

RESISTING ELECTRONIC DISCOVERY: EXPANDING ATTORNEY-CLIENT PRIVILEGE, WORK PRODUCT PRIVILEGE, AND THE RIGHT TO PRIVACY

Oscar Franklin B. Tan
Kristina P. Castaneda

TABLE OF CONTENTS

INTRODUCTION.....	732
I. OVERVIEW OF THE INTERNET AND ELECTRONIC DISCOVERY....	737
A. An Overview of the Internet.....	737
B. Electronic Mail: Casually Used and Casually Overlooked.....	739
II. THE ATTORNEY-CLIENT PRIVILEGE	743
A. History of the Attorney-Client Privilege.....	743
B. The Attorney-Client Privilege Today.....	746
III. APPLICATION OF THE ATTORNEY-CLIENT PRIVILEGE.....	752
A. Expanding the Application of the Privilege.....	752
B. The Confidentiality of E-mail.....	760
C. Dealing with Inadvertent Disclosure.....	764
IV. THE WORK PRODUCT PRIVILEGE	775
V. APPLICATION OF THE WORK PRODUCT PRIVILEGE	780
VI. INSUFFICIENCY OF THE PRIVILEGES	788
VII. THE CONSTITUTIONAL RIGHT TO PRIVACY	796
A. Decisional Privacy and the Due Process Clause.....	796
B. The Penumbra and Informational Privacy.....	804
C. Informational Privacy and Unreasonable Search.....	807
D. Informational Privacy and the Right Against Self-Incrimination	819
E. Informational Privacy and Speech, Association and Anonymity	821
VIII. APPLICATION OF THE RIGHT TO PRIVACY	825
IX. CONCLUSION	837

RESISTING ELECTRONIC DISCOVERY: EXPANDING ATTORNEY-CLIENT PRIVILEGE, WORK PRODUCT PRIVILEGE, AND THE RIGHT TO PRIVACY*

Oscar Franklin B. Tan**

Kristina P. Castaneda***

"No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case."

—Justice Francis William Murphy, *Hickman v. Taylor* (1947)¹

"Litigation should not be carried on in the dark... [T]he rules on discovery are accorded broad and liberal interpretation."

—Justice Artemio Panganiban,
Security Bank v. Court of Appeals (2000)²

* The ideas in this article were formed during this author's early forays into the right to privacy and Internet law. Oscar Franklin Tan, *Touch Me Not: Expanding Constitutional Frameworks to Challenge LTO-Required and Other Mandatory Drug Testing*, 76 PHIL. L.J. 618 (2002); Oscar Franklin Tan, *Sticks and Stones May Break Bones But Can E-Mail Ever Hurt Me?: Exploring the Application of Tort Doctrine to the Internet's Constitutional Dilemmas* (Mar. 2003) (unpublished 2003 Baviera Prize paper on file with the Dean's Office and Professor Araceli Baviera). Cite as Oscar Franklin Tan & Kristina Castaneda, *Resisting Electronic Discovery: Expanding Attorney-Client Privilege, Work Product Privilege, and the Right to Privacy*, 79 PHIL. L.J. 732, (page cited) (2004).

** Chair, PHILIPPINE LAW JOURNAL; Member, Student Editorial Board (2004). Fourth Year, LL.B., University of the Philippines (2005 expected). B.S. Management Engineering / A.B. Economics Honors, *Cum Laude*, Ateneo de Manila University (2001). First Freshman Awardee, Justice Irene R. Cortes Prize for Best Paper in Constitutional Law (2002). Awardee, Professor Araceli T. Baviera Prize for Best Paper in Civil Law (2003). First Awardee, Professor Bienvenido C. Ambion Prize for Best Paper in Private International Law (2004).

This author hopes this piece honors his Remedial and Constitutional Law professors: Antonio Bautista, Anacleto Diaz, Teresita Herbosa, Rogelio Vinluan Eduardo Robles, Carmelo Sison, Marvic Leonen, Rudyard Avila, and Florin Hilbay. He especially hopes that it honors Deans Pacifico Agabin and Raul Pangalangan, and the second half of this paper is an offshoot of freshman year conversations with them regarding the right to privacy and a thirty-minute argument with Professor Hilbay in his office regarding the right's true origin.

*** Second Year LL.B., University of the Philippines (2007 expected). B.S. Management Economics, Ateneo de Manila University (2003).

¹ *Hickman v. Taylor*, 329 U.S. 495, 507 (1947), *quoted in* *Republic v. Sandiganbayan*, G.R. No. 90478, Nov. 21, 1991.

"[T]o the extent that [discovery] permits a plaintiff with a largely groundless claim to simply take up the time of a number of other people, with the right to do so representing an in terrorem increment of the settlement value, rather than a reasonably founded hope that the process will reveal relevant evidence, it is a social cost rather than a benefit."

—Justice William Rehnquist,
Blue Chip Stamps v. Manor Drug Stores (1975)²

"Somewhere, something incredible is waiting to be known," said American astronomer and writer Carl Sagan.⁴ This thought animates the hundreds of law review articles on the discovery of electronic evidence around the world.⁵ One called it "the hottest topic in legal technology."⁶ Another called electronic discovery a "treasure trove" and the "modern litigator's newest tool,"⁷ something that should be used to sift through an opponent's backup systems and his former employees' personal computers.⁸ Still another stated that the ability to manipulate electronic data has become so indispensable to comprehending it that producing printouts in response to a subpoena is considered abusive,⁹ and with such ability, it is no longer

² *Security Bank Corp. v. Court of Appeals*, G.R. No. 135874, 323 SCRA 330, 333, Jan. 25, 2000.

³ *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 741 (1975).

⁴ ThinkExist.com, Carl Sagan at

http://www.thinkexist.com/English/Author/x/Author_2479_1.htm (last visited Feb. 28, 2004).

⁵ Some of the sentiment was already reduced to writing as early as 1980. For example, "[W]e know we now live in an era when much of the data which our society desires to retain is stored on computer disks. This process will escalate in years to come; we suspect that by the year 2000 virtually all data will be stored in some form of computer memory." *National Union Electric Corp. v. Matsushita Electric Industrial Co.*, 494 F.Supp. 1257, 1262-63 (E.D. Pa. 1980).

⁶ Toby Brown, *Electronic Discovery Basics*, 52-AUG R.I. B.J. 7, 7 (2003).

⁷ Carol Heckman & Jerold Brydges, *Winning Electronic Discovery Motions*, 4 SEDONA CONF. J. 151, 151 (2003). See Lesley Rosenthal, *Electronic Discovery Can Unearth Treasure Trove of Information or Potential Land Mines*, 75-SEP N.Y. ST. B.J. 32, 32 (2003).

