

Legal Ethics: Critical Issues for Corporate Counsel

WACHTELL, LIPTON, ROSEN & KATZ

Topics to be Covered

Privilege and Confidentiality in Daily Practice

Privilege and Confidentiality in the Corporate Context

Privilege in the Merger Context

Protecting Privilege and Confidentiality: *An Attorney's Ethical Duty*

“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) or required by paragraph (c).”

III. Rule of Professional Conduct 1.6(a)

Protecting Privilege and Confidentiality: *Limits to the Duty of Confidentiality*

- (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
 - (1) to prevent the client from committing a crime in circumstances other than those specified in paragraph (c);
 - (2) to prevent the client from committing 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;
 - (6) to comply with other law or a court order; or
 - (7) to detect and resolve conflicts of interest if the revealed information would not prejudice the client

III. Rule of Professional Conduct 1.6(b)

Protecting Privilege and Confidentiality: *Limits to the Duty of Confidentiality*

“A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent reasonably certain death or substantial bodily harm.”

Ill. Rule of Professional Conduct 1.6(c)

Privilege and Confidentiality in Daily Practice

Protecting Privilege and Confidentiality: *The Use of Technology*

- “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.”

III. Rule of Professional Conduct 1.6(e)

- “Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to:”
 - “the sensitivity of the information”
 - “the likelihood of disclosure if additional safeguards are not employed”
 - “the cost of employing additional safeguards”
 - “the difficulty of implementing the safeguards”
 - “the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”

III. Rule of Professional Conduct 1, Cmt. 18.

- “A client may require the lawyer to implement special security measures not required by this Rule.”

III. Rule of Professional Conduct 1, Cmt. 18.

Protecting Privilege and Confidentiality: *The Use of Technology*

- “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.”
- “This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions.”
- “Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.”
- “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

III. Rule of Professional Conduct 1, Cmt. 19.

Case Study: Personal Email Addresses

QUESTION:

- You are an employee of Company A. You also serve as an outside director for Company B. You would like to use your Company email address, even for Company B-related, confidential communications. When is it acceptable to use your Company A email address for these purposes?
 - A. It is never acceptable to use your Company A email address in this circumstance.
 - B. It is acceptable so long as there are only board members on the email chain.
 - C. It is acceptable if the email contains “Privileged and Confidential.”
 - D. It is acceptable if Company A creates an expectation of privacy in its email addresses, or if you take steps to guard against access by Company A and other third parties.

In re Asia Global Crossing (S.D.N.Y. Bkrcy. 2005)

- Four-factor test for weighing whether employee broke privilege by using work email to discuss unrelated privileged matters:
 1. Whether “the corporation maintain[s] a policy banning personal or other objectionable use”;
 2. Whether “the company monitor[s] the use of the employee's computer or e-mail”;
 3. Whether “third parties have a right of access to the computer or e-mails”; and
 4. Whether “the corporation notif[ied] the employee, or ... the employee [was] aware, of the use and monitoring policies.”

In re WeWork (Del. Ch. Dec. 22, 2020)

In *In re WeWork Litigation*, the Court of Chancery found that there was no expectation of privacy, as Sprint had a clear policy that employees would have no expectation of privacy in information they sent/received through their Sprint addresses, the Sprint execs were aware of these policies, and they took no effort to “defeat access” by Sprint, “such as shifting to a webmail account or encrypting their communications.”

Thus, directors who serve on multiple boards or advise multiple companies must be cautious in using personal or non-company email addresses for company-related, privileged matters.

Companies looking to guard against the risk of waiver should consider implementing policies that either require the use of corporate email addresses for confidential communications, or create a reasonable expectation of privacy in non-corporate emails.

Twitter v. Musk (Del. Ch. 2022)

- Elon Musk used SpaceX and Tesla email accounts to communicate about the acquisition of Twitter.
- The email policies “ma[d]e clear that employees have no privacy interest in their work emails and warn that the companies reserve the right to monitor those emails”
- However, the Court held that Musk still had an objectively reasonable expectation of privacy, based on affidavits submitted by Musk, IT managers, and Tesla’s GC stating that:
 - The companies had a policy of limiting circumstances where they would monitor employee emails
 - Musk had “unrestricted” personal use of his Tesla email account, that “no one” at Tesla can access those emails without Musk’s consent or “to the extent legally necessary,” and that “nobody” at SpaceX can access his email account without Musk’s express consent.

