THE CALCULUS OF CONFIDENTIALITY: ETHICAL AND LEGAL APPROACHES TO THE LABYRINTH OF CORPORATE ATTORNEY-CLIENT COMMUNICATIONS VIA E-MAIL AND THE INTERNET - FROM *UPJOHN CO. v. UNITED STATES* AND ITS PROGENY TO THE HAND CALCULUS REVISITED AND REVISED

"[W]hat a chain of accidental circumstances had had the theatre for its final link."[1]

I. INTRODUCTION

Every lawyer, most certainly, wants to avoid any "chain of accidental circumstances"[2] that could lead to an inadvertent disclosure of confidential client communications. These accidental disclosures may be prevented if the lawyer undertakes to employ adequate safeguards.[3] It is without question that every lawyer additionally wants to avoid the public "theatre"[4] of a potentially detrimental legal malpractice action[5] or reprimand.[6] The Model Codes of Professional Responsibility and the Model Rules of Professional Conduct set forth certain guidelines for lawyers regarding their obligations to their clients and the safeguards they should undertake to secure confidential client communications.[7] They do not, however, specifically address communications made over electronic mail (e-mail) and the Internet.

The uncertainties surrounding confidential attorney-client communications in the context of modern computer technology have arisen in part because of substantial confusion over the definition of computer communications[8] and how to apply existing case law in this

---

[1]CHARLES DICKENS, DAVID COPPERFIELD 338 (Bantam Books 1981) (1850).

[2]*Id.*

[3]*See* discussion *infra* Parts III.A.-B.

[4]DICKENS, *supra* note 1, at 338.

[5]*See* discussion *infra* Part IV; Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982) (holding that accidental disclosure in response to discovery production request did not constitute waiver of attorney-client privilege).

[6]ABA STANDARDS FOR IMPOSING LAWYER SANCTIONS Standard 4.23 (1986) (amended 1992).

[7]MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997).

[8]As used in this note, "computer communications" includes both e-mail and Internet communications unless a further distinction is made. *See* Reno v. American Civil Liberties

new context.[9] Defining computer communications becomes important because the Model Codes and the Model Rules are presently only capable of dealing with standard forms of communication such as letters and (paper) files.[10] With the Model Codes and the Model Rules limited in the e-mail and Internet arenas, and confusion with respect to how to define computer-based communications, lawyers are left in a substantial quandary if they have to communicate with a client over the computer as opposed to communication by letter or in person. Couple these concerns with lack of judicial precedent and a corporate context, and the lawyer's quandary is far more aggravated and intense.

This note evaluates the ethical considerations[11] that a lawyer must undertake to safeguard confidential client communications made via e-mail or the Internet. This note begins in Part II.A with a survey of the attorney-client privilege defined through the Model Codes, the Model Rules, and applicable corporate case law. Part II.B examines the test for the corporate attorney-client privilege.[12] It is essential to understand when and what communications are privileged because privilege presupposes a confidentiality that is *judicially* recognized.[13] In light of discussing what is and what is not privileged, two conflicting Illinois cases are examined in Part II.C for their importance in demonstrating the confusion that exists regarding the attorney-client privilege.[14] This note continues in Part II.C with a discussion of the leading case on the corporate attorney-client privilege, *Upjohn v. United States*,[15] and considers whether e-mail communications would receive the expanded scope of *Upjohn*. *Upjohn* is fundamentally important because it sets forth

---

Union, 117 S. Ct. 2329, 2334-35 (1997) (discussing origins of the Internet, its operation, and e-mail).

[9]One writer maintains that "[i]t is not appropriate to extend existing case law to e-mail." Wendy R. Leibowitz, *Communication in the E-Mail Era: Deciphering the Risks and Fears*, NAT'L L.J., Aug. 4, 1997, at B9.

[10]*See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983) (discussing an attorney's duty to preserve confidences); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997) (discussing attorney-client confidentiality).

[11]Ethical considerations are evaluated in the context or in terms of the ABA Association Model Code of Professional Responsibility, Canon 4, and ABA Association Model Rules of Professional Conduct, Rule 1.6. An additional discussion is given on selected state and ABA ethics opinions. *See infra* notes 47-51.

[12]*See* discussion *infra* Part II.A-B.

[13]*See infra* notes 58-61 and accompanying text

[14]The note examines the two conflicting cases: Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254 (N.D. Ill. 1981), in conjunction with Mendenhall v. Barber-Greene Co., 531 F. Supp. 951 (N.D. Ill. 1982).

[15]449 U.S. 383 (1981).

the policy implications of expanding the privilege as well as the potential problems inherent in not extending the privilege.[16]

The next step in the analysis proceeds with a discussion of computer-based communications in the private (Part III.A.1) and public (Part III.B) arenas and the potential need for data encryption in these two very different domains.[17] The first case, *United States v. Maxwell*,[18] was chosen for its discussion of e-mail in the private domain, that is, in the context of a privately owned company, America Online. *Maxwell* is not entirely on point for reasons discussed in the main text, however, its discussion of an objective expectation of privacy that remains intact even if a communication is intercepted by a hacker is particularly insightful. It is useful to illustrate the concerns surrounding potential third party interception of attorney-client e-mail communications and its relation to waiver of the privilege.[19]

In light of *Maxwell*'s limits, it is considered in conjunction with a current constitutional case, *American Civil Liberties Union v. Reno*.[20] *Reno* sets forth substantial findings of fact regarding the Internet.[21] As such, it is arguably a reasonable companion case alongside *Maxwell*. The cases complement each other well in that they tend to examine the full spectrum of possible computer communications — from the private to the public sectors respectively. These cases are presented in the discussion of the need for data encryption in the private and public spheres.[22] This note concludes in Part IV with a study of two famous tort cases, *United States v. Carroll Towing Co.*[23] and *T.J. Hooper*,[24] against the backdrop of the "Hand Calculus."[25] The Hand Calculus is examined as one possible method for determining what safeguards a lawyer might want to take to prevent a "chain of accidental circumstances"[26] from causing injury or potential injury to his client. The Hand Calculus is then revised to reflect

---

[16]*See* discussion *infra* Part II.C.2.

[17]*See* discussion *infra* Part III.A-B.

[18]45 M.J. 406 (C.A.A.F. 1996).

[19]*Id.*

[20]929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, Reno v. American Civil Liberties Union, 117 S. Ct. 2329 (1997).

[21]*See infra* notes 155-56 and accompanying text.

[22]*See* discussion *infra* Part III.A.-B.

[23]159 F.2d 169 (2d Cir. 1947).

[24]60 F.2d 737 (2d Cir. 1932).

[25]The "Hand Calculus" refers to a mathematical equation developed by Judge Learned Hand in *Carroll Towing* to define an individual's duty to prevent injury to others. *See infra* notes 176-87 and accompanying text.

[26]DICKENS, *supra* note 1, at 338.

the complexities of the issues presented in the note.[27]

This note concludes in Part V with a brief summary of the models discussed throughout the text and whether data encryption is necessary.

II. THE ATTORNEY-CLIENT PRIVILEGE

A. *Defining the Privilege*

1. Ethics and Codes of Professional Responsibility: The Problematic Nature of the Ethical Obligation Under Canon 4 and the Disciplinary Rules

It is often noted that the attorney-client privilege is "the oldest of the privileges for confidential communications."[28] The attorney-client relationship is fiduciary in nature and involves the utmost good faith and loyalty on the part of the attorney towards his client.[29] The attorney-client relationship as *fiduciary* is further liberally implied throughout the

---

[27]*See* discussion *infra* Part IV.

[28]8 JOHN H. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2290 (McNaughton rev. 1961); Baird v. Koerner, 279 F.2d 623, 629 (9th Cir. 1960) (noting that the attorney-client privilege is of "ancient origin"). In *Baird*, the court held that appellant attorney, employed by the Internal Revenue Service (IRS), could not be compelled to release the names of clients who had sent him money in an attempt to remedy past income taxes owed to the IRS. *Id.* at 635. The court reasoned in part that the attorney could not be compelled to release the taxpayers' identities because the payments were voluntarily made, "unsued on, and with no government audit or investigation into that client's income tax liability pending." *Id.*

[29]7 AM. JUR. 2D *Attorneys at Law* § 137 (1980). The following definition regarding the attorney-client relationship as fiduciary and confidential is as follows:

> The relationship between an attorney and a client is highly fiduciary in its nature and of a very delicate, exacting, and confidential character, requiring a high degree of fidelity and good faith. It is purely a personal relation, involving the highest personal trust and confidence, which cannot be delegated without consent. . . . In a limited and dignified sense the relation between attorney and client is essentially that of principal and agent.

Id. at 189-90.

The relationship between attorney and client also requires that the "attorney must faithfully, honestly, and consistently represent the interests . . . of his or her client . . . [and] observe the highest and utmost good faith toward the client." 7 AM. JUR. 2D *Attorneys at Law* § 138 (1980). In terms of professional responsibility, the attorney-client relationship has also been described as follows: "[e]xcept to the extent authorized by a code of professional responsibility, an attorney has a duty to preserve both a client's confidences and secrets, and may not reveal a confidence or secret of the client without the client's consent." 7 C.J.S. *Attorney & Client* § 52, at 920-21 (1980). Thus, the attorney's relationship towards his client is characterized in the language of tort negligence as that of a duty.

American Bar Association Model Code of Professional Responsibility.[30] Canon 4 establishes the ethical considerations that a lawyer must assume when guarding a client's confidences.[31] It states that "[a] [l]awyer [s]hould [p]reserve the [c]onfidences and [s]ecrets of a [c]lient."[32] The underlying reasons for the Code are rooted in policy concerns for the "proper functioning of the legal system,"[33] which enables the client to "feel free to discuss"[34] his problem with his lawyer without fearing disclosure.[35]

Though the Code of Professional Responsibility establishes the ethical principles under which lawyers are presumed to conduct their relationships with their clients, the Code may be at once overinclusive and underinclusive.[36] This presents a problematic tautology of sorts,

---

[30]*See, e.g.*, MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983) (noting the "fiduciary relationship" between lawyer and client).