⁸ Clyde Wilson & Douglas Cherry, *Success in Electronic Discovery*, 39-MAY TRIAL 60, 61 (2003). "With the trend toward the paperless office, there is more to discover in a corporation's computer network than there is in its filing cabinets." *Id.* at 60.

⁹ Kenneth Withers, *Advanced Discovery Issues: Discovery and Protection of Electronic Data*, SH093 ALI-ABA 737, 741 (2003). See *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 427 (S.D.N.Y. 2002). "The plaintiffs would also forego the use of TIFF files, which they argue is unnecessary and unduly expensive. According to one of the plaintiffs' consultants, Charles R. Kellner of Electronic Evidence Discovery, Inc. ("EED"), TIFF files are not themselves searchable, since they are merely graphic depictions of electronic text. Because they are not searchable, they do not facilitate the removal of duplicate documents from a file. And, as an image of an

assumed unreasonable for a judge to order the production of millions of pages' worth of data.¹⁰ The topic has grown to the point that individual journal articles are devoted even to the recruitment of the right "computer forensic expert."¹¹

The wide-eyed wonder is universal, such that a recent issue of the PHILIPPINE LAW JOURNAL even proclaimed:

The real issue that comes to the fore is whether legal practitioners are willing and ready to accept the paradigm shift in litigation that discovery seeks to usher in – litigation guided by disclosure of truth and not by the inclination to suppress the truth.¹²

Seemingly, every trial lawyer who realizes that computers exist today has suddenly been transformed, by a stroke of Rule 27,¹³ into an Archimedes

electronic document, the TIFF version contains less information than the original document." Michael Traynor and Lori Ploeger, *Hot Topics in Electronic Discovery*, 712 PLI/PAT 51, 66 (2002), citing *Anti-Monopoly v. Hasbro, Inc.*, 1995 WL 649934, at *2 (S.D.N.Y. 1995); *In re Air Crash Disaster at Detroit Metro. Airport*, 130 F.R.D. 634, 636 (E.D. Mich. 1989); *National Union Electric Corp. v. Matsushita Electric Industries Co.*, 494 F. Supp. 1257 (E.D. Pa. 1980); *United States v. Davey*, 543 F.2d 996, 1000 (2nd Cir. 1976).

¹⁰ Steven Bennett & Thomas Niccum, *Two Views from the Data Mountain*, 36 CREIGHTON L. REV. 607, 619-20 (2003).

¹¹ Wade Davies, 27-JUN CHAMPION 30, 31 (2003). The term is already recognized by the Philippine Supreme Court. According to a news report, "computer forensics experts from the Supreme Court" reviewed how disbarred lawyer Danilo de Guzman used a simple network connection in a law office to access the computer of his boss and bar examiner Marcial Balgos. De Guzman then obtained a copy of the bar questions Balgos typed and leaked them to his fraternity brothers, leading to de Guzman's disbarment. Although it was an unsophisticated exercise that could have taken place over school, office, or even home computers inexpensively connected with a set of cables, it is a start for Philippine electronic evidence. Erwin Oliva, *Computer experts show how bar exam questions hacked*, PHIL. DAILY INQUIRER, Mar. 8, 2004, at C1.

¹² Edgardo Carlo Vistan, *The Philippine Voyage into Electronic Discovery*, 78 PHIL. L.J. 27, 30 (2003).

¹³ RULES OF COURT, Rule 27, § 1. "Section 1. Motion for production or inspection—Upon motion of any party showing good cause therefor, the court in which an action is pending may (a) order any party to produce and permit the inspection and copying or photographing, by or on behalf of the moving party, of any designated documents, papers, books, accounts, letters, photographs, objects or tangible things, not privileged, which constitute or contain evidence material to any matter involved in the action and which are in his possession, custody or control; or (b) order any party to permit entry upon designated land or other property in his possession or control for the purpose of inspecting, measuring, surveying, or photographing the property or any designated

crying "Eureka!",¹⁴ a young D'Artagnan offered the Queen's hand to kiss in the darkness,¹⁵ or even a Jonathan Harker who thinks he has accounted for all of Count Dracula's hidden lairs.¹⁶ Amidst this intoxicating sense of marvel, however, one wonders if too many litigators have forgotten a much older reality: That there are two sides to every litigation.

Simply, what is one to do if one finds oneself on the *receiving* end of a subpoena for gigabytes of electronic information?

In the face of "the pervasiveness of information," another author wrote, "Without an adequate standard for limiting digital discovery, however, in-house lawyers must assume that their companies will be subject to requests for discovery of virtual mountains of electronic information."¹⁷ With molehills electronically transformed into mountains, discovery stands to be anything but speedy and inexpensive, leading a New York Justice to quip, "[T]oo often, discovery is not about uncovering the truth, but about how much truth the parties can afford to disinter."¹⁸

This paper seeks to stifle some of the euphoria that surrounds electronic discovery, and trek the far more difficult, less explored road of blunting it. Again, there are two sides to every litigation, and no lawyer should accept that technological advances make the offense the best stance to take before going to trial. Though they have received much less in-depth

relevant object or operation thereon. The order shall specify the time, place and manner of making the inspection and taking copies and photographs, and may prescribe such terms and conditions as are just."

¹⁴ Marjorie Dorfman, *The BathTub: Archimedes, Eureka, The Bath And Beyond, Home is Where the Dirt is*, at <http://www.housenotsobeautiful.com/Articles/bath.html> (last visited Feb. 28, 2004).

¹⁵ ALEXANDRE DUMAS, *THE THREE MUSKETEERS* 219 (Signet Classic, 1991) (1844). "Finally, a hand and an arm, surpassingly beautiful in their form and whiteness, came through an opening in the tapestry. D'Artagnan at once understood that this was his reward. He fell to his knees, took the hand, and touched it respectfully with his lips."

¹⁶ BRAM STOKER, *DRACULA* 365 (Penguin, 1994) (1897). "There he turned and spoke to us: 'You think to baffle me, you - with your pale faces all in a row, like sheep in a butcher's. You shall be sorry yet, each on of you! You think you have left me without a place to rest; but I have more. My revenge is just begun! I spread it over centuries and time is on my side.'"

¹⁷ Kenneth Dort & George Spat, *Discovery in the Digital Era: Considerations for Corporate Counsel*, 20 NO. 9 COMPUTER & INTERNET LAW. 11, 11 (2003).

