Davis Wright Tremaine LLP

DEFINING SUCCESS TOGETHER

Legal and Ethical Impacts of Technology on Negotiation, Confidentiality, and Business Operations

DWT In-House CLE Series

May 12, 2010

Embracing Technology

- **Why do we embrace technology?**
  - The promise of improved efficiency and productivity
  - The “cool factor”
  - The ability to protect, manage, or facilitate access to assets
- **But technology puts pressure on traditional models and methods**
  - Efficiency is often the enemy of confidentiality, privacy and security
  - Security and privacy are often at odds
  - Tendency to embrace technology incrementally and without strategic assessment (e.g. IM) which leads to bad habits and unforeseen consequences

Let's Keep it All in Context

- Twenty Eight Years Ago (1982):
  - CDs are invented;
  - Sendmail, an early e-mail program is invented
  - Only obnoxious Wall Street types have mobile phones and they are the size of bricks
  - IBM introduced its first desktop PC
  - Fax machines just beginning widespread acceptance
  - FedEx implements "overnight letter" service

- Fifteen Years Ago (1995):
  - The Mosaic browser released (Beginning of the Web)
  - State Bar Associations still debating whether e-mail and mobile phone calls are secure communications
  - "Learning to Dictate" part of new lawyer orientation
  - No Outside E-mail services
  - No Blackberrys; No expectation that lawyers owned mobile phones

And change is happening more rapidly now!

And We Know That…

- The law is always behind technology
- And bar associations are always behind the law

New Technology's Impact

- Pressures on Ethical Licensing and Negotiating Practices
- Added Risk of Breach of Confidentiality
- The "We Can" = "We Should" Conundrum

What Does Ethics Mean?

- There are the technical RPCs and ethical/malpractice considerations, true
- But there are attorney-client privilege issues
- And overall organizational confidentiality issues
- And overall organizational risk issues

The Contracting Process

- Technology has flattened hierarchies and brought new players (both internal and external) who are often unsophisticated legal consumers
- Access to information has changed the contracting process and the assessment of risk
- Streamlined contracting processes have involved non-lawyers in the traditional lawyering process (e.g. contract administrators)
- How does the duty of candor impact negotiation
- New technology (e.g. mobile phones, e-mail, etc.) has permitted communication with opposing parties using communication media with new risks
- Drafting Issues, i.e. metadata; inadvertent disclosure
- Managing dishonest clients; duty to escalate

Unsophisticated Internal Clients

- Expect representation at speeds inconsistent with good legal representation (e.g. Speed Kills)
- Have an incomplete understanding of the law, but think they have a complete understanding (e.g. Curse of Wikipedia)
- Strong views on legal issues, including copyright ("Information wants to be free") and privacy ("No such thing. Get over it.")
- May not be used to dealing with lawyers; Don't understand the risk management perspective ("We all get along.")
- Business model problems
- More concerned with short term opportunities than long term risks (e.g. marketing or sales departments); They won't be around for when the risk hits
- Don't provide counsel with the full picture; Hiding the ball ("Don't let legal find out.")

Unsophisticated Opposing Parties or Customers

- Volatility of loyalty of likely plaintiffs (i.e. the myth of rationality) – especially within technology and entertainment communities
- Consumers with little understanding of the law and little respect for intellectual property
- The culture of “Modding”/Fan Films, etc.; the danger of being loved too much
- Danger of Wikipedia; A little knowledge can be a dangerous thing
- Young lawyers are often representing clients in areas and at levels that they are not ready for
- Opposing parties, particularly start-ups, who think that you are their lawyer as well (and internal clients who don’t discourage this)
- Many lawyers represent technology companies (or licensees of same) without using technology or understanding how the technology works

Ethical Contact of Opposing Parties

- Governed by Rule 4.2 and Rule 4.3
- Rule 4.2: Lawyer shall not communicate with person lawyer knows to be represented by counsel, unless obtained lawyer's consent
  - Requires lawyer's consent, not represented party's consent
  - Applies even if represented party initiates the conversation
  - Does not require lawyer to differentiate between in-house and outside counsel (ABA Opinion 06-443)
- Rule 4.3: In dealing with unrepresented persons, lawyer shall not state that lawyer is disinterested
  - May negotiate the terms of a transaction and prepare documents for signature with an unrepresented person, but must be clear that your represent an adverse party. (Comment 2)
- Negotiations with "contract administrators" or "paralegals"?
- In-house independent contractors that are present during negotiations with their company (awkward sidebars)
- When are parties actually adverse? (e.g. standards bodies)

Attorney-Client Privilege

- In-house counsel entitled to assert attorney-client privilege
- But:
  - EU In-House Counsel do not have a right to the attorney-client privilege
  - In-house counsel generally do not have a right to claim the privilege when performing non-legal duties. *What is the line?*
- Failure to keep legal discussions confidential will compromise the privilege:
  - Discussions in elevators, airplanes, etc. (e.g. Michael Jackson recording)
  - Discussions with independent contractors and free-lancers present
  - Public internet spaces; Open laptops; Unsecured WiFi?
- The counseling of employees or independent contractors on or through computer systems owned by employer (i.e. is the privilege compromised by a company's IT policies)
- Privilege compromised through our custom and practice