Twitter v. Musk (Del. Ch. 2022)


A cynic might doubt that Musk-specific policies exist at SpaceX and Tesla. Defendants' factual arguments to that effect rely solely on the affidavits of Musk, who has a lot at stake in this litigation, and three of his direct reports, and none of the affidavits are supported by any corporate records reflecting Musk-specific rules. Still, to this jurist, the evidence rings true. The court has little doubt that neither SpaceX nor Tesla view him as on par with other employees, that he has the power to direct operational decisions, and that nobody at either company would access his information without first obtaining his approval. One can debate whether this corporate reality makes for good "corporate hygiene,"⁵⁸ but it is difficult to discredit the recitation of the facts.⁵⁹

Case Study: The Ethics of the Cloud

QUESTION:

- You're approached by a newly launched "cloud" storage provider that offers to cut your storage costs by 50%. Is it appropriate to transfer your privileged and confidential data to this new system?
 - A. No — all client confidential information must be stored on devices that you control.
 - B. No — it is too risky to use a new service that may prove deficient or vulnerable to hacking.
 - C. Yes — but only if you review the terms of service first.
 - D. Yes — because cloud-based storage is widely used by the general public and lawyers.

Case Study: The Ethics of the Cloud

 **ISBA Professional Conduct Advisory Opinion**
ILLINOIS STATE BAR ASSOCIATION

Opinion No. 16-06
October 2016

Subject: Client Files; Confidentiality; Law Firms

Digest: A lawyer may use cloud-based services in the delivery of legal services if the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer's duty to protect the client information does not end once the lawyer has selected a reputable provider.

References: Illinois Rules of Professional Conduct, Rules 1.1, 1.6, 5.1 and 5.3
Illinois Rules of Professional Conduct, Rule 1.1, Comment 8 (amended Jan. 1, 2016)
ISBA Op. 10-01 (2009)
American Bar Association, Legal Technology Resource Center, www.americanbar.org.
Alabama Ethics Opinion 2010-2 (2010)
Arizona Ethics Op. 09-04 (2009)
Iowa Ethics Opinion 11-01 (2011)
Nevada Formal Opinion No. 33 (2006)
Tennessee Formal Ethics Op. 2015-F-159 (2015)
Washington State Bar Association Advisory Op. 2215 (2012)

FACTS

G:\LEGAL\Opinions 2016\16-06.docx

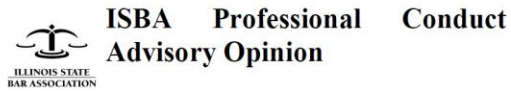
A lawyer may use cloud-based services to store confidential client information provided the attorney uses reasonable care to ensure that client confidentiality is protected and client data is secure. A lawyer must comply with his or her duties of competence in selecting a provider, assessing the risks, reviewing existing practices, and monitoring compliance with the lawyer's professional obligations.

ISBA Prof. Conduct Advisory Op. No. 16-06 (Oct. 2016)

Case Study: The Ethics of the Cloud

At the outset, as recognized by the inquiring lawyer here, lawyers must conduct a due diligence investigation when selecting a provider. Reasonable inquiries and practices could include:

1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
3. Investigating the provider's reputation and history;
4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data;
7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.



Opinion No. 16-06
October 2016

Subject: Client Files; Confidentiality; Law Firms

Digest: A lawyer may use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer's obligation to protect the client information does not end once the lawyer has selected a reputable provider.

References: Illinois Rules of Professional Conduct, Rules 1.1, 1.6, 5.1 and 5.3

Illinois Rules of Professional Conduct, Rule 1.1, Comment 8 (amended effective Jan. 1, 2016)

ISBA Op. 10-01 (2009)

American Bar Association, Legal Technology Resource Center,
www.americanbar.org.