¹⁸ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 423 (S.D.N.Y. 2002), quoted in Stephen Snyder & Abigail Crouse, *Applying Rule 1 in the Information Age*, 4 SEDONA CONF. J. 165, 165 (2003).

academic discussion, the two most common defensive weapons are the attorney-client privilege and the work product privilege.¹⁹ When these are invoked and established, the target of discovery is no longer obliged to make the disclosures, and one must realize that these privileges expand along with the residual records left behind by today's computer processes. Given the dearth of Philippine material, this paper will explore the history and application of both privileges in American jurisprudence, and show that they find wider application than one might think. The work product privilege is especially important to the Philippine practitioner, because it has very tenuous foundations in jurisprudence to date, yet is becoming increasingly important in the United States.

The paper, however, will then show that the arsenals provided by present procedure are woefully lopsided. The defending party is placed at a severe disadvantage because the very slope of the terrain is pitted against him; the present mentality, especially as gleaned from the language of the landmark cases *Republic v. Sandiganbayan*²⁰ and *Security Bank v. Court of Appeals*,²¹ is to treat discovery and production as the general rule and privilege as the exception. It is little explored, however, that the 1987 Constitution may mandate a leveling of this playing field, and a stricter view of discovery at least with respect to electronic documents.

Where a man's most intimate, everyday thoughts might have once been left in a small, yellowed diary, they are sprinkled over a trail of e-mail and personal records today.²² The ease with which a man leaves written documentation of his life brings the Constitutional right to privacy to the

¹⁹ Eric Van Buskirk, *Practical Strategies for Digital Discovery*, 32-SPG BRIEF 50, 51 (2003); Carey Sirota Meyer & Kari Wraspir, *E-Discovery: Preparing Clients for (and Protecting Them Against) Discovery in the Electronic Information Age*, 26 WM. MITCHELL L. REV. 939, 953 (2000). A third piece of armor is the confidentiality of trade secrets and proprietary material. Sheila Carpenter & Shaunda Patterson, *Discovery of Electronic Documents*, 29-SUM BRIEF 64, 66 (2000). For example, a particular computer program itself might be proprietary. Francis Burke, *The Discoverability of Computerized Information*, SH037 ALI-ABA 63, 99 (2003). However, this will not be discussed in this paper. See *Fortune Corp. v. Court of Appeals*, G.R. No. 108119, January 19, 1994; *Microwave Research Corp. v. Sanders Associates, Inc.*, 110 F.R.D. 669, 672 (D. Mass. 1986). Finally, one author discusses hearsay exceptions applied to e-mail. Mark Robins, *Evidence at the Electronic Frontier: Introducing E-Mail at Trial in Commercial Litigation*, 29 RUTGERS COMPUTER & TECH. L.J. 219 (2003).

²⁰ *Republic v. Sandiganbayan*, G.R. No. 90478, 204 SCRA 212, Nov. 21, 1991.

²¹ *Security Bank Corp. v. Court of Appeals*, G.R. No. 135874, 323 SCRA 330, Jan. 25, 2000.

²² See Nicholas Barone, *Computer Discovery*, SG007 ALI-ABA 539, 541 (2001).

fore, and as Justice Reynato Puno's *ponencia* in *Ople v. Torres* noted, society has "lost its benign capacity to forget."²³

This paper will discuss the history and doctrine of privacy, as well as American decisions that have increasingly, explicitly honored it in discovery. It will show that in many cases, discovery should be barred altogether, instead of merely denying admissibility later at trial. It will then end by summarizing the ideas and jurisprudence presented into a call to review discovery rules, such that individuals need not go through everyday business fearing that their every stray word will be thrown back at them in litigation, as though in a virtual Panopticon.²⁴

I. AN OVERVIEW OF THE INTERNET AND THE POTENTIAL OF ELECTRONIC DISCOVERY

A. AN OVERVIEW OF THE INTERNET

The Internet changed the way we do things today, and has become a significant part of daily routines. It has become omnipresent, used by people from the teenager surfing the Net from the comfort of his bedroom to the multinational conglomerates who rely on it in order to communicate from across various ends of the globe. The Internet has become an important part of our world, and it has become so with remarkable speed.²⁵

The Internet was not originally intended to be used the way it is today. In the 1960s, a group associated with the Defense Advanced Research Projects Agency devised systems to move programs and data between the relatively few large computers used for defense-related research, primarily for load sharing and remote entry of jobs. That evolved into the

²³ *Ople v. Torres*, G.R. No. 127685, 293 SCRA 141, Jul. 23, 1998.

²⁴ JEREMY BENTHAM, *Panopticon*, in *THE PANOPTICON WRITINGS* (Miran Bozovic ed., 1995). Bentham depicted a prison whose cells' walls were made of clear glass, allowing a guard in a central watchtower to monitor prisoners' every action round the clock. See CTRL [SPACE]: RHETORICS OF SURVEILLANCE FROM JEREMY BENTHAM TO BIG BROTHER, (Thomas Levin et al. ed., 2002).

²⁵ Allan Brill, *The Technologies of Privacy and Privacy Invasion: An Introduction*, 748 PLI/PAT 85, 93 (2003).

military data network, or Milnet, and eventually into what became known as the Internet.²⁶

Today, the Internet is nothing more or less than tens of thousands of interconnected computer networks that follow a number of common rules or protocols for sending various kinds of information between users. There are protocols for web pages, e-mail, instant messages, file transfers and dozens of other specific kinds of transmissions.²⁷

Written communications are an important part of evidence, and this makes the Internet important to practitioners because it is primarily a means of communication. However, electronic evidence is broader than Internet evidence, and includes:

- Computers network and connected by cable but not necessarily through the Internet, with networked hard drives and local drives "shadowing" each other
- "Disaster" recovery procedures which may retrieve deleted files
- Information in laptop computers and personal digital assistants (PDAs)
- Document management and word processing programs
- New e-mail handlers, such as Microsoft Exchange 2000, which allow full text indexing of e-mails and attachments
- Internet-based applications that allow multiple users to simultaneously create and edit (and delete) files and information
- Financial and data processing programs²⁸

"And just as the ocean is not just water, electronic data is not just another way to store information."²⁹ In requesting for production of

²⁶ Barry Leiner et al., *Internet Society: A Brief History of the Internet*, at <http://www.isoc.org/internet/history/brief.shtml> (last visited Feb. 28, 2004).

²⁷ Brill, *supra* note 25, at 94.

²⁸ Jonathan Redgrave & Ted Hiser, *Fishing In The Ocean, A Critical Examination Of Discovery In The Electronic Age*, 2 SEDONA CONF. J. 195, 196-97 (2003).