Multi-Jurisdictional Practice

- Rule 5.5 affirms the general principle that lawyers who are not licensed in a particular jurisdiction shall not practice law in violation of the regulation of the legal profession in that jurisdiction
- Rule 5.5(d), however, permits the performance of legal services for the lawyer's employer or affiliates
  - Not all states have adopted this multi-jurisdictional practice model rule as written
  - Many states have special registration and licensing procedures for corporate counsel.
  - Requires that the in-house lawyer only give legal advice to the organization that employs them (not, for instance, officers on a personal basis)

Negotiations; Duty of Candor

- In the course of representing a client a lawyer shall not knowingly make a false statement of material fact (Rule 4.1)
- Statements regarding a party's negotiating goals or its willingness to compromise as well as statements that can be fairly characterized as negotiation "puffing" are ordinarily not false statements of material fact (ABA Formal Opinion 06-439)
- Rule 8.4 – "It is professional misconduct to… (c) engage in conduct involving dishonest, fraud or misrepresentation"

When is it okay to bluff?????

Duty of Candor and Misrepresentations

- Rule 4.1 applies only to statements of material fact that the lawyer knows to be false
- Partially true but misleading statements or omissions may be "tantamount to affirmative false statements"
- Care must be taken by lawyer to ensure that "puffing" regarding client's positions are not statements "of fact" (compare statements regarding client's willingness to compromise v. statement of insurance limits)
- The rules do not require a higher standard of truthfulness in any particular negotiation contexts (e.g. mediation)
- No duty of good faith and fair dealing; Self-interest does not equal bad faith
- What about:
  - Withholding or manipulating information?
  - Lying about the best alternative to reach an agreement?
  - Lying about authority to accept an offer?
- But (of course!) cannot rise to the level of fraud (which would violate RPC 8.4)

Communication

- Rule 1.6 (A lawyer shall not reveal information relating to the representation of a client)
- Lawyers must use care with respect to their communications
  - Cell-Yelling
  - Exchanging e-mail without review of the entire e-mail string for potentially privileged communications
  - Use of ccs to clients and the reply to all function; Reply to all and the “bcc” function
  - Use of insecure third party communications media (e.g. gmail)
  - Risks of conducting discussions recorded on voice mail
- E-Mail disclaimers may demonstrate “reasonable precautions to prevent transmitted communications from coming into the hands of unintended recipients (Comment 17 to Rule 1.6)
- Recipient of inadvertently disclosed e-mail must notify sender (Rule 4.4(b)), but has no obligation to take additional steps
- ABA and many states’ ethics committees have opined that communicating with or about clients using unencrypted email is appropriate except in the most extreme circumstances

Drafting Issues

- Metadata in document drafts; embedded comments; internal messages
  - Sender obligated to use reasonable care when transmitting documents to prevent the disclosure of metadata containing client confidences or secrets (NY Ethics Opinion 782)
  - Unclear whether “reasonable care” includes use of scrubbing or filtering technology
  - States split on propriety of searching, mining, and using metadata in received electronic docs (see, e.g. Rule 1.3, NY State Bar Opinion 749 v. DC Bar Assn. Opinion 341)
  - ABA Opinion 06-442 requires recipient to notify sender
- Version Control Issues

Duty to Warn; Duty to Terminate

- In-House Counsel also have a duty to warn under Rule 1.13(b) ("If a lawyer for an organization knows that an officer, employee…is engaged in action…that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization")
  - Includes a duty to escalate to the highest authority
  - Consider subprime lender in-house counsel in 2007
- The duty to terminate representation if representation will result in violation of RPC under Rule 1.16 also applies to in-house counsel

Information Leakage; Confidentiality Compromise

- Security Breaches
- Bad Behavior
- Carelessness

Electronic and Network Security

- "Undersecurity"
  - Importance of Tracking "Industry Standards" (emerging negligence claim)
  - Failure to properly secure network
  - Failure to do physical due diligence of outsourced site
  - Failure to monitor outside vendors (Iron Mountain; Outsourcing)
  - Patriot Act/HIPAA issues (Safeguarding Rules)
  - Force Majeure in Post-Katrina environment
- "Oversecurity"
  - Spam management issues and Spam Filter over-inclusiveness issues
  - Designing inconvenient security or network security that is incompatible with business needs
- Breach Response Plan
  - Failure to develop comprehensive plan
  - Failure to control retaliatory "hacking"
- Unusual Side Effects (e.g. Sexual harassment for failure to monitor and prevent sexually oriented spam)
- Statutory Obligations (e.g. G-L-B/HIPAA)