Alabama Ethics Opinion 2010-2 (2010)

Arizona Ethics Op. 09-04 (2009)

Iowa Ethics Opinion 11-01 (2011)

Nevada Formal Opinion No. 33 (2006)

Tennessee Formal Ethics Op. 2015-F-159 (2015)

Washington State Bar Association Advisory Op. 2215 (2012)

FACTS


G:\LEGAL\Opinions\201616-06.docx

Case Study: Tracking Software

QUESTION:

- Opposing counsel sends you an email containing a hidden “tracking” image, which allows them to monitor when you open the email and to whom you’ve forwarded it. You do not detect the tracker and forward the email to your consulting experts, allowing opposing counsel to identify them. Did opposing counsel breach ethical rules by sending the tracker? Did you breach ethical rules by failing to detect it?
 - A. This is fine — it is equivalent to a “read receipt” on an email or a text message.
 - B. Both parties breached — opposing counsel acted dishonestly, but you should have detected the tracker under your duties of competence and confidentiality.
 - C. Only you breached — you should have taken affirmative steps to protect the confidential information.
 - D. Only opposing counsel breached.

Case Study: Tracking Software

 **ISBA Professional Conduct Advisory Opinion**
ILLINOIS STATE BAR ASSOCIATION

Opinion No. 18-01
January 2018

Subject: Communication with Confidentiality, and

Digest: A lawyer may not communicate with a client without first using tracking software. It is not reasonable to require that lawyers acquire special devices or programs to detect or defeat tracking software.

References: Illinois Rules of Professional Conduct 1.1, 1.6, 1.9, 4.4, and 8.4
Illinois Supreme Court Rules 9(a); 11(d); 131(d); 201(p); and 756(c)(4)
ISBA Professional Conduct Advisory Opinions No. 95-10 (January 1996) and No. 98-04 (January 1999)
American Bar Association Formal Opinions 01-422 (June 24, 2001); 06-442 (August 5, 2006); 477R (May 22, 2017); and 479 (December 15, 2017).
Alaska Bar Assn.
New York State
720 ILCS 5/14-2

The inquiring lawyer asks whether the use of tracking software known as “web bugs,” “web beacons,” or “cookies” in electronic communications with other lawyers is permissible.

ANALYSIS


G:\LEGAL\Opinions\2018\Opinion 18-01.docx

At a minimum, concealing the use of tracking software constitutes “dishonesty” and “deceit” within the meaning of Illinois Rule 8.4(c).

More fundamentally, this type of deception, if used in email correspondence with another lawyer in the course of representing a client, covertly invades the client-lawyer relationship between the receiving lawyer and that lawyer’s client.

ISBA Prof. Conduct Advisory Op. No. 18-01 (Jan. 2018)

Case Study: Tracking Software

 **ISBA**
Advisory

Opinion No. 18-01
January 2018

Subject: Communication
Confidentiality

Digest: A lawyer may communicate with a client without such software devices or programs.

References: Illinois Rules
Illinois Supreme Court
ISBA Professional Responsibility
No. 98-04 (January 2004)
American Bar Association
(August 5, 2004)
Alaska Bar Association
New York State Bar Association
720 ILCS 5/1-10.1

The inquiring lawyer known as "web bugs," "web tracking," or "web communications with other lawyers."

G:\LEGAL\Opinions\2018\Opinion 18-01.doc

of such software appear to vary among vendors. Typically, however, tracking software inserts an invisible image or code into an email message that is automatically activated when the email is opened. Once activated, the software reports to the sender, without the knowledge of the recipient, detailed information regarding the recipient's use of the message. Depending on the vendor, the information reported back to the sender may include: when the email was opened; who opened the email; the type of device used to open the email; how long the email was open; whether and how long any attachments, or individual pages of an attachment, were opened; when and how often the email or any attachments, or individual pages of an attachment, were reopened; whether and what attachments were downloaded; whether and when the email or any attachments were forwarded; the email address of any subsequent recipient; and the general geographic location of the device that received the forwarded message or attachment. At the sender's option, tracking software can be used with or without notice to the recipient. There do not appear to be any generally available or consistently reliable devices or programs capable of detecting or blocking email tracking software.

Case Study: Tracking Software

Although Comment [8] to Illinois Rule 1.1 and Illinois Rule 1.6(e), express a general duty that a lawyer should keep abreast of the benefits and risks associated with relevant technology as well as make “reasonable efforts” to prevent unauthorized access to client information, requiring the receiving lawyer to first discover and then defeat every undisclosed use of tracking software would be unfair, unworkable, and unreasonable.