²⁹ *Id.* at 196.

communications, for example, one should now specifically include those done electronically such as e-mail.³⁰

B. AN OVERVIEW OF ELECTRONIC MAIL: CASUALLY USED AND CASUALLY OVERLOOKED

Electronic mail or e-mail is one of the most widely-used conveniences brought by the Internet into this world. What was once accomplished by a note or a phone call is now communicated by e-mail. Further, Instant Messaging ("IM") programs³¹ have moved from home to office use, where workgroup members can zap short, one-line messages back and forth as fast as they can type, resulting in a real-time conversation albeit using a keyboard.³² The pervasiveness of e-mail is described:

In 1998, the U.S. Postal Service processed approximately 1.98 billion pieces of mail. During that year, there were approximately 47 million e-mail users in the United States who sent an estimated 500 million e-mail messages per day, for a total of approximately 182.5 billion e-mails – more than 90 times as many messages as the U.S. Postal Service handled.³³

On servers, hard drives and other electronic media worldwide, data mounts up by the nanosecond. By one measure, 99.997% of all information storage is now in electronic form; printed material of all kinds makes up less than .003% of all stored information.³⁴

Nearly all critical business records, and much personal correspondence are now generated and stored electronically.³⁵

³⁰ Michael Connolly & A.W. Phinney, *Requests for Documents and Things and for Entry Upon Land*, I MASSACHUSETTS DISCOVERY PRACTICE (Main Handbook), chap. II, §11.2.6 (2002).

³¹ These use small windows on one's computer screen where one types short messages that are displayed real-time for all users to see. As messages fill the window, the result is similar to the transcript of a conversation, except one can instantaneously add to it. Instant messenger programs facilitate one-on-one "chats," and even keep a real-time list of friends whose Internet connections are on and thus available to talk. See <http://messenger.yahoo.com>; <http://www.aol.com/aim/home.html>.

³² Brill, *supra* note 25, at 93.

³³ Jonathan Redgrave, *The Sedona Conference Working Group on Electronic Document Retention and Production*, 4 SEDONA CONF. J. 197, 200 (2003).

³⁴ Rosenthal, *supra* note 7, at 32.

³⁵ *Id.*

Such widespread use is easily explained: E-mails are cheaply transmitted, instantaneously sent, and can carry large amounts of data. E-mails and attached electronic documents are also far more easily and quickly replicated than printouts, and without degradation. Common e-mail programs, for example, are equipped with options to send the same message to multiple recipients. These recipients can in turn forward the same message to others, and so on. Such forwarding differs from an extended game of telephone, however, because the messages are instantly duplicated and stored in each recipient's computer as the messages are sent and resent.³⁶

A single corporation can generate and exchange millions of files in a day. At least 93 % of information created today is first generated in digital format, 70% of corporate records may be stored in electronic format,³⁷ and 30% of electronic information is never printed on paper.³⁸ As a result, what would have taken thousands of filing cabinets of documents to store are now easily stored in a single computer.³⁹

Many lawyers and litigants now perceive e-mails and other electronic documents as "treasure trove[s] – or potential land mines" of information.⁴⁰ For example, quite unlike printed letters, the recipients of a particular e-mail are always listed at its beginning.⁴¹ These documents are very difficult to erase, unlike a papers and faxes which can be destroyed for sure using a shredder. Electronic communications can be reconstructed from residual electronic fragments or retrieved from backup systems,⁴² or a duplicate copy from someone else's computer may surface at an inconvenient time.⁴³

³⁶ Redgrave, *supra* note 33, at 201.

³⁷ *Id.*

³⁸ Richard Marcus, *Confronting the Future: Coping with Discovery of Electronic Materials*, 64 SUM LAW & CONTEMP. PROBS. 253, 280-281 (2001).

³⁹ Redgrave, *supra* note 33, at 200.

⁴⁰ Rosenthal, *supra* note 7, at 32.

⁴¹ Heckman & Brydges, *supra* note 7, at 154 citing Karen Hagberg & Max Olson, *Shadow Data, E-Mail Play a Key Role in Discovery*, TRIAL, N.Y.L.J., S3, June 16, 1997.

⁴² A backup tape is a copy of an electronic storage device, regularly made in case of a system failure or other event such as a virus attack. It normally contains documents created by systems users, such as e-mail messages, word-processing documents, spreadsheets, database entries and the like, but often includes copies of the system files required to make the computer's operating systems function properly.

⁴³ Mark Robins, *Computers and the Discovery of Evidence – A New Dimension to Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 413 (1999); Rosenthal, *supra* note 7, at 33. "Unlike the visual impact of paper records, business people in an

As one writer phrased, "electronic data has a bad habit of hanging around, even after one thinks one has discarded it."⁴⁴ This is because the "delete" function of e-mail programs does not really erase the message; it merely marks the computer space used as reusable. Thus, the message remains stored until overwritten by new data, or cleared using special software.⁴⁵

Some "residual data" can be recovered even if these were deleted so long ago that neither the user nor the computer itself is aware of their existence.⁴⁶ The quest for such has become so popular that several American companies have entered the "computer forensics" business, which involves high-technology archaeological expeditions into "the recovering of deleted files for companies undergoing litigation, regulatory review or attempting to document workplace misconduct."⁴⁷ Such electronic relics are now an important concern in litigation:

[M]any clients involved in litigation face difficult decisions when the business managers find a new web-based platform to share and build ideas. Rather than immediately benefit from the new efficiencies promised by the technology, companies must halt and consider how the systems work and whether the billions of streaming bits of data must be captured for all posterity even though the very concept was to create an "idea flow" that purposely discarded ideas that are deemed unworthy to pursue.⁴⁸

However, naturally, not all documents are deleted or disposed of. Today, electronic backup copies and archives can be retained cheaply and with little storage space, especially compared to printouts – as all lawyers now know, the entire Supreme Court Reports Annotated fits in just two compact discs that can be packed with a laptop computer for portable use. The use of backup files makes deletion even more difficult than it already is, however, and exponentially increases the amount of discoverable infor-

organization do not see electronic data 'piling up.' As noted above, it is much more likely to remain, often in numerous places, than paper documents." Redgrave & Hiser, *supra* note 28, at 206.

⁴⁴ Rosenthal, *supra* note 7, at 33.

⁴⁵ Sherry Talton, *Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure Of Confidential Information*, 20 REV. LITIG. 271, 281 (2000).

⁴⁶ Shira Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 337 (2000).

⁴⁷ Rosenthal, *supra* note 7, at 35.