[31]*Id.*

[32]*Id.*

[33]*See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY EC 4-1 (1983); Cannon v. U.S. Acoustics Corp., 398 F. Supp. 209, 222 (N.D. Ill. 1975) (referring to ethical canon 4-1 in that the reason for the privilege is also to "encourage[ ] laymen to seek early legal assistance"), *aff'd in part and rev'd in part*, 532 F.2d 1118 (7th Cir. 1976).

[34]MODEL CODE OF PROFESSIONAL RESPONSIBILITY EC 4-1 (1983).

[35]See, e.g., Baird v. Koerner, 279 F.2d 623, 629-30 (9th Cir. 1960), stating that

> [w]hile it is the great purpose of law to ascertain the truth, there is the countervailing necessity of insuring the right of every person to freely and fully confer and confide in one having knowledge of the law, and skilled in its practice, in order that the former may have adequate advice and a proper defense. *This assistance can be made safely and readily available only when the client is free from the consequences of apprehension of disclosure . . . of the skilled lawyer.*

Id. (emphasis added). One commentator discusses the current need for lawyers to become increasingly "vigilant" with respect to guarding client confidences, especially in today's modern law offices. J.R. Phelps, *What is Your Office Policy on Client Confidentiality?*, L. PRAC. MGMT., Apr. 1993, at 58. It is argued that in today's law firms where there may be a constant turn-over of employees and staff, a breach of confidence can very easily occur. *Id.* The article states that "[s]ometimes, even the *perception* of a breach of confidentiality can be disastrous in terms of client feelings and loyalty." *Id.* at 59. Thus, one interesting question necessarily arises: how might a client perceive the confidentiality of communications over e-mail or the Internet especially given the complex dynamics of a large firm? *See, e.g.*, State v. Cory, 382 P.2d 1019, 1021 (Wash. 1963) (stating that an attorney "cannot make a 'full and complete investigation of . . . the law' unless he has the full and complete confidence of his client, and such conference cannot exist if *the client cannot have the assurance that his disclosures to his counsel are strictly confidential*") (emphasis added).

[36]*See, e.g., Cannon*, 398 F. Supp. at 215 (noting that "[n]o code of ethics could establish unalterable rules governing all possible eventualities[, u]ltimately, therefore, the resolution of these problems rests in the reasoned discretion of the court"). *Id.* This suggests that the ethics codes may provide only a framework at best for evaluating breaches of client

especially in light of communications over e-mail or the Internet. Courts are faced with a near legal tautology: it is[37] unethical to disclose confidential client communications which are confidential communications. Yet, how exactly to define e-mail and computer-based communications in terms of the ethical definitions is unclear because computer communications arguably differ from other common modes of communication. The Code of Professional Responsibility sets forth the following ethical considerations:

> The attorney-client privilege is more limited than the ethical obligation of a lawyer to guard the confidence and secrets of his client. This ethical precept, unlike the evidentiary privilege, exists without regard to the nature or source of information or the fact that others share the knowledge. A lawyer should endeavor to act in a manner which preserves the evidentiary privilege; for example, he should avoid professional discussions in the presence of persons to whom the privilege does not extend. A lawyer owes an obligation to advise the client of the attorney-client privilege and timely to assert the privilege unless it is waived by the client.[38]

The Disciplinary Rules set forth a broader definition of confidences and secrets:

---

confidentiality. Ultimately, the courts will have to decide how to address the problem. Most likely, the courts will evaluate breaches of confidentiality on a case by case basis. In *Cannon*, the court was concerned with the ethical dilemma raised when an attorney sought to represent both the individual and corporate defendants in a derivative shareholder's action. *Id.* at 213.

[37]Perhaps adding even more confusion to the legal tautology is the "should" language of Canon 4. The Model Code of Professional Responsibility states, "A [l]awyer [s]hould [p]reserve the [c]onfidences and [s]ecrets of a [c]lient." MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983).

[38]MODEL CODE OF PROFESSIONAL CONDUCT EC 4-4 (1983). It should also be noted that the attorney's obligation under the Code extends to providing protection for client confidences and secrets "following the termination of the practice of the lawyer, whether termination is due to death, disability, or retirement." *Id.* EC 4-6. *But see, e.g., In re* Sealed Case, 124 F.3d 230, 235 (D.C. Cir. 1997) (holding that the attorney-client privilege does not protect a deceased client's communication with counsel when the information related to a grand jury matter and was difficult to otherwise obtain). This narrowly carved exception might have an application to discovery of e-mail communications in that such materials might not be privileged if they could not be obtained in any other way. *See* FED. R. CIV. P. 26(b)(2) (defining limits on the scope of discovery materials).

> "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.[39]

According to the Disciplinary Rules, a "confidence" is that protected by the privilege and a "secret" refers to a client's request to his attorney to keep certain information confidential.[40] One must then ask whether computer communications are or perhaps more importantly, *should be* protected by the attorney-client privilege under the Code: whether they are exclusively a "confidence" or, alternatively, a "secret" such that, in regard to a "secret," the onus rests more on the client than the lawyer. Yet, if the communication is a "confidence," it is automatically privileged according to the Code. To avoid the legal tautology, one must determine whether such a communication is protected and if so under what circumstances should the protection be afforded.

2. Rule 1.6 of the Model Rules: Shifting from the "Specificity" of the Disciplinary Rules to More General "Information" Pertaining to Protected Materials

Under Rule 1.6, a lawyer is precluded from disclosing *information*, in its entirety, that is related to the client's representation, regardless of whether it is a "confidence" or a "secret."[41] However, under the Disciplinary Rules only a "confidence" which was privileged or a "secret" that the client did not want his lawyer to disclose could be protected under the privilege.[42] One further distinction between Rule 1.6 and the Model Code lies in the fact that under Rule 1.6, information is held confidential if the information was acquired "before or after the relationship existed" and the client does not have to ask his lawyer to keep the information confidential.[43]

Further, the lawyer need not "speculate whether particular information might be embarrassing or detrimental" to his or her client.[44]

---

[39]MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101 (1983).

[40]*See id.*

[41]MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997).

[42]*Id.*

[43]*Id.* MODEL CODE COMPARISON at 25.

[44]*Id.*

Rule 1.6 states that "[a] lawyer *shall not* reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except . . . [as further] . . . stated."[45] It is equally important to notice that Rule 1.6 does not specify how a disclosure might be made. Rule 1.6 could arguably cover any disclosures made by an attorney that are deliberate or careless in derogation of the duty to maintain confidentiality. Under a Rule 1.6 analysis, even e-mail communications between attorney and client may be protected regardless of whether one considers such mode of communication to be privileged because it is broadly asserted that "information" is protected.[46] Rule 1.6 is merely a model rule, however, and variations may exist among the states.[47]

The model rules and canons can present conflicting analyses when a court is faced with the dilemma of computer communications. Under the Model Code of Professional Responsibility Canon 4, it is asserted that a lawyer *should* maintain the "[c]onfidences and [s]ecrets of a [c]lient"[48] and yet the Model Rules of Professional Conduct Rule 1.6 states that "[a] lawyer shall not reveal information relating to representation of a

---

[45]MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997) (emphasis added).

[46]*Id.*

[47]See, e.g., Texas Rule 1.05 which provides in part:

> "Confidential information" includes both "privileged information" and "unprivileged client information." "Privileged information" refers to the information of a client protected by the lawyer-client privilege of Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence or by the principles of attorney-client privilege governed by Rule 501 of the Federal Rules of Evidence for United States Courts and Magistrates. "Unprivileged client information" means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client.

JOHN S. DZIENKOWSKI, PROFESSIONAL RESPONSIBILITY STANDARDS, RULES, AND STATUTES, Model Code Comparison, at 172 (West 1997). Thus, under the Texas rule, confidential information is given an expansive definition. The Texas rule further stipulates that "a lawyer shall not *knowingly* . . . [r]eveal confidential information of a client." *Id.* at 172-73 (emphasis added). Here, the use of the word "knowingly" might make a malpractice action difficult for a client to bring because the client would have to prove that the lawyer knowingly disclosed confidential information. This scienter requirement is difficult to establish. Thus, even a plaintiff to a malpractice action under Texas law brought in federal court may have this elevated scienter burden of producing sufficient evidence which if believed a jury could reasonably so find for the plaintiff in a malpractice action. *See generally* FED. R. EVID. 501 (stating that "the privilege of a . . . person . . . shall be determined in accordance with State law").

[48]MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1981).

client."[49] One cannot avoid the unsettling observation of changes in language from "should" to "shall" respectively and the further complexities of what should and should not be revealed.[50]

Because the Codes of Professional Responsibility and the Model Rules of Professional Conduct do not give a clear picture as to what safeguards, if any, a lawyer should (or must) take to guard against unintentional breach of confidential communications, one must then look to different models presented in the case law to attempt to figure out a possible answer to this perplexing issue.[51] First, one should begin with

---

[49]MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997).

[50]Another twist in the reticular intertwining of the language and the Codes of Ethics comes in Canon 37: "It is the duty of a lawyer to preserve his client's confidences." ABA CANONS OF PROF. ETHICS Canon 37 (1969). The Canons of Professional Ethics were "superseded in 1969 by the Model Code of Professional Responsibility." DZIENKOWSKI, *supra* note 41, editorial comment at 352. At least this may suggest a negligence approach when considering a breach of confidentiality.