It is appropriate and reasonable to expect lawyers to understand metadata and other ubiquitous aspects of common information technology.⁸ But it would be neither appropriate nor reasonable to charge all lawyers with an understanding of the latest version of tracking software that might be chosen, and then employed without notice, at the option of opposing counsel.



Opinion No. 18-01
January 2018

Subject: Communication with
Confidentiality, and

Digest: A lawyer may not use
communications with other lawyers or clients in the course of representing a
client without first obtaining the informed consent of each recipient to the use of
such software. It is not reasonable to require that lawyers acquire special
devices or programs to detect or defeat tracking software.

References: Illinois Rules of Professional Conduct 1.1, 1.6, 1.9, 4.4, and 8.4

Illinois Supreme Co

ISBA Professional C

No. 98-04 (January

American Bar Assoc

(August 5, 2006); 4

Alaska Bar Associat


New York State Bar

720 ILCS 5/14-2 (20

The inquiring lawyer asks v
known as “web bugs,” “web beaco
communications with other lawyer

G:\LEGAL\Opinions\2018\Opinion 18-01.docx

Case Study: Tracking Software

 **ISBA Professional Conduct**
Ad

Opinion No. 18-01
January 2018

Subject: **Communications Confidential**

Digest: A lawyer may not communicate with a client without the client's consent, even if such software or devices or products are used.

References: Illinois Rule 1.6, Illinois Supreme Court Rule 137, ISBA Professional Conduct No. 98-04 (October 1, 2003), American Bar Association Formal Opinion 402 (August 5, 2003), Alaska Bar Association Formal Opinion 09-01 (2009), New York State Bar Association Formal Opinion 720 ILCS 5/1-102.

The inquiring lawyer asked whether the use of tracking software known as "web bugs," "web beacons," or "cookies" in electronic communications with other lawyers or law firms is permissible under the rules of professional conduct.

ANALYSIS

G:\LEGAL\Opinions\2018\Opinion 18-01.docx

Even assuming that “defensive” software or devices capable of discovering and/or defeating tracking software were to become available, it would be unworkable to, in effect, force every Illinois lawyer to become and remain familiar with the various tracking programs on the market and then immediately purchase and install whatever new anti-tracking software or device that may, or may not, protect against the latest version. Given the typical rapid changes in technology, few, if any, solo or small firm lawyers could reasonably do so. Aside from creating sustained employment for IT consultants and software vendors, that approach would only precipitate an “arms race” in which the developers and users of tracking software would always be a step ahead.

Case Study: Artificial Intelligence

QUESTION:

- You are approached by an Artificial Intelligence service provider that offers to create a generative text platform tailored to your company's documents. Can you provide confidential and privileged documents for processing?
 - A. Yes — it's no different than a search index on a local computer.
 - B. Yes — provided that the information is compartmentalized and the model won't be used to service other customers.
 - C. No — off-site storage and processing of the documents will break privilege.

Case Study: Artificial Intelligence

Outside Counsel is retained by Acme to prepare a purchase agreement. Acme provides Outside Counsel with 20 precedent agreements — all strictly confidential — to indicate its preferred terms in different scenarios. Outside Counsel feeds these precedents into a generative AI system, and uses the resulting model to assist it in preparing the contract. Was that an ethical breach?

Case Study: *Mata v. Avianca, Inc.* (S.D.N.Y. 2023)

Here's What Happens When Your Lawyer Uses ChatGPT

A lawyer representing a man who sued an airline relied on artificial intelligence to help prepare a court filing. It did not go well.

The New York Times, May 27, 2023

Case Study:

Mata v. Avianca, Inc. (S.D.N.Y. 2023)

“In researching and drafting court submissions, good lawyers appropriately obtain assistance from junior lawyers, law students, contract lawyers, legal encyclopedias and databases such as Westlaw and LexisNexis. Technological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings. Rule 11, Fed.R.Civ.P. [Respondents] abandoned their responsibilities when they submitted non-existent judicial opinions with fake quotes and citations created by the artificial intelligence tool ChatGPT, then continued to stand by the fake opinions after judicial orders called their existence into question.”