⁴⁸ Redgrave & Hiser, *supra* note 28, at 206.

mation for litigation.⁴⁹ Such information might contain "potentially damaging documents thought to have been destroyed years ago."⁵⁰

Thus, as dependence on computers increases, discovery battles – at least in the United States – are now "being waged on a more esoteric level."⁵¹ Kenneth Starr, of Monica Lewinsky case fame, can readily attest to the potency of the newest weapon in the legal market:⁵²

One of the turning points of Kenneth Starr's case was his discovery of a "talking points" memo on a computer file that Monica Lewinsky thought she had deleted.⁵³

So might Nancy Temple of Arthur Andersen:

"I suggested deleting some language that might suggest we have concluded the release is misleading," is the content of the e-mail sent by Nancy Temple that became central to the jury's verdict of convicting the accounting firm. Andersen's inconsistently applied policy in the retention of documents, and its failure to suspend it when required, was a major factor in the firm's obstruction of justice conviction and ultimate demise.⁵⁴

Most recently, e-mails from around the world supported an American conviction of four co-defendants charged with materially supporting the Al-Qaeda terrorist group.⁵⁵

E-mail messages are especially useful to lawyers building cases because their cheap, quick nature makes their use casual. More often than

⁴⁹ Joshua Masur, *Safety in Numbers: Revisiting The Risks to Client Confidences And Attorney-Client Privilege Posed By Internet Electronic Mail*, 14 BERKELEY TECH. L.J. 1117, 1132 (2003).

⁵⁰ Betty Ann Olmstead, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523, 523 (1996).

⁵¹ Heckman & Brydges, *supra* note 7. Electronic evidence is any electronically-stored information (which includes all information stored digitally, optically, or in analog form) subject to pretrial discovery.

⁵² Martin Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 564 (2001).

⁵³ Schira Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 up to the Task?*, 41 B.C. L. REV. 327, 331 (2000).

⁵⁴ Rosenthal, *supra* note 7, at 34. See John Fatino, *Public Employers and E-mail: A Primer for the Practitioner and the Public Professional*, 23 N. Ill. U. L. Rev. 131, 133 (2003); William Porter & Michael Giffaton, *Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace*, 70 DEF. COUNS. J. 65, 75 (2003).

⁵⁵ *United States v. Khan*, 2004 WL 406338 (E.D.Va. 2004).

not, messages are "spontaneous, open, candid and sometimes even salacious,"⁵⁶ and many an employee has e-mailed an informal note, "frequently using casual, off-the-cuff language,"⁵⁷ to a boss that he would never have written on a piece of paper.⁵⁸ E-mail has "evolved into a hybrid of oral and written communications."⁵⁹ One writer stated that it is "like a phone call, only written. It's like a paperless letter, but faster. It's like a casual conversation, or a postcard, or a scribbled note to a classmate in the middle of class. It's all of the above, and... none of them."⁶⁰

Put more bluntly: "It's as if people put their brains on hold when they write e-mail. It's a substitute for a phone call, and that's the danger."⁶¹ Such informality creates the illusion that nothing is being recorded as in a telephone conversation, which is far from the truth. This tendency increases the risk of "creating a record of decontextualized statements."⁶² Thus, electronic messages have become the "digital smoking gun" in more and more lawsuits.⁶³

II. THE ATTORNEY-CLIENT PRIVILEGE

A. HISTORY OF THE ATTORNEY-CLIENT PRIVILEGE

The attorney-client privilege is considered the oldest privilege in the law.⁶⁴ The lawyer's loyalty to his client prohibits him from testifying in the client's case, a concept traceable to Roman times.⁶⁵ In the Elizabethan era,

⁵⁶ Michael Marron, *Discoverability of "Deleted" E-mail: Time for a Closer Examination*, 25 SEATTLE U.L. REV. 895, 906 (2003). See Robins, *Evidence at the Electronic Frontier*, *supra* note 19, at 223.

⁵⁷ Devin Murphy, *The Discovery Of Electronic Data in Litigation: What Practitioners And Their Clients Need to Know*, 27 WM. MITCHELL L. REV. 1825, 1827 (2001).

⁵⁸ Marron, *supra* note 56, at 906.

⁵⁹ *Id.* at 907.

⁶⁰ *Id.* at 906.

⁶¹ *Id.* at 898.

⁶² James Lehman, *Litigating in Cyberspace: Discovery of Electronic Information*, 14 S.C. LAW. 15, 17 (1997).

⁶³ *Id.*

⁶⁴ *Swidler & Berlin v. United States*, 524 U.S. 399, 400 (1998); *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981); *Hunt v. Blackburn*, 128 U.S. 464 (1888); *Hodges, Grant & Kaufmann v. United States*, 768 F.2d 719, 720-21 (5th Cir. 1985); *Sullivan v. Superior Court*, 29 Cal. App. 3d 64, 71 (1972).

⁶⁵ CHARLES MCCORMICK ON EVIDENCE, § 87 (John Strong ed., 1992).

the thrust of this confidential relationship was to protect the integrity of the lawyer, not primarily to insulate the client's cause. Exemptions from disclosure were seen until the 1700s, arising from the importance society attributed to the lawyer's "point of honor."⁶⁶

Despite the confidentiality principle's prominence, its authority saw erosion during the late 1700s. Society leaned towards a higher premium on judicial truth and justice;⁶⁷ the good of the public came to be more important than the preservation of a few individuals' honor.

The privilege, however, survived because of the need to remove the clients' inhibitions in consulting lawyers. The necessity to free clients from apprehension propelled the development of detailed rules to be applied in the courts. However, the resurrection was not easy. The new client-centered notion struggled, for some time, with the old concept of protecting the lawyer's honor.⁶⁸

Today, the attorney-client privilege is based on three propositions:

- (1) The lawyer's competence in settling legal disputes is needed in order for the client to adhere to our complex way of life;
- (2) The lawyer will not be able to respond to this need, without full knowledge of the facts which surround the client's case;
- (3) The client cannot be expected to reveal everything to the lawyer without the assurance that his confidences will be protected.⁶⁹

"It is the glory of the legal profession that its fidelity to its client can be depended on; that a man may safely go to a lawyer and converse with him upon his rights or supposed rights in any litigation with absolute assurance that the lawyer's tongue is tied from ever disclosing it."⁷⁰

⁶⁶ JOHN WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW, § 2290 (McNaughton rev. ed. 1961).

⁶⁷ *Id.* at 543.

⁶⁸ *Id.*

⁶⁹ McCormick, *supra* note 65, at 120-21.

⁷⁰ United States v. Costen, 38 Fed. 24 (1880).

