors used:
  1. Policy banning personal use?
  2. Monitoring of use of computer and e-mail?
  3. Third parties have right of access?
  4. Notified employee or was the employee aware?
     - Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005)
- Court: no sufficient, reasonable expectation of privacy; denied the privacy claim

INADVERTENT DISCLOSURE OF ESI

PA Rule 4.4 Respect for Rights of Third Persons

- "(b) A lawyer who receives a document, *including electronically stored information*, relating to the representation of the lawyer's client and knows or reasonably should know that the document, including electronically stored information, was inadvertently sent shall promptly notify the sender (emphasis supplied)."

Comment 2

- "A document, including electronically stored information, is inadvertently sent when it is accidentally transmitted, such as when an e-mail or letter is misaddressed or a document, including electronically stored information, is accidentally included with information that was intentionally transmitted."
- "Document includes paper documents, e-mail and other forms of electronically stored information, including embedded data (metadata)."
- Metadata triggers the obligation if the receiving lawyer knows / reasonably should know that the metadata was inadvertently sent.

Comment 3

- Professional judgment: return document or delete ESI.

ABA COMMISSION'S REPORT, ADOPTED BY PBA

Technology increased the risk that confidential information is inadvertently disclosed.

Word "document" is inadequate to express various kinds of information in a digital age: e-mails, flash drives, data embedded in electronic documents.

Replaced with "document or electronically stored information."

If lawyers receive documents that they know/reasonably should know were inadvertently sent, they must *notify* the sender. Not resolved: permitted to look?

Receipt of metadata triggers the notification duties but only when the receiving lawyer knows or has reason to believe the data was inadvertently sent.

WITHDRAWN OPINION

ABA Formal Opinion 06-440 (2006) on Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382

- Withdrawn opinion of 1994:
  - Refrain from reviewing the inadvertently sent document
  - Notify adverse party or counsel
  - Follow adverse party or counsel instructions
  - Refrain from using the information
- Withdrawn because not based on the rules
- No Rule 4.4(b) in 1994

AMERICAN BAR ASSOCIATION
Center for Professional Responsibility

INADVERTENT SENDING OF DATA IN LITIGATION: FED. RULES OF CIV. PROC.

- **Fed. R. Civ. Proc. 26(b)(5)(B):**
  - subject to privilege or work product
  - notify receiving lawyer
  - receiving lawyer must promptly return, sequester or destroy
  - receiving lawyer must not use or disclose the information until claim is resolved
  - must take reasonable steps to retrieve if already disclosed
- **Potential consequence: disqualification**
  - information crucial to defense

INADVERTENT SENDING OF DATA IN LITIGATION: FED. RULES OF EVIDENCE

- **FRE 502(b)**
- **Wise v. Washington County (W.D. Pa. 2013)**
  - First step: privileged?
  - Second step: if so, waived unless three elements are met:
    1. disclosure is inadvertent
    2. holder of the privilege took reasonable steps to prevent disclosure
    3. holder of the privilege promptly took reasonable steps to rectify the error

INADVERTENT DISCLOSURE

- "…, Pennsylvania courts have recognized that 'an attorney receiving confidential documents has ethical obligations that may surpass the limitations implicated by the attorney-client privilege and that apply regardless of whether the documents in question retain their privileged status.' …"
- "It is these principles that underlie the oft-cited protocol directing counsel, upon discovering the confidential nature of documents, to cease review, notify the owner, and abide by the owner's instructions regarding the documents' disposition. …"

Burt Hill, Inc. v. Hassan, 2010 U.S. Dist. LEXIS 7492 (W.D. PA 2010)

OUTSOURCING: COMPETENCE

PA Rule 1.1 Competence

- Retaining or contracting with other lawyers
- New: comment 6 and comment 7

Comment 6

- Reasonable belief: nonfirm lawyer will contribute to competent, ethical representation
- Circumstances: education, experience, reputation; nature of services assigned; legal protections, conduct rules in the jurisdiction of performance, particularly relating to confidential information

Comment 7

- Lawyers from more than one law firm are providing legal services
- The lawyers *should* ordinarily consult with each other and the client

OUTSOURCING: NONLAWYERS OUTSIDE THE FIRM

PA Rule 5.3 Nonlawyer Assistance

- Responsibility: reasonable supervision

Comment 3

- Investigative, paraprofessional services, document management company, printing/scanning by vendor, internet-based service to store client information.
- Make reasonable efforts to ensure that services are provided in a manner that is compatible with lawyer's professional obligations.
- Obligation depends on the circumstances: experience of nonlawyer, *terms regarding confidentiality, legal and ethical environment of the jurisdiction*, particularly regarding confidentiality.

Comment 4

- If client directs selection of service provider: lawyer ordinarily should agree with client on responsibility for monitoring.

CONFLICT CHECKS

PA Rule 1.6 Duty of Confidentiality

- "(c) A lawyer may reveal such information to the extent that the lawyer reasonably believes necessary:
- (7) To detect and resolve conflicts of interest 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."

Comment 19

- Substantive discussions regarding the new relationship have occurred
- Limited to identity of the persons, brief summary of issues, and information about termination
- To the extent reasonably necessary to detect/resolve conflicts
- Prohibited if attorney-client privilege is compromised or prejudice to client

BEST PRACTICE: LAW FIRM POLICY REGARDING CONFIDENTIAL INFORMATION

- Address whether to allow own devices: control / enforcement
- May be preferable to provide firm's devices
- Impose security protocol on all employees, attorneys and staff
- Have technical safeguards
- Educate
- Impose a return policy on all devices
- Destroy all digital information on returned devices
- Test / Enforce the policy

Meetings, paper documents and vaults?

NOTE: CHANGES TO CLE REQUIREMENTS

The Supreme Court of Pennsylvania Continuing Legal Education Board

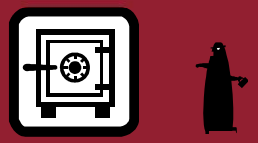
- February 4, 2014: changes to Pa.R.C.L.E. Rule 108(e)
- Increased Ethics Requirement and Distance Learning Options
  - Amount of credits lawyers may earn via alternative delivery:
    - from four (4) to six (6) credit hours annually
    - = half of the total credits required per year
  - Ethics component:
    - from one (1) to two (2) credit hours annually
  - Total remains twelve (12) credit hours
- Effect as of CLE compliance periods with deadlines in 2015

See: https://www.pacle.org/

QUESTIONS?

Jonathan W. Hugg | 215.640.8547
Stephanie K. Rawitt | 215.640.8515
Karolien M. Vandenberghe | 215.640.8536

Clark Hill PLC
One Commerce Square
2005 Market Street, Suite 1000
Philadelphia, PA 19103



CLARK HILL