Mata v. Avianca, Inc., 678 F. Supp. 3d 443, 448 (S.D.N.Y. 2023)

Case Study: International Travel

QUESTION:

- You are traveling across the U.S. border, when a border agent instructs you to hand over your phone for inspection. Your phone contains clients' confidential information. What should you do?
 - A. Hand it over — a border agent's authority is absolute.
 - B. Throw your phone out of the window.
 - C. Assert the attorney-client privilege and do not permit inspection unless “reasonably necessary” to comply with the border agent's claim of lawful authority.
 - D. You should not have taken your phone, as you should never carry clients' confidential information across the border.

Case Study: International Travel

“An attorney should not carry clients’ confidential information on an electronic device across the border except where there is a professional need to do so, and [] attorneys should not carry clients’ highly sensitive information except where the professional need is compelling.”

New York City Bar Ass’n Formal Op. 2017-5 (May 9, 2018)

The opinion also lists precautionary measures, including “using a blank ‘burner’ phone or laptop” and “uninstalling applications that provide local or remote access to confidential information.”

Privilege and Confidentiality in the Corporate Context

Privilege and Confidentiality in the Corporate Context

Directors

Corporate Affiliates

Insurers

Privilege and Confidentiality in the Corporate Context: *Directors*

- Under Delaware law, directors are treated as a “joint client” when legal advice is rendered to the corporation through one of its officers or directors.
 - *Kirby v. Kirby*, C.A. No. 8604 (Del. Ch. 1987)
- Rationale: “the board of directors, in its capacity as the governing entity for a corporation, is equivalent to the corporation. Thus, a privilege proper to the corporation cannot be asserted against a person who, at the time, was himself properly representing and, indeed, in some sense, was the corporation.”
 - *Dow Chem. Co. v. Reinhard*, No. 07-12012-BC, 2008 WL 2245007, at *7 (E.D. Mich. 2008)
- Exceptions:
 - By *ex ante* agreement
 - To appoint a special committee
 - Where sufficient adversity exists
- Former Directors: legal advice furnished ***during the director’s tenure***.
- Plaintiff Directors: privilege generated ***in defense of litigation***.

Case Study: *Hyde Park Venture Partners Fund III v. FairXchange* (Del. Ch. 2023)

- Delaware corporation was acquired over the objection of one of its directors, who served on the board as a representative of his venture capital firm. Post-merger, the director's venture capital firm launched an appraisal proceeding in Delaware court.
- The company asserted attorney-client privilege to block discovery into information created during the director's tenure.
- Did the company have a reasonable expectation of confidentiality as to the director and his venture capital firm during the director's tenure?
 - No.
 - Directors are treated as joint clients under Delaware law, so the company could not assert privilege as against him.
 - Delaware recognizes that in certain circumstances where a director serves on the board as a designee of an investor, "there is an implicit expectation that the director can share information with the investor."

Hyde Park Venture Partners Fund III, L.P. v. FairXchange, LLC,
No. 2022-0344-JTL, 2023 WL 2417273 (Del. Ch. Mar. 9, 2023)

Case Study: *Hyde Park Venture Partners Fund III v. FairXchange* (Del. Ch. 2023)

VC Laster reviewed the three “recognized methods” for altering the default rule:

1. The company can require the director to sign a confidentiality agreement.
2. The board of directors can form a committee that excludes the director and then separately retain counsel.
3. If there is a sufficient adversity of interests arises between the corporation and the director, “the corporation can put the director on notice of that fact, enabling the director to retain his own counsel and, if he wishes, call the question of information access through litigation.”