There are, however, objections to these utilitarian justifications. Jeremy Bentham, one of the most famous critics of the doctrine, opined that the privilege is superfluous when applied to an innocent party — an innocent client need not hide anything from the public. The confidentiality privilege is guilty-oriented; it has the tendency to suppress the truth.⁷¹

In response, however, Dean John Wigmore wrote that first, “[t]here are no hard and fast lines between guilt and innocence;” therefore, stigmatizing the accused is not justified. Second, it is not possible that “all the acts and facts” of one party are unlawful in their entirety while the other party is completely righteous. It is possible that there is “a mixture of these qualities in infinitely varying proportions.” Third, even assuming that one party is indeed wholly wrong and the other wholly right, removing the privilege would only deter guilty parties from seeking legal advice, and would not lead to what Bentham referred to as “unmixed good.” Further, Bentham’s argument presupposed that all lawyers who encounter such guilty parties would yield to their whims.⁷²

B. THE ATTORNEY-CLIENT PRIVILEGE TODAY

The privilege is now embodied in Rule 130:

An attorney cannot, without the consent of his client, be examined as to any communication made by the client to him, or his advice given thereon in the course of, or with a view to, professional employment, nor can an attorney’s secretary, stenographer, or clerk be examined, without the consent of the client and his employer, concerning any fact the knowledge of which has been acquired in such capacity.⁷³

It has three elements:

1. There must be a relation of attorney and client;
2. The communication must have been made to the attorney in the course of or with a view to professional employment.

⁷¹ *Id.*

⁷² WIGMORE, *supra* note 66, at 23, §2291, at 552-553.

⁷³ RULES OF COURT, Rule 130, § 24(b).

3. The communication must be confidential.⁷⁴

To further stress the privilege's significance, the Revised Penal Code also penalizes lawyers who reveal clients' secrets obtained from their relationship.⁷⁵

1. Attorney-client relationship

For a professional relationship to arise, the meeting of the parties should be under circumstances that would lead a reasonable man to conclude that the potential client intended to obtain legal advice or representation. Thus, for example, the privilege cannot be claimed by a lawyer against a partner or other collaborating lawyer he worked with.⁷⁶ However, the privilege does apply to situations where no professional relationship ripened. For example, information obtained during a preliminary consultation is privileged even if the client chose not to employ the lawyer, or the latter declined to represent him.⁷⁷ Information exchanged after such a preliminary conference, however, is not covered.⁷⁸

Further, a relationship that revolved around nonlegal matters falls outside the privilege. In *Pfeider v. Palanca*,⁷⁹ the Court ruled that a lawyer may divulge a list of creditors given to him in order to pay them. The list was not

⁷⁴ RICARDO FRANCISCO, EVIDENCE 50-151 (1996). Wigmore further breaks this down into: "(1) where legal advice was sought; (2) from a professional legal advisor in his capacity as such; (3) the communications relating to that purpose; (4) made in confidence; (5) by the client; (6) are at his instance permanently protected; (7) from disclosure by himself or by the legal advisor, (8) except the protection be waived." *United States v. Evans*, 113 F.3d 1457, 1461 (7th Cir. 1997), citing 9 WIGMORE, *supra* note 66, § 2292. In re Grand Jury Subpoena Duces Tecum, 731 F.2d 1032, 1036 (2nd Cir. 1984).

⁷⁵ REV. PEN. CODE, Art. 209. "Betrayal of trust by an attorney or solicitor.—Revelation of secrets.— In addition to the proper administrative action, the penalty of *prision correccional* in its minimum period, or a fine ranging from 200 to 1,000 pesos, or both, shall be imposed upon any attorney-at-law or solicitor (*procurador judicial*) who, by any malicious breach of professional duty or inexcusable negligence or ignorance, shall prejudice his client, or reveal any of the secrets of the latter learned by him in his professional capacity.

"The same penalty shall be imposed upon an attorney-at-law or solicitor (*procurador judicial*) who, having undertaken the defense of a client or having received confidential information from said client in a case, shall undertake the defense of the opposing party in the same case, without the consent of his first client."

⁷⁶ *People v. Superior Court*, 83 Cal. App. 4th 387, 405 (2000).

⁷⁷ JONES ON EVIDENCE 774 (6th ed.).

⁷⁸ FRANCISCO, *supra* note 74, at 150 citing 58 AM. JUR. 267.

⁷⁹ *Pfeider v. Palanca*, 35 SCRA 75 (1970).

given because of their existing professional relationship, but on account of paying the debt. Similarly, a client who sought accounting and not legal services may not claim the privilege.⁸⁰

As a rule, the lawyer's duty to maintain his client's confidence is perpetual and outlasts his professional employment. In other words, even the severance of the relationship cannot break the seal of privilege; it may only be removed by the client himself or, after his death, by his heir or legal representative. The lawyer is thus forever prohibited from doing anything possibly injurious to his client and from disclosing any information acquired due to the professional relationship.⁸¹

The privilege is accorded such strength that it is deemed to reach out from beyond the grave. In *Swidler & Berlin v. United States*, Deputy White House Counsel Vincent Foster asked a lawyer to represent him in a White House investigation, nine days before the former committed suicide. In upholding the lawyer's nondisclosure of his handwritten notes made during consultations with Foster, the Court rejected the appellate court's balancing test and ruled that the office investigating Foster had failed to show that "reason and experience" warranted an exception to the privilege, even for a deceased client.⁸²

Further, a lawyer may even decline to divulge even the name of his principal, if it would expose him to litigation. This was upheld in *Regala v. Sandiganbayan*, as contended by members of the Cruz, Concepcion, Regala & Abello (ACCRA) law firm. The Court opined that if the accused were given a choice between legal representation without effective communication or legal representation with the threat of having his confidences revealed, he might opt for the former. This would lead to a vicious dilution of his right to be presumed innocent. It stated that the privilege "gives flesh to one of the most sacrosanct rights available to the accused, the right to counsel," and that full disclosure "opens the door to a whole spectrum of legal options."⁸³

⁸⁰ *Couch v. United States*, 409 U.S. 322, 335 (1973); *Olender v. United States*, 210 F. 2d 795, 805-06 (9th Cir. 1954).

⁸¹ RUBEN AGPALO, *THE CODE OF PROFESSIONAL RESPONSIBILITY FOR LAWYERS* 275-76 (1991).

⁸² *Swidler & Berlin v. United States*, 524 U.S. 399 (1998).

⁸³ *Regala v. Sandiganbayan*, G.R. No. 105938, 262 SCRA 122, 150, Sept. 20, 1996.