[51]Though not fully addressed in this note, the ethics opinions present a clearer picture than the Model Codes of what safeguards a lawyer should take to guard against disclosure of confidential computer communications. Although, the ethics opinions have minimal precedential value. For example, one ABA Formal Opinion discusses a lawyer giving a computer maintenance company access to information in client files and the safeguards he needs to take:

> A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer may be obligated to disclose it to the client.

ABA Ethics Opinions, *ABA/BNA Lawyers' Manual on Professional Conduct*, Formal Op. 95-398, at 124 (Oct. 27, 1995). This opinion notes that the Model Rules have not yet addressed the issue of rapidly developing technology. *Id.* at 124-25.

The Colorado Bar Association, in one of its ethics opinions from 1992, discussed confidentiality and disclosure with regard to recorded conversations:

> A lawyer using electronic communication devices such as cordless telephones, cellular telephones, computer modems, electronic mail, and facsimile machines must exercise reasonable care to protect client confidences and secrets from inadvertent disclosure. Merely putting a "confidentiality notice" on a facsimile transmission may not suffice; a lawyer must exercise reasonable care in ascertaining the correct facsimile number of the intended recipient, inputting it, and guarding against the transmission's inadvertent disclosure. A lawyer communicating by telephone answering machine, computer modem or electronic mail must exercise reasonable care in determining that the message has been left on the correct machine and that only the intended recipient has access to it.

Ethics Comm. of the Colorado Bar Ass'n, Op. 90 (1992). The requirement of reasonableness reflects similar rasonable notice language of *Mullane v. Central Hanover Bank & Trust Co.*: "notice reasonably calculated." Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950). One other state has addressed the confidentiality issue with regard to e-mail and

a discussion of the existence of the attorney-client privilege in the corporate context.

B. *The Test for the Application of an Attorney-Client Privilege*: United States v. United Shoe Machine Corp.[52]

In this civil antitrust action, the court set forth the criteria for determining the application of the attorney-client privilege in a corporate context:

> The privilege applies only if (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is a member of the bar of a court, or his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client.[53]

Thus, application of the attorney-client privilege under *United Shoe Machinery* presupposes the existence of an attorney-client relationship.[54]

---

has essentially found that while operating a law office over the computer "via electronic media does not in itself violate the rules, the practice of law through such means raises several issues regarding . . . certainty of confidentiality. . . . Absent informed consent, confidential communications with clients would be jeopardized." South Carolina Ethics Op. 94-27 (1995). The opinion further remarks that the lawyer may just want to give general discussions of legal topics "on the electronic media . . . without giving advice or representing clients." *Id.*

[52]89 F. Supp. 357, 360-61 (D. Mass. 1950) (finding that certain exhibits were subject to the attorney-client privilege depending on the nature of one's work within the corporation as legal advisers or employees in a patent department).

[53]*Id.* at 358-59. This test has been cited frequently for the purpose of setting forth parameters for when the attorney-client privilege applies. *See* Natalie A. Kanellis, Comment, *Applicability of the Attorney-Client Privilege to Communications Intercepted by Third Parties*, 69 IOWA L. REV. 263, 266 n.32 (1983) (discussing the use of *United Shoe Mach.* for purposes of outlining the applicability of the privilege).

[54]As a side note, the physician-patient relationship bears some analogy to the attorney-client relationship and is thus informative if one analogizes e-mail to a telephone communication. One very recent case concerning the physician-patient relationship focused upon an informal telephone conversation between one physician and another who was directly treating a patient. The physician who had initiated the phone call sought advice on how to

This is critically important because, without an attorney-client relationship, the threshold inquiry is not met and a plaintiff cannot bring a legal malpractice claim. This becomes increasingly complicated with regard to computer communications because one must first establish that the attorney was consulting with a client or prospective client on advice of a legal nature. In fact, a problem can easily arise because, to determine if the communications were confidential, one would have to invade the attorney-client relationship to determine if it exists. Once the threshold relationship is established, the subsequent existence of privilege can depend on any number of factors beyond those cited in *United Shoe Machinery*.[55] For example, existence of the privilege can depend upon a broad interpretation of the attorney-client privilege[56] and/or how the information came to be intercepted by a third party.[57]

Discussion of materials that may or may not be privileged is critical to an analysis of attorney-client confidentiality. A document that is privileged, or more generally information that is privileged, means that the information's confidentiality is judicially recognized.[58] This confidentiality/privilege interplay stems from the intricate fiduciary relationship existing between attorney and client.[59] It is because the

---

treat and diagnose her minor patient whose condition was complicated and in whom the disease path was unclear. The young patient became a quadriplegic as a result of treatment, and the boy's mother and father brought a medical malpractice action against the physician from whom the advice was sought over the telephone. Yet, before any action for medical malpractice could be brought, plaintiffs had to establish the existence of a physician-patient relationship between the toddler and the physician who merely gave advice over a telephone. The court held that no physician-patient relationship existed. *See* Reynolds v. Decatur Mem'l Hosp., 660 N.E.2d 235 (Ill. App. 1996).

One recent article suggests that doctors also have concerns over using electronic mail and on-line services stating, "Doctors are concerned that the Internet makes all health information appear equal. They also fear the lost control over patient relationships and that poor security may corrupt records." Aimee Sullivan Bloomberg News, *Firm Sees Potential in On-Line Services for Health Care Industry*, J. REC., Mar. 19, 1997, at 2.

[55]*See* discussion *supra* Part II.B.

[56]*See, e.g.*, Upjohn v. United States, 449 U.S. 383 (1981) (expanding the scope of the corporate attorney-client privilege beyond that of the "control group"). This leading case for the corporate attorney-client privilege also re-established that the "privilege applies when the client is a corporation" despite the complex dynamics inherent in a corporation. *Id.* at 390.

[57]Kanellis, *supra* note 53, at 266-67.

[58]Attorney-client privilege may only be asserted in a judicial proceeding.

[59]Privileged communications are defined as:

> Those statements made by certain persons within a protected relationship such as husband-wife, attorney-client, priest-penitent and the like which the law protects from forced disclosure on the witness stand at the option of the witness, client, penitent, spouse. In federal courts, the extent and scope of the specific privilege is to be governed by federal common law or state rules

relationship is fiduciary that confidence and privilege automatically derive from the relationship.[60] Thus, to state that something has the special tag of "privilege" judicially affixed to it means that the law has recognized that this is confidential information and it will not be disclosed.[61] If it is recognized that e-mail and computer communications are privileged, then, it follows that there is a confidentiality onus imposed upon the lawyer deriving from the attorney-client relationship. This will affect what precautions, most likely in the form of data encryption, are required to be taken by the attorney. Because the Model Codes and Model Rules are ill equipped to deal with the new horizon of technology, one must attempt to extrapolate certain principles from the case law. Then, one must weave into the tapestry a consideration of the ethical implications imposed, even if not always explicit in the case law.

C. *Communications Privileged and Not Privileged*

1. *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*[62] and *Mendenhall v. Barber-Greene Co.*[63]: Conflicting Views on Disclosed Letters as Privileged and Nonprivileged Materials and the Need for *Upjohn*

In 1981, an Illinois federal court faced for the first time a perplexing issue concerning whether "confidential" rough drafts of letters, intended only for the eyes of corporate counsel but discarded in a trash dumpster, should be awarded the attorney-client privilege.[64]

The issue of whether to admit as evidence incriminating items found discarded in the trash is well settled in criminal procedure.[65] In a

---

governing evidentiary privileges.

BLACK'S LAW DICTIONARY 832 (6th ed. 1991). Not only does the privilege have its roots in evidence law, but the privilege actually derives from the *special nature of the relationship.*

[60]*See supra* note 29.

[61]Privilege is also found in the Federal Rules of Civil Procedure, where the rules limit materials discoverable and further limit those under the work-product doctrine. FED. R. CIV. P. 26(b)(1).

[62]91 F.R.D. 254 (N.D. Ill. 1981). It is important to mention that these cases have also been chosen because they discuss materials in the form of letters and both *Maxwell* and *Reno* analogize e-mail to letters.

[63]531 F. Supp. 951 (N.D. Ill. 1982).

[64]*Sew 'N Sweep*, 91 F.R.D. at 255.

[65]*See, e.g.*, California v. Greenwood, 486 U.S. 35, 40 (1988) (holding principally that when trash is left on the curbside, a police search of the trash that subsequently yields evidence indicative of narcotics use is admissible because of a diminished expectation of privacy and an objective belief that the trash may be "readily accessible to animals, children, scavengers,

criminal context, it is generally held that items discarded in the trash are sufficiently abandoned such that there is a lessened objective expectation of privacy with regard to the items subsequently found through a government "intrusion."[66] In such cases, there is no Fourth Amendment protection and the items found can generally be admitted in a criminal trial.[67]

It is important to make the distinction that for Fourth Amendment protection to be afforded, there must be a governmental actor involved in the intrusion. However, *Sew 'N Sweep* was a civil antitrust action in which plaintiffs Sew 'N Sweep suspected defendants Swiss-Bernina of trade restraints in violation of the Clayton Act and the Sherman Antitrust Act.[68]

To satisfy their suspicions, plaintiffs searched through defendants' trash dumpsters and, over the course of approximately two years, uncovered incriminating documents that they sought to be admitted in discovery proceedings.[69] The documents were rough drafts written by Swiss-Bernina's president to Swiss-Bernina's corporate counsel.[70] The court held that when a third party intercepts documents intended by the attorney and client as confidential, the documents lose their privilege.[71] This holding was grounded, in part, on several prior eavesdropping cases[72] and on the finding that the parties might have taken more adequate precautions to keep the items confidential.[73]

---

snoops, and other members of the public"). Brennan and Marshall dissented and discussed precedent that has held other personal items such as a 200-pound double-locked footlocker, suitcase, totebag, and packages wrapped in green opaque plastic are subject to a reasonable expectation of privacy. *Id.* at 48.