Technology's Magnification of Bad Habits or Carelessness

- Use of technology in public or quasi public places (e.g. Cell-Yelling; speaker phones; laptops in coffee shops)
- Use of outside communications services for work purposes
- Use of software or services without sufficient customization (Obama social network)
- Implications of Blogs, both official and unofficial (e.g. Cisco)
- The immediacy of e-mail (autofill in Outlook; Alex v. Brad Berenson)
- Public Internet Spaces
- Viral Marketing (Aqua Teen Hunger Force); Easter Eggs
- Users failure to understand the devices they use (U.S. Government and Adobe Acrobat; Contract Management Software; Google "Confidential, do not distribute"; and Airbus)
- Magnification of failures to understand subject differences (TSTV; Anime v. Hentai)

Technology's Impact on Bad Behavior

- Technology Simplifies and Intensifies the Damage Done by Bad Behavior
  - "Nothing is Ever Deleted"
  - PR Nightmares: E-Mail Forwards (the infamous voice mail message; Brad the Cad; Ketchup Stain; Bla, bla, bla); Bloggers (Fred Durst and Paris Hilton); Podcasts; Photo Phones (Lindsay Lohan; Dog Poop Girl)
  - Easy Access to "James Bond" Technology: Spyware; Bugging (Fox Executive); Keyloggers (CA Student)
  - New Technology as Large Scale Theft Devices (Pod Slurping)
  - Consequences of Ubiquitous Monitoring (private law enforcement – suburban TP mom)
  - Lowers risk for data theft and corporate espionage (HP pretexting; phishing, evil twins)

Self Made Traps

- No specificity regarding mode of communication (i.e. If I call your mobile phone, you received the message) – What happens if you don't carry your phone on your belt?
- Organizational culture values efficiency over confidentiality
- E-mail retention and destruction policies create process presumptions
- Client communication via various communications media not controlled by organization (e.g. IM; Mobile Phones; E-mail)
- Open Curtains; Virtual Tours
- Failure to have a process for keeping confidential information confidential
- Failure to properly use NDAs in business discussions
- Failure to properly notify employees and independent contractors of confidentiality obligations (and conflicts of interest)
- Use of anecdotes in speeches and presentations

You Can, But Should You?

- Deciding When and How to Implement New Technology

Assessing Implementation of New Technology

- What is the efficiency v. security calculus when embracing the technology?
- How will the technology morph to create risks over the long term (e.g. iPod; RFID Tags)
- Will embracing technology subject you to new legal contexts (e.g. FCC regulation; international) or positional conflicts
- What are the liability consequences for disclosure (i.e. are the consequences greater because the data is aggregated)?
- What is the brand consequence for failing to embrace the technology? (e.g. late addition of e-commerce)
- Will employees/users bypass late adoption and create more risk (e.g. IM)
- How will users practically use the technology? (e.g. document management systems; oversecurity issues); What kind of risks will that lead to
- Understanding the potential for abuse of a technology. (e.g. black boxes; OnStar)

A Word About Social Networking/Blogging

- Avoiding the appearance of an attorney-client relationship
  - ABC NYOp 1998-2 – lawyers must exercise "caution and vigilance" to avoid the appearance of a relationship
  - Include appropriate disclaimers on your blog
  - Avoid legal advice
  - Clearly indicate that you are not requesting confidential information and reject it if you receive it
  - Lawyer discipline for revealing confidential client information
  - Facebook Case – Philadelphia Bar Association found deceptive friend request to gain information from a witness = dishonesty, fraud, misrepresentation in violation of Rule 8.4
- Many parties will review social networking sites for various applicants; not just for jobs (e.g. Florida Board of Bar Examiners)
- Supervisor-supervised issues (i.e. do I have to accept my boss' friend request?) (Judge discipline)
- No presumption of confidentiality in social networking page (e.g. Moreno v. Hanford Sentinel)

Practical Solutions

- **Good customer and employee relations:** Many problems occur because of disgruntled employees/dissatisfied customers. (See, e.g. Lucas)
- **Educate employees re good practices and basic legal concepts:** What are the implications of a breach; does the organization value speed and efficiency more
- **Ensure that security practices provide real security, not just the appearance of security:** (e.g. complicated passwords)
- **Be familiar with technology:** The legal department (and execs) are often behind the curve on identifying the legal risks of a certain technology
- **Monitor the Marketing Department, particularly the viral marketing:** The most creative group in the organization is also the group most focused on short-term results
- **Develop a plan for responding to data breaches, intrusions, etc.:** Have a plan because it'll be an emergency (Also, choose PR or Legal Solution)

Practical Solutions (Cont'd)

- **Implement technology on a timely basis and use realistic guidelines:** Employees will independently adopt technology that the organizations don't. Employees will circumvent unrealistic prohibitions
- **Undertake a network and physical security audit; Undertake an intellectual property audit:** Know what exists
- **Slow down where possible.** Risks magnify because of the pressure to meet aggressive timeframes
- **Monitor jurisdictional and channel "creep":** Technology facilitates efficient expansion, but such expansion may have significant legal risks
- **Watch vendor relationships:** Are they too close? Do they disrupt your ability to have an honest discussion?
- **Remind employees to be cognizant of surroundings:** Nothing creates problems faster than bad habits or carelessness

THANK YOU

Kraig L. Marini Baker

kraigbaker@dwt.com

206-757-8007