2. Communication by the client to the attorney

First of all, the person consulted for legal advice must be a lawyer, or the privilege may not be invoked. However, information disclosed to someone who fraudulently pretend to be a lawyer remains privileged.⁸⁴ The scope of the privilege extends to non-lawyers acting as the lawyer's agents, such as secretaries, stenographers, messengers, and assistants employed to build the client's case. Documents obtained by the lawyer such as reports made by a doctor, engineer or accountant and secured as part of attorney-client communication are likewise protected.⁸⁵ Dean Wigmore recognized the lawyer's indispensable need to employ other persons when handling a client's affairs, especially given the complexity of modern transactions,⁸⁶ excluding these agents collapses the privilege's barrier. Such extension to non-lawyers, however, must be "strictly confined within the narrowest possible limits consistent with the logic of its principle," and strictly for purposes related to securing legal advice.⁸⁷

In modern litigation, taking the other end of the relationship, the scope of the privilege is likewise stretched to the client's employees and agents. This was upheld in *Upjohn Co. v. United States*, where the American Court upheld a lawyer's nondisclosure of questionnaires filled up and submitted to him by the client's managers. Otherwise, the lawyer would be severely hampered in gathering information from lower-level employees who could aid him in preparing for litigation. Alternately, the same lawyer would be hampered in advising the same employees on corporate officers' orders, and these lower-level managers could embroil the corporation in litigation.⁸⁸

Finally, the privilege protects primarily the communication's content, and generally not the peripheral facts surrounding it such as the actual fact of consultation, its nature, and the general details of the billing

⁸⁴ FRANCISCO, *supra* note 74, at 150, *citing* *People v. Barker*, 27 N.W. 539, 546.

⁸⁵ RUBEN AGPALO, HANDBOOK ON EVIDENCE 131.

⁸⁶ WIGMORE, *supra* note 66, §2301, at 583.

⁸⁷ *Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1514 (D.C.Cir. 1993), *quoted in* *Blumenthal v. Drudge*, 186 F.R.D. 236, 243 (D.D.C. 1999).

⁸⁸ *Upjohn Co. v. United States*, 449 U.S. 383, 392 (1981).

arrangement.⁸⁹ *Regala* is an exception, where such peripheral facts would themselves have exposed the client to litigation.

3. Confidentiality of the communication

Confidentiality is the third and most important requisite.⁹⁰ This pertains to information disclosed during the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing or detrimental to him.⁹¹ Thus, a lawyer cannot be forced to disclose that he was paid with silver coins when his client is precisely charged with theft of such coins.⁹² The communication itself must satisfy three further criteria:

- (1) the client intended it to be confidential;
- (2) the client's expectation of confidentiality was reasonable under the circumstances of its utterance;
- (3) the confidentiality was subsequently maintained.⁹³

Regala held:

All communications made by a client to his counsel for the purpose of professional advice or assistance, are privileged, whether they relate to a suit pending or contemplated, or to any other matter proper for such advice or aid.... And whenever the communication made, relates to a matter so connected with the employment as attorney or counsel as to afford presumption that it was the ground of the address by the client, then it is privileged from disclosure.⁹⁴

Despite this broad statement, there are many exceptions to confidentiality. Information disclosed by a client to his lawyer for the purpose of passing such to a third party is not privileged after it has been so communicated. *Uy Chiao v. Union Life Insurance Society* held that policies written on a document turned over to the insurance company by the lawyer

⁸⁹ *Humphreys v. Donovan*, 755 F.2d 1211, 1219 (6th Cir. 1985); *Valenti v. Allstate Insurance Co.*, 243 F.Supp.2d 200, 218 (M.D.Penn. 2003); *Stabilus v. Haynsworth, Baldwin, Johnson and Greaves, P.A.*, 144 F.R.D. 258, 268 (E.D.Pa. 1992).

⁹⁰ *In re Grand Jury Proceedings*, 727 F. 2d 1352, 1355-56 (4th Cir. 1984).

⁹¹ AGPALO, CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 81, at 274-77

⁹² FRANCISCO, *supra* note 74, at 151.

⁹³ William Matthews, *Comment, Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 KAN. L. REV. 283 (1996).

⁹⁴ *Regala v. Sandiganbayan*, G.R. No. 105938, 262 SCRA 122, 150, Sep. 20, 1996.

on the client's instructions were not privileged. Such disclosure to a third party is "essentially inconsistent with the confidential relation." Further, the lawyer served as a mere intermediary and not as a professional advisor.⁹⁵

Similarly, the privilege cannot be claimed against a letter from a client to his lawyer if a copy enters the opponent's hands. *Barton v. Leyte Asphalt* ruled that if such a letter is deemed authentic, the courts will not scrutinize how it was obtained.⁹⁶ As Dean Wigmore wrote:

Since the means of preserving secrecy of communication are entirely in the client's hands, and since the privilege is a derogation from the general testimonial duty and should be strictly construed, it would be improper to extend its prohibition to third persons who obtain knowledge of the communications.⁹⁷

This exception, however, is not applied to persons who surreptitiously read or obtain documents. The rule is also reconciled with the Constitution's total exclusionary rule which invalidates illegally obtained evidence. The presence of third parties or strangers during an attorney-client meeting negates the communication's confidentiality, however, since the reasonable expectation of confidentiality ceases to exist.⁹⁸

Finally, the privilege prescribes no mode of communication, and covers written and oral exchanges alike. All forms of communication fall under it so long as these were intended to be part of or significant to the legal advice sought.⁹⁹ The gauging of confidentiality with respect to technologically enhanced communication will be further discussed in the next section of this paper.

4. The crime-fraud and waiver exceptions

The privilege is not absolute, however, and may not be claimed in some cases if all of the above requisites are met. First, communications in furtherance of future illegal conduct fall under the "crime-fraud" exception. The protection is intended to support the proper functioning of the adversarial justice system,¹⁰⁰ but ceases when the desired advice refers not to

⁹⁵ *Uy Chico v. Union Life Insurance Society*, G.R. No. 9231, 29 Phil. 163, Jan. 6, 1915.

⁹⁶ *Barton v. Leyte Asphalt & Mineral Oil Co.*, G.R. No. 21237, 46 Phil. 938, Mar. 22, 1924.

⁹⁷ WIGMORE, *supra* note 66, §2301, at 584.

⁹⁸ *United States v. Evans*, 113 F. 3d 1457 (7th Cir. 1997).

⁹⁹ AGPALO, CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 81, at 132.

¹⁰⁰ *United States v. Zolin*, 491 U.S. 554 (1989).

prior wrongdoing, but to future crimes.¹⁰¹ Wigmore explains that this is not really an exception, but "delineates the outer contours" of the privilege.¹⁰² Factual basis of such crime or fraud must of course be shown before the privilege is set aside.¹⁰³

Second, the privilege may be waived if by the client voluntarily discloses the confidential information. The client possesses the privilege, and has the power to waive it.¹⁰⁴ The waiver may be explicit or implicit; the latter is achieved by committing acts that are inconsistent with the reasonable maintenance of confidentiality.¹⁰⁵ These include:

1. A client's failure to object to an attorney's testimony or other disclosure;
2. A client's giving evidence on the privileged communication;
3. A client calling or cross-examining his attorney regarding privileged communication¹⁰⁶

Thus, when the client declares in court that he indeed signed notes to be delivered to his lawyer, the lawyer is bound to confirm the existence of such notes. The privilege cannot be claimed where the client himself already revealed the confidential information;¹⁰⁷ the former cannot thereafter insist that the mouth of the attorney be shut.¹⁰⁸ If the client presents part of a document as evidence, he waives privilege with respect to the remainder.¹⁰⁹ In *Orient Insurance Co. v. Revilla and Teal Motor*, the Supreme Court ruled that

¹⁰¹ WIGMORE, *supra* note 66, §2298, at 573.