Case Study: *Icahn Partners LP v. deSouza* (Del. Ch. 2024)

- Director of a Delaware corporation shared privileged company information with his employer, a Carl Icahn-controlled entity and a 1.3% stockholder of the company. Icahn used the company information to bring claims against the directors in Delaware court.
 - The company sought to strike the portions of the complaint that contained privileged and confidential information that the director obtained after joining the board.
 - Did the director have a right to share privileged and confidential company information with his employer?
 - No.
 - A director generally may share company privileged communications with a designating stockholder when:
 - (1) a stockholder has the right to designate a director, either by contract or through its voting power; or
 - (2) the director serves as a controller or fiduciary of the designating stockholder.
 - The court granted the motion to strike.
- Icahn Partners LP v. deSouza*, No. 2023-1045-PAF, 2024 WL 180952 (Del. Ch. Jan. 16, 2024)

Privilege and Confidentiality in the Corporate Context: *Corporate Affiliates*

- “Confidential documents shared between members of a corporate family do not waive the attorney-client privilege.”
 - *In re JP Morgan Chase & Co. Sec. Litig.*, 2007 WL 2363311, at *6 (N.D. Ill. 2007)
- Under Delaware law, “courts have recognized that parents and their wholly owned subsidiaries have the same interests because all of the duties owed to the subsidiaries flow back up to the parent.”
 - *In re Teleglobe Commc’ns Corp.*, 493 F.3d 345, 366 (3d Cir. 2007)
- But context matters:
 - “Even in the parent-subsidiary context a joint representation only arises when common attorneys are ***affirmatively doing legal work for both entities on a matter of common interest***. . . . A broader rule would wreak havoc because it would essentially mean that in adverse litigation a former subsidiary could access all of its former parent’s privileged communications because the subsidiary was, as a matter of law, within the parent entity’s community of interest.” *Id.* at 379.

Case Study: Insurers

QUESTION:

- Acme has obtained liability insurance from InsureCo, in an agreement that includes a standard “cooperation” clause. A customer brings a liability suit, but InsureCo denies coverage and declines to assume defense. Acme defends the liability suit, but also pursues coverage litigation against InsureCo. InsureCo seeks production of all communications between Acme and its counsel in the underlying litigation. Can Acme rely upon attorney-client privilege to resist production?
 - A. Yes. A broadly worded cooperation clause does not evince intention to supercede attorney-client privilege.
 - B. Yes. Because InsureCo declined coverage, it cannot avail itself of the cooperation obligation.
 - C. No. The cooperation clause creates a contractual obligation for Acme to provide all communications with counsel concerning the underlying claim.

Privilege and Confidentiality in the Corporate Context: *Insurers*

- An insurance cooperation clause can defeat privilege in litigation with the insurer.
 - *Waste Mgmt., Inc. v. Int'l Surplus Lines Ins. Co.*, 144 Ill. 2d 178, 192 (1991)
- In *Waste Management*, the Supreme Court considered a cooperation clause that:
 - required insureds to “assist insurers in the conduct of suits and in enforcing any right to contribution or indemnity against persons potentially liable to insureds”
 - provided that insurers were “entitled to conduct any claim, in the name of insureds, for indemnity or damages against persons, and that insureds shall give all such information and assistance as the insurers may reasonably require.”
- (1) Insurers had a “contractual obligation” to disclose to the insurers “any communications they had with defense counsel representing them on a claim for which the insurers had the ultimate duty to satisfy.”
- (2) Because counsel in the underlying litigation was “act[ing] for the mutual benefit of the insured and the insurer,” the insurer shared a common interest that defeated attorney-client privilege.

Privilege in the Deal Context

Privilege in the Deal Context

Common Interest

Financial and PR Advisors

Post-Merger Control of Privileged Communications

Privilege in the Deal Context: *Common Interest*

Courts have applied different standards to determine whether parties share in a common interest:

- **Common interest where the parties “may be regarded as acting as joint venturers.”** *3Com Corp. v. Diamond II Holdings*, 2010 WL 2280734, at *7 (Del. Ch. May 31, 2010)
- *Delaware codified the privilege in Del. Uniform R. of Ev. 502(b)*
- **No common interest where there is no pending or anticipated litigation.** *Ambac Assur. Corp. v. Countrywide Home Loans, Inc.*, 27 N.Y.3d 616, 620, 57 N.E. 3d 30, 32 (2016).
- **No common interest between buyer and seller in an asset sale.** *Post v. Killington, Ltd.*, 262 F.R.D. 393, 397-98 (D. Vt. 2009).
- **Common interest where, in a patent case, buyer and seller had aligned interests with respect to the strength of the patents.** *Crane Sec. Techs., Inc. v. Rolling Optics, AB*, 2017 WL 470890 (D. Mass. Feb. 3, 2017).