Implicit in the *Greenwood* majority are the concepts of control and abandonment which are fundamental concepts from property law. *See* Pierson v. Post, 3 Caines 175 (N.Y. 1805) (discussing the concept of control and ownership in the context of hunting animals). *See also* Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990) (holding in part that patient lost right to a claim of conversion for a cell-line derived surreptitiously from his tissues because of the overriding need for medical advancement, continued research, and lack of a retained ownership interest in the excised materials).

[66] *Greenwood*, 486 U.S. at 45.

[67] *Id.*

[68] *Sew 'N Sweep*, 91 F.R.D. at 255.

[69] *Id.* at 255-56.

[70] *Id.* at 256.

[71] *Id.* at 260.

[72] *See, e.g.*, Clark v. State, 261 S.W.2d 339 (Tex. Crim. App. 1953) (holding that conversations overheard by a telephone operator eavesdropping on an attorney-client conversation were not privileged and were admissible at defendant's murder trial).

[73] *Sew 'N Sweep*, 91 F.R.D. at 260. *See* discussion *infra* Part IV.

Sew 'N Sweep presents a limited paradigm for analyzing the attorney-client privilege and potential precautions to be undertaken in the context of safeguarding e-mail communications. In dicta, the *Sew 'N Sweep* court stated that the "[eavesdropping] cases cannot be easily summarized or reconciled, but do reveal that the privilege is not easily invoked and is easily destroyed."[74] Under *Sew 'N Sweep*, if a third party intercepts an e-mail communication, the privilege might be lost even if the attorney and client intended the communications to be confidential.[75] The attorney may have been required to have safeguarded his e-mail communications through the use of data encryption. At the very least, the data encryption might have suggested an intent to keep the communications confidential.[76] The court stated: "In determining whether the precautions taken were adequate, two considerations are paramount: (1) the effect on uninhibited consultation between attorney and client of not allowing the privilege in these circumstances; and (2) the ability of the parties to the communication to protect against the disclosures."[77]

One must seriously question the import of the *Sew 'N Sweep* test for adequacy of the precautions in light of corporate attorney-client communications over the computer. Similar to the ethical precepts,[78] the adequacy test is not very clear. On the one hand, communications between attorney and client may be severely inhibited because of the lack of privilege. Clients may feel uneasy disclosing information to their attorneys if there is no privilege to be asserted.[79] Thus, policy concerns automatically arise, such as hampering the proper functioning of the legal system and making clients reluctant to discuss details with their lawyers, thus barring free disclosure. On the other hand, this may favor liberal communication between attorneys and clients though not in matters of a legal context. Furthermore, data encryption may not be enough if the code can be broken.[80]

---

[74]*Sew 'N Sweep*, 91 F.R.D. at 258.

[75]*See id.* at 260.

[76]*See id.* The court stated that "the relevant consideration is the intent of the defendants to maintain the confidentiality of the documents as manifested in the precautions they took." *Id.*

[77]*Id.*

[78]*See supra* Part II.A.1-2.

[79]Recall that under EC 4-4, an attorney has an obligation to advise his client that the attorney-client privilege exists.

[80]Congress has recently been faced with the daunting task of United States encryption policies. *See* David J. Loundy, *Congress Scrambles to Address Encryption*, CHI. DAILY L. BULL., Mar. 13, 1997, at 1. The article discusses the alleged governmental need for encrypted

Sew 'N Sweep further examines the attorney's and the client's ability to "protect against the disclosures."[81] This is problematic because under the Model Rules and the Codes of Professional Responsibility, the onus for keeping information confidential lies solely with the attorney.[82] The client has little, if any, responsibility for securing confidential information.[83] Under *Sew 'N Sweep*, it is not clear what the client's

---

communications to trap certain criminal acts and international terrorism. *Id.* The article states that "one manufacturer of security software offered a reward to the first person who could crack the strongest level of encryption ... under ... [current government] ... policy -- it [reportedly] took a college student only 31/2 hours to collect." *Id.* at 2. This suggests that certain high levels of encryption available for export can be easily solved. Current proposed federal legislation includes the Security and Freedom Through Encryption Act (SAFE Act) reintroduced HR 695 and proposed by Rep. Bob Goodlate, R-Va. *Id.* The SAFE Act details that "any U.S. citizen shall have the right to use encryption, of any type, and of any strength or 'key length,' and in any medium ... [and] provide[s] additional penalties for anyone who uses encryption in the furtherance of the commission of a crime." *Id.* The article states that:

> [f]urthermore, the legislation eases export restrictions on any "generally available" or public domain software with a cryptographic component unless there is "substantial evidence that such software will be (A) diverted to a military end-use or an end use supporting international terrorism; (B) modified for military or terrorist end-use; or (C) re-exported [without any required authorization]."

Id. Two other bills include the Encrypted Communications Privacy Act of 1997 (S 376 IS) and the Promotion of Commerce Online in the Digital Era (Pro-CODE/S 377). *Id.* at 2-3. One relevant note, is that the legislature *has* established criminal penalties for third party interception of oral or wire communications.

> (1) Except as otherwise specifically provided in this chapter any person who-
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication ...
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through interception of a wire, oral or electronic communication in violation of this subsection ... shall be punished ... or shall be subject to suit.

18 U.S.C. § 2511 (1994).

[81] *Sew 'N Sweep*, 91 F.R.D. at 260.

[82] Recall the language of Rule 1.6: "A *lawyer* shall not reveal information relating to representation of a client...." MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1997). Recall also Canon 4: "A Lawyer Should Preserve the Confidences and Secrets of a Client." MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983).

[83] The Model Rules do not put the onus of confidentiality on the client. According to the rules, the onus of confidentiality rests solely with the lawyer. *See supra* note 82.

responsibility is unless one incorporates an analysis of the Model Rules and the Codes of Professional Responsibility. From the attorney's point of view, one must consider the potential financial burden of having to use data encryption and how this burden might be weighed against the risk of third party interception of privileged materials.[84]

It is interesting to note that *Sew 'N Sweep* suggested that, if the parties to the communication had intended confidentiality of the communications, disclosure may have been "prevented by destroying the documents or rendering them unintelligible before placing them in a trash dumpster."[85] Comparing this to third party interception of electronic mail communications, one might infer that encryption might be a prudent safeguard. In fact, the Iowa Supreme Court has already issued a 1996 Ethics Opinion in which it discusses this very issue and states:

> A law firm that has a home page or web site on the Internet must comply with the advertising rules. Disclosures must be on the home page or on the first screen of each page. This would not apply to a pure exchange of legal information with another lawyer. Pure exchange of legal information with clients is also an exception to this rule, *but sensitive material must be encrypted.*[86]

It thus might be entirely reasonable to require encryption in this circumstance. It appears as if the *Sew 'N Sweep* trend and the ethics opinions lean towards requiring encryption.

Mendenhall, on the other hand, contradicts *Sew 'N Sweep* and essentially finds for the existence of a privilege in far more egregious circumstances.[87] In *Mendenhall*, a patent infringement action, the plaintiff's lawyer had inadvertently disclosed confidential letters to the defendant's patent lawyer.[88] When the defendants later sought to have the letters produced, Mendenhall argued that the letters fell within the attorney-client privilege.[89] The court disagreed with the *Sew 'N Sweep*

---

[84]*See infra* Part IV (discussing the Hand Calculus).

[85]*Sew 'N Sweep*, 91 F.R.D. at 260. In a footnote, the decision mentions that during oral argument it was revealed that Swiss-Bernina had recently acquired a paper shredding device. *Id.* at 260 n.6.

[86]Iowa Supreme Court Board of Professional Ethics and Conduct, Op. 95-30 (May 16, 1996) (emphasis added).

[87]*Mendenhall*, 531 F. Supp. at 951, 954.

[88]*Id.* at 952 n.2 (providing the relevant facts).

[89]*Id.* at 952.

holding[90] and essentially outlined three scenarios in which to question whether the disclosed letters were still privileged.[91] The court essentially found that it was nearly impossible to circumvent a privilege unless, in the very unrealistic case, the plaintiff's attorney had just been acting as a "conduit" between his client and the foreign patent agents.[92] Yet, the court found that no facts suggested this type of scenario.[93]

While *Sew 'N Sweep* provides an interesting framework for analysis of the issue, it is inherently limited. A critical limitation of *Sew 'N Sweep* is that it is not followed in its own state by *Mendenhall.* The analysis is further limited in part because its fact pattern addresses letters instead of electronic communications. Another limiting feature is that the documents were discarded by *the client* and not the corporate counsel.[94] In *Mendenhall* the letters were divulged by the plaintiff's own attorney.[95] *Sew 'N Sweep,* like *Mendenhall,* is further limited because it does not consider the complex nature of the large corporation. Given the dynamics of the modern corporation with its various levels of staff, executives, and departments, the need for greater safeguards to ensure confidential communications becomes more critical and compounded. Thus, one must turn to the landmark case on the scope of the corporate attorney-client privilege, *Upjohn v. United States.*[96] In *Upjohn,* the Supreme Court sought to avoid the type of chaos and confusion that the Illinois court faced in *Sew 'N Sweep* and *Mendenhall.*

2. The Supreme Court and the Road to *Upjohn*'s "Functionalist" Approach Beyond Precedent to Deciding Privilege

Upjohn presented the Supreme Court with the dilemma of whether to extend the corporate attorney-client privilege beyond the "control group" recognized by the Sixth Circuit Court of Appeals.[97] In its highly policy-driven decision, the Supreme Court held that the corporate attorney-client privilege extends to those persons beyond the "control

---

[90]*Id.* at 955 n.8 (discussing the rejection of *Sew 'N Sweep*).