Privilege in the Deal Context: *Common Interest*

- Illinois appears to favor a narrower construction of the common-interest doctrine.
- “Courts have considered such questions as whether the common-interest exception extends beyond actual cases to potential litigation, whether the doctrine extends beyond litigation interests to other interests, and whether a written common-interest agreement is required or the extent to which the parties must establish some form of advance agreement to confidentially share information While the Restatement provision answers many of these questions, we will leave it to our supreme court whether to adopt that Restatement; being in uncharted terrain, we will confine our analysis to the facts before us and the questions we must necessarily resolve.”

Selby v. O'Dea, 2017 IL App (1st) 151572, ¶ 73

Case Study: More *Twitter v. Musk* (Del. Ch. 2022)

- Musk was advised by Morgan Stanley and received funding from another Morgan Stanley entity.
- Musk asserted privilege over emails exchanged with both Morgan Stanley entities.
- Twitter argued that under NY law, any potential privilege had been waived because
 - the communications did not concern pending or anticipated litigation; and
 - the lender entity was a commercial counterparty to Musk.
- Morgan Stanley argued that under Delaware law, the common interest privilege protected the communications because the parties shared a common interest in "seeing the merger to its completion."

Privilege in the Deal Context: *Financial and PR Advisors*

Traditionally, disclosure to a third party will waive privilege. However, courts have generally found two major exceptions to this rule:

Assisting in Understanding and Interpreting Complex Principles (*Kovel* Doctrine)

- Consulted for the purpose of **improving the attorney's comprehension** of relevant factual information or the client's comprehension of legal advice rendered by the attorney.
- Must act in an **interpretive** function.
- The communication must be made in confidence for the purpose of obtaining **legal** advice from the attorney

U.S. v. Kovel, 296 F.2d 918 (2d Cir. 1961)

Functionally Acting as an Employee (Functional Equivalent Doctrine)

- The individual is, **functionally speaking, acting as a corporate employee** rather than a fully independent contractor.
- Not hired to assist the attorney; rather essentially **integrated** into the company.
- Courts look various criteria such as the person's responsibility and role in the company, relationship with principals, and access to information.

Case Study: *Stafford Trading, Inc. v. Lovely* (N.D. Ill. Feb. 22, 2007)

In *Stafford Trading*, the court held that communications with an investment banker were privileged where the communications were confidential and made for the purpose of **obtaining or providing legal advice**.

Determinations are made on a document-by-document basis:

Privileged: An email from GS forwarding to Kirkland term sheets for blacklining. The court explained that, “[b]ecause GS was acting as [the party’s] agent, seeking legal advice necessary to facilitate the transaction,” the document was privileged.

Not Privileged: Emails regarding whether certain business information should be disclosed to the other side. Counsel was neither asked for nor provided legal advice, but merely forwarding the information to the chain. Thus, the substance of the communications was **business**, not **legal** in nature.

Privilege in the Deal Context: *Post-Merger Control of Privileged Communications*

- Where a successor succeeds to the rights of a predecessor corporation by merger, it controls the privilege with respect to certain matters arising before the merger.

New York

Tekni-Plex (1996)

A surviving corporation claimed that it controlled privilege over pre-merger communications between the target corporation (which had merged into the surviving corporation) and its law firm. The Court of Appeals held that although privilege over general business communications vests in the surviving corporation, privilege over **communications relating to the merger negotiations does not**.

Tekni-Plex, Inc. v. Meyner & Landis, 89 N.Y.2d 123 (1996)

Delaware

Great Hill (2013)

In contrast to the court in *Tekni Plex*, *Great Hill* held that, under § 259 of the DGCL and **in the absence of express contractual provisions otherwise**, privilege over **all** the target's pre-closing communications—including communications relating to the **merger itself**—vests in the surviving corporation upon the merger (absent any contractual provision to the contrary). To rule otherwise, the court concluded, would be in clear contradiction of Delaware statutory law.

Great Hill Equity Partners IV, LP v. SIG Growth Equity Fund I, LLLP, 80 A.3d 155 (Del. Ch. 2013)

- Takeaway: Parties should contract for express provisions regarding post-merger control of pre-closing communications.