[91]*Mendenhall,* 531 F. Supp. at 952.

[92]*Id.* at 954.

[93]*Id.*

[94]Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 256 (N.D. Ill. 1981).

[95]*Mendenhall,* 531 F. Supp. at 952.

[96]449 U.S. 383 (1981).

[97]*Id.* at 388-89. The "control group" is defined as "'officers and agents . . . responsible for directing [the company's] actions in response to legal advice." *Id.* at 391 (quoting Upjohn v. united States, 600 F.2d 1223, 1225 (6th Cir. 1979)).

group."[98] The Court recognized that information gleaned from employees and other management that relates to the corporation's solicitation of legal advice will also fall within the scope of the attorney-client privilege.[99]

In one sense, the *Upjohn* holding can be interpreted as a functionalist approach, because the Court's holding went beyond the rules of case precedent. In its decision the Court projected outward, evaluating the potential impact that an extension of the attorney-client privilege might have and the ramifications surrounding a refusal to extend the privilege.[100] The holding marked a new line of thinking about the ramifications of the corporate attorney-client privilege. It was no longer necessary to consider the rigid, narrow, and formalist[101] approach taken by the court of appeals because it simply did not work in the context of the complex dynamics of a large corporation.[102]

a. Upjohn*'s Critical Facts*

In *Upjohn*, the company's corporate attorneys learned that money might have been paid to by one of its foreign subsidiaries "to or for the benefit of foreign government officials in order to secure government business.[103] Upjohn's attorney undertook an independent investigation of these "questionable payments."[104] He drafted a letter containing a questionnaire seeking information on the potential payments, that was sent to "All Foreign General and Area Managers."[105] The managers had been "instructed to treat the investigation as 'highly confidential' and not to discuss it with anyone other than Upjohn employees who might be

---

[98]*Id.* at 397.

[99]*Id.*

[100]Generally, "formalism" and "functionalism" are more appropriate for analysis of constitutional cases; however, a brief survey of functionalism in the context of *Upjohn*, is appropriate given *Upjohn*'s implied extension beyond case precedent and its policy-driven approach to the attorney-client privilege.

[101]*See supra* note 100.

[102]*Upjohn*, 449 U.S. at 397. The Supreme Court actually struck down the court of appeals' holding based in part on the Federal Rules of Evidence, Rule 501, on grounds of "reason and experience." *Id.* The law reflected by the court of appeals did not comport with the common law and the rules of evidence. *Id.* Rule 501 states in part: "Except as otherwise required by the Constitution of the United States or provided by Act of Congress . . . the privilege of a witness, person . . . shall be governed by the principles of the common law . . . in the light of reason and experience." FED. R. EVID. 501.

[103]*Upjohn*, 449 U.S. at 386.

[104]*Id.*

[105]*Id.*

helpful in providing the requested information."[106] Upjohn then voluntarily submitted a report to the Securities and Exchange Commission and the Internal Revenue Service disclosing the questionable payments.[107] The Internal Revenue Service subsequently sought to have the confidential investigative documents produced because the Service was concerned about possible taxes owed on the payments.[108]

b. *The Court of Appeals*

The Court of Appeals for the Sixth Circuit held that the documents were discoverable, because the attorney-client privilege did not apply.[109] The court was concerned that, if the privilege was extended in this situation, it might create a "broad 'zone of silence' among upper-echelon management."[110] Thus, the court of appeals held that the attorney-client privilege only existed within the parameters of the "control group," meaning that information obtained from employees was not privileged.[111]

c. *The Supreme Court and Policy*

The Supreme Court began its analysis by first recognizing that the attorney-client privilege applies to corporations.[112] The Court then

---

[106]*Id.* at 387. Recall that this desire to keep the information confidential satisfies the *Sew 'N Sweep* test for when precautions taken are adequate. *See* discussion *supra* Part II.C.1.

[107]*Upjohn*, 449 U.S. at 387.

[108]*Id.* at 387-88.

[109]*Id.* at 388.

[110]*Id.*

[111]*Upjohn*, 449 U.S. at 388-89.

[112]*Id.* at 390 (stating that "this Court has assumed that the privilege applies when the client is a corporation"). The Court referred to United States v. Louisville & Nashville Railroad, 236 U.S. 318, 336 (1915). In that case, the Court explained that

> [t]he desirability of protecting confidential communications between attorney and client as a matter of public policy is too well known and has been too often recognized by text-books and courts to need extended comment now. If such communications were required to be made the subject of examination and publication, such enactment would be a practical prohibition upon professional advice and assistance.

Id. The Court again seems to support the long-held belief that the privilege is of "ancient origin." *See* Baird v. Koerner, 279 F.2d 623, 631 (9th Cir. 1960) (holding that "there is no federal body of law that *requires* the exclusion of the identity of the client from the extent of the attorney-client privilege"); Clement v. Prestwich, 448 N.E.2d 1039, 1041 (Ill. App. 2d 1983) (holding that claims for violation of the attorney-client privilege are not assignable in a legal malpractice action).

provided a reasoning similar to that of *Diversified Industries, Inc. v. Meredith*,[113] in which the Eighth Circuit stated:

> In a corporation, it may be necessary to glean information relevant to a legal problem from middle management and nonmanagement personnel as well as from top executives. The attorney dealing with a complex legal problem "is thus faced with a 'Hobson's Choice'. If he interviews employees not having 'the very highest authority', their communications to him will not be privileged. If, on the other hand, he interviews *only* those with 'the very highest authority', he may find it extremely difficult, if not impossible, to determine what happened."[114]

The *Upjohn* Court was similarly concerned with the overriding policy implications as set forth in the Model Rules and the Model Codes, namely, if the privilege is not extended, its fundamental purpose may be frustrated, hampering the functioning and the exchange of information between attorney and client. The Court reasoned that "[i]n the corporate context . . . it will frequently be employees beyond the control group as defined by the court below — 'officers and agents . . . responsible for directing [the company's] actions in response to legal advice' — who will possess the information needed by the corporation's lawyers."[115] The main purpose of the attorney-client privilege cannot be served if the court of appeals' "control group" test governs the limits of the privilege.[116] Ironically, though the Court was reluctant "to lay down a broad rule or series of rules to govern all conceivable future questions in this area,"[117] the Court was highly concerned about uncertainty and unpredictability, stating:

> But if the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports

---

[113]572 F.2d 596 (8th Cir. 1977) *modified en banc*, 572 F.2d 606 (8th Cir. 1978).

[114]*Id.* at 608-09.

[115]*Upjohn*, 449 u.S. at 391.

[116]*Id.*

[117]*Id.* at 386.

> to be certain but results in widely varying applications by the courts, is little better than no privilege at all.[118]

Therefore, under *Upjohn*, it appears that the requirement for data encryption, if there is to be one, must be universally applied in all courts and jurisdictions. Arguably, given the highly complex nature of technology and its inherent unpredictabilities and uncertainties, the need for uniformity becomes paramount.[119]

The need to expand the privilege to cover e-mail communications becomes clear under *Upjohn*. In fact, Chief Justice Burger, concurring in part and in the judgment, further elaborated on the need for a standard that would guide corporations with regard to the privilege, "[f]or this very reason, I believe that we should articulate a standard that will govern similar cases and afford guidance to corporations, counsel advising them, and federal courts."[120]

Even though *Upjohn* presents the framework under which to begin an evaluation of the need for data encryption and the scope of the attorney-client privilege in the context of computer communications, it is only a starting point. *Upjohn* is a controversial decision, and it is not followed by all of the states;[121] however, it is promising that one recent Massachusetts case has applied *Upjohn* to determine whether e-mail communications are privileged materials.[122]

---

[118]*Id.* at 393.

[119]An interesting note to the phenomenon of uncertainty and unpredictability involves the uncertainty principle found in quantum theory. The uncertainty principle involves the ability to make a known measurement of a given quantum mechanical system in a given time frame. The "uncertainty principle is concerned precisely with the question of the interference produced by [the] observation." DAVID S. SAXON, ELEMENTARY QUANTUM MECHANICS 47 (1968). Applying the uncertainty principle to the phenomenon that *Upjohn* was trying to avoid, means that one might never be able to avoid absolute uncertainty because there would always exist some difficulty in measuring exactly what should be required to reduce the uncertainty. Thus, uncertainty and unpredictability will always exist on a theoretical level, but at least *Upjohn* provides a good paradigm for trying to alleviate most of the uncertainty in a corporate context.

[120]*Upjohn*, 449 U.S. at 402.

[121]For a decision that departs from *Upjohn*, see Jarvis, Inc. v. American Tel. & Tel. Co., 84 F.R.D. 286, 291 (D. Colo. 1979) (concluding that the "control group test . . . most effectively meets the concern for creating too large a zone of silence while recognizing a proper scope for the attorney-client privilege").

[122]*See* National Employment Serv. Corp. v. Liberty Mutual Ins. Co., No. 93,2528-G, 1994 WL 878920 (Mass. Super. 1994). The court, in the absence of Massachusetts precedent, followed *Upjohn*'s holding. *Id.* at *1. The case turns on the plaintiff's claim that the defendant breached a contract and engaged in unfair business practices. *Id.* The plaintiffs sought 32 electronic mail communications which defendants claimed as being protected under

It becomes incumbent upon one to look at how the Supreme Court and the U.S. Court of Appeals for the Armed Forces have interpreted e-mail and the Internet beyond purposes of privilege. If *Upjohn* cannot get an e-mail communication privileged within its protective scope with any certainty and predictability among the states and jurisdictions, then one needs another approach to getting computer communications recognized as confidential. In this sense, it is necessary to link the holding of *Upjohn* with that of *United States v. Maxwell*[123] and *American Civil Liberties Union v. Reno.*[124] These cases speak directly to the issue of e-mail communications beyond the need for recognizing a "privilege."

III. THE INFORMATION SUPER-HIGHWAY: E-MAIL IN THE PRIVATE AND PUBLIC ARENA

A. *America Online: Reduced Need for Data Encryption?*

In *United States v. Maxwell,*[125] the U.S. Court of Appeals for the Armed Forces faced a case involving e-mail communications over the privately owned company, America Online (AOL), made by a respected

---

the attorney-client privilege. *Id.* In deciding whether to apply *Upjohn* to the scope of electronic mail communications, the court was concerned about the type of advice that was given over the computer. *Id.* at *2. The court focused on whether Liberty Mutual's corporate counsel was acting in a legal capacity as opposed to a business capacity at the time the communications were made. *Id.* The court then set forth a standard to determine whether a lawyer has acted in a professional capacity for the purposes of holding certain e-mail communications as privileged:

> One factor which must be evaluated in order to determine whether an attorney communicated in his professional capacity as a lawyer is whether the task could have been readily performed by a nonlawyer % — as when facts are gathered for business decisions. A related factor is whether the function that the attorney is performing is a lawyer-related task such as: applying law to a set of facts; reviewing client conduct based upon the effective laws or regulations; or advising the client about status or trends in the law . . . . Thus, there is a distinction between a conference with counsel, and a business conference at which counsel was present. Documents which do not ordinarily qualify for the privilege are: business correspondence; interoffice reports; file memoranda; and minutes of business meetings.

Id. The court, after an in camera inspection of the documents, concluded that the documents contained legal advice "in anticipation of litigation," and there was no indication that the communications resulted from strictly a business relationship. *Id.* at *3. Thus, the communications were privileged. *Id.*

[123]45 M.J. 406 (C.A.A.F. 1996).

[124]929 F. Supp. 824 (E.D. Pa. 1996), *aff'd,* Reno v. American Civil Liberties Union, 117 S. Ct. 2329 (1997).

[125]45 M.J. 406 (C.A.A.F. 1996).

career officer.[126] The officer was charged with communication of indecent language in violation of The Uniform Code of Military Justice and distribution of child pornography.[127] An informant had alerted AOL's vice-president of marketing about the child pornography, who notified the FBI, which notified the Goodfellow Air Force Base in Texas.[128] Officer Maxwell was convicted by a general court martial on the indecent language charges and the child pornography charges, and the U.S. Air Force Court of Criminal Appeals affirmed the conviction.[129]

In affirming the conviction, the U.S. Air Force Court of Criminal Appeals recognized the need to analyze the government's seizure of Maxwell's computer files under the Fourth Amendment's reasonableness standard alongside the objective expectation of privacy.[130] The court held:

> In our view, appellant [Maxwell] clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was *virtually no risk that appellant's [Maxwell's] computer transmissions would be received by anyone other than the intended recipients.*[131]

Though Maxwell had a recognized objective expectation of privacy, evidence seized from the computers was still admissible based on probable cause and the failure of the court to invoke the exclusionary rule.[132] The U.S. Air Force Court of Criminal Appeals did not provide much factual background on e-mail; instead, the court spoke in terms of the risk associated with e-mail transmissions and, specifically, the risk

---

[126]*Id.* at 410.
[127]*Id.* at 410, 412.
[128]*Id.* at 412.
[129]United States v. Maxwell, 42 M.J. 568 (A.F.C.C.A. 1995).
[130]*Id.* at 575.
[131]*Id.* at 576 (emphasis added).
[132]*Id.* at 579.

that another party might intercept those transmissions.[133] Because America Online is a private company, Maxwell's expectation of privacy was greater than it might have been had it been an impliedly public forum.[134]

In 1996, the U.S. Court of Appeals for the Armed Forces reversed, finding that though Maxwell had an expectation of privacy in his e-mail messages, the expectation had some limitations.[135] Furthermore, the U.S. Court of Appeals for the Armed Forces generated a lengthy discussion of e-mail, the Internet, and various types of e-mail communications with periodic references to *ACLU v. Reno*.[136] The subtle change in holdings suggests that the issue of privacy and e-mail is currently the subject of great debate even among various judicial bodies. This reflects Chief Justice Burger's concern in *Upjohn* that the Court "should articulate a standard" for other courts and corporations to follow.[137] This further echoes the chaos seen in the Illinois courts.[138]

1. *Maxwell*'s Facts on E-Mail in the Private Sector

Because the attorney-client privilege is lost if another party intercepts the communication,[139] it is important to have some sense of the likelihood that a third party might be able to intercept an e-mail communication. This likelihood[140] is inextricably linked with the type of

---

[133]*See generally Maxwell*, 42 M.J. 568 (focusing on the minimal risk, if any, of a third party (hacker) intercepting the e-mail messages in the private domain with regard to America Online).

[134]*Id.* at 576. It should be noted that an objective expectation of privacy is an expectation of privacy that society is willing to recognize. Katz v. United States, 389 U.S. 347 (1967) (holding that the Fourth Amendment applies to conversations placed over a public telephone in a booth) (Harlan, J., concurring, requiring that "the expectation be one that society is prepared to recognize as 'reasonable'"). *Id.* at 361.

[135]*Maxwell*, 45 M.J. at 417.

[136]*Id.*

[137]Upjohn v. United States, 449 U.S. 383, 402 (1981) (Burger, C.J., concurring).

[138]*See supra* Part II.C.

[139]*See* Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254 (N.D. Ill. 1981); *but see* Mendenhall v. Barber-Greene Co., 531 F. Supp. 951 (N.D. Ill. 1982) (granting the protection of attorney-client privilege).

[140]"Likelihood" in terms of probability means "when faced with several parameter values, any of which might be the true one for a population, the best 'bet' is that parameter value which makes the sample actually obtained have the highest probability." ROBERT L. WINKLER & WILLIAM L. HAYES, STATISTICS: PROBABILITY, INFERENCE, AND DECISION 345 (2d ed. 1975). For the purposes of this note, it is useful to think of likelihood and probability as referring to the "risk" that someone else might come across the confidential communication and this "risk" depends on what type of communication is at issue: private or public.

e-mail communication — that is whether the communication is over a private or public medium. Maxwell's communications took place over AOL, which is a privately owned company.[141] The court described the AOL computer set-up as the ability to "communicate with others via each individual's personal computer terminal and computer telephone modem . . . which transmits electronic impulses over telephone lines."[142] The court discussed the privacy implications of the AOL e-mail service as:

> The only authorized way to have access to an e-mail message is to be the recipient of the original message or a forwarded message. All of a user's mailboxes are distinct; thus if one has five separate screen names, that individual would have to log on to the system separately under each user name in order to retrieve all the e-mail received. Once the original e-mail message has been sent, the originator of the message has no control over to whom or how many times the message is forwarded.[143]

The court further explained that e-mail messages are stored for a maximum of five weeks and then are expelled from the system.[144] One other key fact is that "AOL executives and employees do not read or monitor e-mail."[145] The court analogized e-mail to a letter and found that, when one seals a letter and addresses it to a given party, the sender enjoys the "privilege" that the letter will only be opened by the designated recipient and no one else, absent some sort of legal or judicial interference.[146] The court then, drawing from parallels between e-mail as a letter and other common forms of communication, stated outright that " [t]he fact that an unauthorized 'hacker' might intercept an e-mail message *does not diminish the legitimate expectation of privacy in any way.*"[147] Interestingly, under *Maxwell*, a third party's interception of an e-mail message might not defeat the attorney-client privilege.

Based on the legitimate expectation of privacy and the statement on "unauthorized hackers," one might infer that data encryption may not be entirely necessary. Though privately owned companies such as AOL

---

[141] *Maxwell*, 45 M.J. at 417.
[142] *Id.* at 411.
[143] *Id.* at 412.
[144] *Id.*
[145] *Maxwell*, 45 M.J. at 412.
[146] *Id.* at 417.
[147] *Id.* at 418 (emphasis added).

may provide some level of privacy, "[t]he major commercial online services have almost twelve million individual subscribers" and appear to be growing exponentially which suggests that in spite of an expectation of privacy in this sector, data encryption might be a prudent safeguard.[148]

B. *The Internet: Recognized Need for Data Encryption*

In 1996, the United States District Court for the Eastern District of Pennsylvania set forth substantial findings of fact on the Internet and various forms of communication over the Internet.[149] The Supreme Court, with Justice Stevens authoring the majority opinion, summarized the undisputed facts from the lower court.[150] *American Civil Liberties Union v. Reno* involved the constitutionality of certain provisions of the Communications Decency Act (CDA), which made it illegal to distribute "indecent" or "patently offensive" materials to an individual under eighteen years old.[151] The American Civil Liberties Union, among others, challenged the constitutionality of the provisions and sought a preliminary injunction against the statute's enforcement.[152] The plaintiffs claimed that the statute violated First Amendment rights to free speech and the Due Process Clause of the Fifth Amendment.[153] The district court held that "the Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion."[154]

In reaching its conclusion, the district court first set forth a detailed description of how the Internet was created and how cyberspace developed, how people access the Internet, and methods of

---

[148]American Civil Liberties Union v. Reno, 929 F. Supp. 824, 833 (E.D. Pa. 1996), *aff'd*, Reno v. American Civil Liberties Union, 117 S. Ct. 2329 (1997).

The exponential nature of the growth of Internet and computer users may be characterized mathematically in terms of an exponential growth function: N(t) = N(o)e^ct. *See, e.g.*, EARL W. SWOKOWSKI, CALCULUS WITH ANALYTIC GEOMETRY 360 (1983). N(t) is the growth at some later time "t," and q(o) is the initial value at time zero. The "e" represents the exponential function, and "c" is some constant. Thus, the number of future users N(t) can be calculated given some initial estimate of the current number of users N(o).

[149]*Reno*, 929 F. Supp. at 830-49.

[150]*Reno*, 117 S. Ct. at 2334-37.

[151]*Reno*, 929 F. Supp. at 828-30.

[152]*Id.* at 827.

[153]*Id.*

[154]*Id.* at 883.

communicating over the Internet.[155] Essentially, the court described the Internet as a "network of networks,"[156] acknowledging that:

> [n]o single entity — academic, corporate, governmental, or non-profit — administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.[157]

The highly public nature of the Internet is cause for concern in light of attorney-client confidentiality and privilege. It is entirely reasonable to infer that, given the complex nature of the Internet, there is a certain likelihood of risk involved with a hacker intercepting a communication intended as confidential. Because the information gets channeled through many systems of networks, as recognized in *Reno*,[158] it is likely that someone could intercept the communication along its destination path. While *Maxwell* might not seem to be concerned with the potential need for encryption given the objective expectation of privacy of e-mail messages,[159] *Reno* presents a different picture because

---

[155]*Reno*, 929 F. Supp. at 830-36.

[156]*Id.* at 830. This rather "reticular" description of the Internet as a network of networks bears a similarity to the reticular formation of certain nerve fibers in the human brain. The reticular formation is defined broadly as "a substantial portion of the dorsal part of the brain stem in which the groups of neurons and intersecting bundles of fibers present a *netlike* (reticular) appearance in transverse sections." MURRAY L. BARR & JOHN A. KIERNAN, THE HUMAN NERVOUS SYSTEM, AN ANATOMICAL VIEWPOINT 149 (6th ed. 1993) (emphasis added). This reticular formation analogy is apt in light of the court's comment that "[i]t is no exaggeration that the content on the Internet is as diverse as human thought." *Reno*, 929 F. Supp. at 842. Interestingly, the reticular formation is involved with sleep and consciousness. BARR & KIERNAN, *supra*, at 149.

[157]*Reno*, 929 F. Supp. at 832.

[158]*Id.* (stating that "messages between computers on the Internet do not necessarily travel entirely along the same path").

[159]*Maxwell*, 45 M.J. at 417 (stating that "AOL differs from other systems, specifically the Internet . . . in that e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-

of the public nature of the Internet. In fact, the court in *Reno* specifically suggested the need for encryption:

> One method of communication on the Internet is via electronic mail, or "e-mail," comparable in principle to sending a first class letter. One can address and transmit a message to one or more people. E-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail *generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and the recipient (unless the message is encrypted).*"[160]

Reno is the only case, affirmed by the Supreme Court, that has explicitly mentioned encryption. The following table summarizes the various analyses presented thus far in this note.

TABLE 1: SUMMARY OF MODELS

MODEL	JUSTIFICATION(S)	LIMITATIONS
Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc. & *Mendenhall v. Barber-Greene Co.*	1. Demonstrates the chaos and confusion within the jurisdictions regarding the attorney-client privilege. 2. Suggests the need for *Upjohn*'s expansion of the scope of the privilege.	1. *Sew 'N Sweep* is called into question within its own jurisdiction. 2. Conflicts with *Mendenhall* thus results are inconclusive under this model.

owned computer bank").

[160] *Reno*, 929 F. Supp. at 834.

Upjohn Co. v. United States	1. Leading case on the corporate attorney-client privilege. 2. Expands the scope of the privilege.	1. Not followed in all jurisdictions.
Maxwell v. United States	1. E-mail communication in the private sector. 2. Explicitly states that a hacker will not defeat the legitimate expectation of privacy of a private e-mail communication.	1. Criminal case. 2. Addressing e-mail communications in the context of Fourth Amendment search and seizure issues.
ACLU v. Reno	1. E-mail communication in the public arena: the Internet. 2. Detailed factual analysis of the Internet. 3. Explicitly suggests encryption.	1. Does not address attorney-client privilege. 2. Addresses First Amendment and Due Process issues.
Canon 4	Ethical considerations.	Language not determinative of outcome: "*should preserve.*"
Rule 1.6	ABA Model Rule of Professional Conduct.	Unclear and conflicts with Canon 4.

Combining the above Models with the Canons of Ethics and Model Rules, it appears that the trend suggests a need for data encryption.[161]

[161]One might add that the need for data encryption extends even into the private domain when one transmits messages via a company such as America Online because even as

This seems reasonable, especially in light of the findings of fact set forth in *Reno*, which strongly suggest that communication over the Internet is not confidential.[162] Lending even greater power to this suggestion is the Supreme Court's decision affirming the district court holding and its subsequent summary of the lower court's findings of fact.[163] It is important to notice that the District Court for the Eastern District of Pennsylvania and the Supreme Court agreed that it was *crucial* to understand the factual findings in order to analyze the legal issues.[164] Following along the chain of reasoning from the Illinois cases through *Upjohn* and then through the *Maxwell-Reno* link, it seems completely reasonable to require data encryption for attorney-client communications. Though the Canons of Ethics and the Model Rules are not presently capable of aiding the lawyer to answer whether or not he should encrypt such communications, the logical inference from current case law in light of the ethical considerations suggests that encryption might be necessary.[165] Furthermore, encryption might be ethically prudent.

IV. NEGLIGENCE AND THE HAND CALCULUS

Failure to encrypt could lead the attorney into a potential malpractice action.[166] Negligence and a standard somewhat above mere negligence is suggested in the language of *Mendenhall*:

Reno suggests, there are millions of subscribers in the private domain. *Id.* at 833.

[162]*Id.* at 834.

[163]Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2334 (1997).

[164]*See Reno*, 929 F. Supp. at 830 (stating that "[a]ll parties agree that in order to apprehend the questions at issue in these cases, it is necessary to have a clear understanding of the exponentially growing, worldwide medium that is the Internet"). *See also Reno*, 117 S. Ct. at 2334, stating that:

> [t]he District Court made extensive findings of fact, most of which were based on a detailed stipulation prepared by the parties. The findings describe the character and the dimensions of the Internet . . . [b]ecause those findings provide the underpinnings for the legal issues, we begin with a summary of the undisputed facts.

Id. (citations omitted).

[165]*See* discussion *supra* notes 158-61 and accompanying text and Table 1 summary. It is even interesting to note that California requires that a lawyer maintain the confidences of his client *at his peril: "It is the duty of an attorney to do all of the following . . . (e) [t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."* CAL. BUS. & PROF. CODE § 6068(e) (West 1990 & Supp. 1997). At the very least, the California Code suggests a negligence standard might be appropriate for a potential breach of the attorney's duty toward his client.

[166]*See* Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982).

> Mendenhall's lawyer (not trial counsel) might well have been negligent in failing to cull the files of the letters before turning over the files. But if we are serious about the attorney-client privilege and its relation to the *client's* welfare, we should require more than such negligence by counsel before the client can be deemed to have given up the privilege.[167]

A failure to take adequate precautions to safeguard confidential materials might also result in reprimand: "Reprimand is generally appropriate when a lawyer negligently reveals information relating to representation of a client not otherwise lawfully permitted to be disclosed and this disclosure causes injury or potential injury to a client."[168] The commentary to Standard 4.23, as quoted above, suggests that one appropriate case for reprimand might "involve a lawyer who negligently leaves a client's documents in a conference room following a meeting, or who discusses a client in a public place."[169] Under a negligence theory, one would have to show a breach of duty to the client and a resulting injury or *potential* injury to the client as a result of the breach. The duty towards the client is already well established once the attorney-client relationship is settled because of the fiduciary nature of the relationship.[170]

What is less clear, however, is the degree of precaution that an attorney must take in the case of whether to encrypt e-mail communications with a client. Fundamental to the degree of precaution or reasonable conduct required is the concept of risk and, in particular, reasonable and unreasonable risks.[171] One commentator has stated:

---

[167]*Id.*

[168]ABA STANDARDS FOR IMPOSING LAWYER SANCTIONS Standard 4.23 (1986) (amended 1992).

[169]*Id.* See also Schwartz v. Wenger, 124 N.W.2d 489 (Minn. 1963), in which the court concluded that:

> where the attorney and client have chosen a public place in which to discuss matters pertaining to their professional relationship, and a third person overhears their conversation without resorting to surreptitious methods, they are deemed to have waived the privilege they might otherwise have enjoyed in so far as the testimony of the third person is concerned

Id. at 492. The court further suggested that the attorney in this case might face disciplinary action. *Id.* at 493.

[170]Recall the attorney-client relationship described in terms of a duty: "Except to the extent authorized by a code of professional responsibility, an attorney has a *duty* to preserve both a client's confidences and secrets, and may not reveal a confidence or secret of the client without the client's consent." 7 C.J.S. *Attorney & Client* § 52 (1980) (emphasis added).

[171]*See* Henry T. Terry, *Negligence*, 29 HARV. L. REV. 40, 42-44 (1915).

> To make conduct negligent the risk involved in it must be unreasonably great; some injurious consequences of it must be not only possible or in a sense probable, but unreasonably probable. It is quite possible in the business of life to avoid taking risks of injury to one's self or others, and the law does not forbid doing so; what it requires is that the risk be not unreasonably great. The essence of negligence is unreasonableness; due care is simply reasonable conduct. There is no mathematical rule of percentage of probabilities to be followed here.[172]

Realistically, one cannot assign a mathematical equation to a lawyer's duty to prevent injury to a client; however, Circuit Judge Learned Hand attempted one such nonlinear relationship to describe prevention of injury to another in *United States v. Carroll Towing Co.*[173] In *Carroll Towing*, a barge (the "Anna C") broke loose and drifted until it struck a tanker and subsequently began to leak and lose its cargo of flour.[174] Another barge might have been able to prevent the "Anna C" from leaking, however, no bargee was on board the "Anna C" to observe the presence of the leak.[175] The issue then became "whether a barge owner is slack in the care of his barge if the bargee is absent."[176] Judge Hand recognized that one could interpret the problem of the owner's duty to prevent injury to others mathematically[177] in what has commonly been referred to as the "Hand Calculus." The Hand Calculus relationship is as follows:

EQUATION 1: HAND CALCULUS

$$B < PL$$[178]

In this coupled inequality, "B" represents the "burden of adequate precautions,"[179] "P" means the "probability that she [a barge] will break away,"[180] and "L" represents the "gravity of the resulting injury"[181] if the

---

[172] *Id.* at 42.

[173] 159 F.2d 169 (2d Cir. 1947).

[174] *Id.* at 171.

[175] *Id.*

[176] *Id.* at 172.

[177] *Carroll Towing*, 159 F.2d at 173.

[178] *Id.*

[179] *Id.*

[180] *Id.*

barge did break away. Judge Hand postulated that the liability imposed upon the owner of a barge would depend on whether the burden (B) was less than the scalar product[182] of probability (P) and gravity of injury (L).[183] However, Judge Hand provided no derivation for his formula and relied instead on a common-knowledge approach to the mathematical relationship. Graphically, liability might be imposed for a shaded region represented below the dotted "line" of $B < PL$.[184]

The Hand Calculus is limited in part because no simple mathematical relationship, without more, can really ever describe such a complex concept as one's tort duty to avoid injuries to another. Thus, the relationship as it stands is overly simplistic.[185] Judge Hand did not consider the necessity of other factors to be explicitly included in the calculation.[186] Especially in the context of the possible need for data encryption, the Hand Calculus falls short because it fails to consider all of the complicating factors involved. The complicating factors plaguing data encryption include: the burden in terms of both economic burden and the burden on restricting the free-exchange of communication in furtherance of the legal process; the probability that a hacker might intercept the communication given the two different arenas (private and public); and the probability that, given all of the mass forms of communication, a hacker could intercept materials of a legal as opposed to a business nature, and, finally, all of the various injuries possible to the client. One can imagine the varying degrees of injury spanning the spectrum of disclosure of information pertaining to high-profile cases to those situations in which disclosure is "embarrassing or . . . detrimental to the client."[187] In the context of the need for data encryption, burden, probability, and injury take on multi-dimensional meanings. A revised

---

[181]*Carroll Towing*, 159 F.2d at 173.

[182]Scalar product means multiplication. Hence, "PL" in the equation means "P" multiplied by "L."

[183]*Id.*

[184]Typically, linear inequalities may be represented graphically with the area in question shaded just below or above a dotted "line." A dotted line suggests that the numbers falling on the line are not included in the solution set while a solid line suggests that the numbers are included in the solution set. In this case, the "line" would be dotted; however, in this situation, two of the variables — probability and injury — are actually coupled, which implies a nonlinear or "chaotic" relationship. Thus, this relationship might not be entirely linear.

[185]Hand subtly suggests limitations on the calculus when he posits that the "likelihood that a barge will break from her fasts and the damage she will do vary with place and time." *Carroll Towing*, 159 F.2d at 173.

[186]*Id.*

[187]MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(A) (1983).

Hand Calculus that considers the complexities described above might look something like:

EQUATION 2: REVISED HAND CALCULUS
$B(c,s) < P(p1,p2)*L(n0 \ldots n)$[188]

Where in this context, burden (B) is now a function of cost for the attorney (c) as well as a function of concern over the flow of speech (s) necessary to further the judicial process. Probability (P) becomes a function then of likelihood of interception in the private (p1) and public (p2) arenas — from America Online to the Internet respectively. Injury (L) considers differing magnitudes of injuries in addition to the mere potential for injury considered in the standards for sanctions.[189] While this is one additional approach for "measuring" the need for data encryption, this type of analysis is limited because it arguably does not consider the broad spectrum of complexities inherent in the data encryption issue. Neither the Hand Calculus nor the revised Hand Calculus presented take into account the Canons of Ethics and the Codes of Professional Responsibility, and this is problematic when one is concerned with the ethical implications of the need for data encryption.

Perhaps the most telling statement from Judge Hand derives not from his opinion in *Carroll Towing*, but rather from his opinion in *T.J. Hooper*,[190] fifteen years prior to *Carroll Towing*. In *T.J. Hooper*, Hand states:

> Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[191]

---

[188]This mathematical relationship is the author's own interpretation of one potential revision of the Hand Calculus in the context of the need for data encryption.

[189]ABA STANDARDS FOR IMPOSING LAWYER SANCTIONS Standard 4.23 (1986) (amended 1992).

[190]T.J. Hooper, 60 F.2d 737 (2d Cir. 1932).

[191]*Id.* at 740.

The better measure of the need for data encryption may lie, instead in Hand's "common prudence" analysis[192] rather than in the Hand Calculus or any revised mathematical formula. At least under the T.J. *Hooper* reasoning, the only calculation that need be made is one of "common prudence."[193] The following table summarizes the various models studied and the potential need for data encryption.

TABLE 2: NEED FOR DATA ENCRYPTION

MODEL	NEED FOR ENCRYPTION
Canon 4 and Rule 1.6	INCONCLUSIVE.
Sew 'N Sweep-Mendenhall	LIKELY - to ensure that adequate precautions were taken to safeguard confidentiality.
Upjohn-Maxwell-Reno	YES - though it might not be entirely necessary with regard to a private company, in the public arena such as with the Internet, it becomes crucial to encrypt.
Carroll Towing-T.J. Hooper-Standard 4.23	MOST LIKELY - especially under a "common prudence" analysis.

V. CONCLUSION

Charles Dickens once wrote that "[i]t's in vain . . . to recall the past, unless it works some influence upon the present."[194] Appealing to the older tort cases such as *Carroll Towing* and *T.J. Hooper* is not a vain act. These cases have endured and been appealed to over the course of nearly a half century. Although limited in their own ways, they still provide solid paradigms for analyzing a lawyer's obligation to prevent

[192] *Id.*

[193] *Id.*

[194] DICKENS, *supra* note 1, at 319.

disclosure of confidential client communications. If nothing more, they suggest a "common prudence"[195] approach to reasonable safeguards.

In addition, *Upjohn* must be included in the calculus of confidentiality at some point for its policy-driven, functionalist approach to the privilege. *Upjohn* becomes imperative to prevent the chaos and confusion as witnessed in the Illinois courts. Moreover, where *Upjohn* is limited, *Maxwell* and *Reno* might be able to fill in any gaps in the equation. Extrapolating all of the above discussed models into a final Hand Calculus, one finds a highly complex set of "equations" which eventually settle into the use of common sense to prevent any uncomfortable disclosures of confidential materials.

Jeanne Andrea Di Grazio

[195] *T.J. Hooper*, 60 F.2d at 740.

INTER-MODAL RAIL: WILL ERISA'S NEWLY DEFINED WELFARE BENEFIT NONINTERFERENCE CLAUSE CURB OUTSOURCING?

I. INTRODUCTION

Since the late 1980s, companies have practiced "outsourcing" as a means of controlling costs and bolstering the fiscal bottom-line.[1] Outsourcing typically involves subcontracting certain routine business functions to outside contractors specializing in these services, or seeking outside assistance when specialized expertise is needed.[2] By outsourcing, companies realize cost savings on salaries, employee benefit plans, and various other overhead costs which would otherwise be incurred if they maintained their own in-house staff to perform these tasks.[3] Not surprisingly, outsourcing is predicted to grow twenty-three percent in the next year into a $180 billion global business,[4] with expansion not limited to magnitude, but including growth in the scope of services sought as well.[5]

Although the outsourcing juggernaut appeared to be unstoppable, the Supreme Court's decision in *Inter-Modal Rail Employees Ass'n v. Atchison, Topeka & Santa Fe Railway*[6] may have shattered this illusion, at least temporarily, by raising some doubts about the legality of this increasingly popular business practice. Because pension and welfare benefit plan cost savings are often a significant consideration when a company decides to outsource, an employer's action affecting these benefits may come under the federal scrutiny of the Employee Retirement

---

[1]*See* Scott M. Riemer, *Corporate Outsourcing and ERISA § 510*, N.Y. L.J., June 27, 1997, at 1.

[2]Typical services that are outsourced include information technology, marketing and sales, financial/accounting, and administration. *First Outsourcing Index Predicts 35 Percent Outsourcing Growth*, Bus. Wire, Feb. 13, 1997, *available in* WESTLAW, BWIRE database. Other common outsourced functions include human resources, tax, and legal services. *Outsourcing Growing Rapidly into a $180 Billion Global Business; Legal and Tax Services Get Highest Satisfaction Ratings from Top Executives, New Research Shows*, PR NEWSWIRE, Sept. 19, 1997, *available in* WESTLAW, PRWIRE database [hereinafter *Outsource Growing Rapidly*].

[3]One source estimates average cost savings to employers are between 12% to 22% for outsourcing. *Outsourcing's Second Wave*, INVESTOR'S BUS. DAILY, Oct. 19, 1995, at A4.

[4]*Outsourcing Growing Rapidly*, *supra* note 2. U.S. companies alone are predicted to spend more than $100 billion this year in outsourcing. Del Jones, *Supreme Court Ruling May Stem Outsourcing*, USA TODAY, May 13, 1997, at 5B.

[5]*Outsourcing's Second Wave*, *supra* note 3, at A4.

[6]117 S. Ct. 1513 (1997).