¹⁰² 8 WIGMORE, *supra* note 66, § 2298, at 572, *quoted in* Rambus, Inc. v. Infineon Technologies AG, 2004 WL 383590, at *17 (E.D.Va. 2004).

¹⁰³ United States v. Zolin, 491 U.S. 554, 572 (1989); United States v. Jacobs, 117 F.3d 82, 87 (2nd Cir. 1997); In re: John Doe, Inc., 13 F.3d 633, 637 (2nd Cir. 1994); In re: Grand Jury Subpoena Duces Tecum, 731 F.2d 1032, 1039 (2nd Cir. 1984).

¹⁰⁴ MCCORMICK, *supra* note 65, §93, 130.

¹⁰⁵ In re Kidder Peabody Sec. Litig., 168 F.R.D. 459, 469 (S.D.N.Y. 1996).

¹⁰⁶ FRANCISCO, *supra* note 74, at 158; McCormick, *supra* note 65, §93, at 131.

¹⁰⁷ Jones v. Harding, No. 4338, 9 Phil. 279, Dec. 2, 1907.

¹⁰⁸ Hunt v. Blackburn, 128 U.S. 464, 470-71 (1888).

¹⁰⁹ Nguyen v. Excel Corp., 197 F.3d 200, 207 (5th Cir. 1999); McCormick, *supra* note 65, at 131, § 93; 8 WIGMORE, *supra* note 66, §2327, *cited in* Naquin v. Unocal Corp., 2002 WL 1837838, at *3 (E.D.La. 2002).

introduction of a document by one party entitles his adversary to use the same document against him.¹¹⁰

Finally, the client should act in way that would lead others to conclude that he intends to maintain confidentiality. In *In re von Bulow*, the Second Circuit held that a client waived any privilege by encouraging his lawyer to publish a book about his case.¹¹¹ Of course, when the client accuses the lawyer of misconduct, the latter is released from the privilege and allowed to disclose the truth in order to defend his own interests.¹¹²

III. APPLICATION OF THE ATTORNEY-CLIENT PRIVILEGE TO ELECTRONIC DOCUMENTS

A. EXPANDING THE APPLICATION OF THE PRIVILEGE

Except for the fact that there are more documents and they are in a more easily manipulated and duplicated electronic form, the framework of electronic discovery is not so different from that of its conventional predecessor. This section shall discuss how the requisites for the attorney-client privilege should be interpreted broadly, given numerous e-mails at its fringes such as those involving the agents of either attorney or client, those not directly discussing legal advice, and those that would appear to waive confidentiality under a very strict view such as an e-mail discussing legal advice with a client's spouse.

One returns to the landmark case *Hickman v. Taylor*, which called discovery rules "one of the most significant innovations of the Federal Rules of Civil Procedure."¹¹³ *Hickman* outlined that limitations arise when it can be shown that discovery:

1. "is being used in bad faith or in such a manner as to annoy, embarrass or oppress the person subject to the inquiry"
2. "touches upon the irrelevant"

¹¹⁰ *Orient Insurance Co. v. Revilla and Teal Motor Co.*, No. 34098, 54 Phil. 919, Sept. 17, 1936.

¹¹¹ *In re von Bulow*, 828 F. 2d 94 (2nd Circ. 1987).

¹¹² AGPALO, CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 81, at 285.

¹¹³ *Hickman v. Taylor*, 329 U.S. 495, 500 (1947).

3. "encroaches upon the recognized domains of privilege"¹¹⁴

The components of this framework are explicit in the Philippine Rules of Court, and this portion of *Hickman* was adopted by Justice Andres Narvasa in *Republic v. Sandiganbayan*.¹¹⁵ The first and second depend largely on the discretion of the judge, and are more difficult to employ given Philippine pronouncements on treating discovery rules with liberality. The easiest evasive maneuver is thus to claim privilege, as this has far better established benchmarks in doctrine. Attorney-client privilege finds the broadest application, since every client will have a lawyer, but not every case will involve a spouse, priest, or physician. Indeed, this and work product privilege are the most widely invoked against electronic discovery.¹¹⁶

Although one establishes the requisites for this privilege normally, as one would for a letter, one argues that the privilege must be expanded to match the similarly expanded use of discovery, because there are now more documents to find. One infers that there are more documents because more communication is being electronically recorded in writing, whether or not more communication is actually being made. Examining the permutations of communication, one recalls that personal communication between the lawyer and the client is not the only kind protected. The lawyer, for example, may use employees, agents, and consultants to aid him. On the other side of the relationship, as seen in *Upjohn*, the client's own employees and agents are also protected.

Recalling that the privilege is "a highly fact-specific one,"¹¹⁷ the new electronic context must be appreciated. For example, the privilege should be applied to discussions of legal advice by co-clients or a corporate client's agents. In *Long v. Anderson University*, when a university was sued by a student, the district court applied the privilege to an e-mail from its director of human resources to its dean of students that discussed legal advice given by their lawyer. The court stated:

¹¹⁴ *Id.* at 507-08. "[L]imitations inevitably arise when it can be shown that the examination is being conducted in bad faith or in such a manner as to annoy, embarrass or oppress the person subject to the inquiry... [F]urther limitations come into existence when the inquiry touches upon the irrelevant or encroaches upon the recognized domains of privilege."

¹¹⁵ *Republic v. Sandiganbayan*, G.R. No. 90478, 206 SCRA 212, Nov. 21, 1991.

¹¹⁶ *Van Buskirk*, *supra* note 19, at 51.

¹¹⁷ *Long v. Anderson University*, 204 F.R.D. 129, 134 (S.D.Ind. 2001).

Management should be able to discuss amongst themselves the legal advice given to them as agents of the corporation with an expectation of privilege.¹¹⁸

The 2003 case *AT&T v. Microsoft* ruled that e-mail between employees discussing an issue in preparation for seeking legal advice on the matter was privileged. The court emphasized an understanding of the subject's legal implications from the start and a showing of confidentiality.¹¹⁹ *In Re Santa Fe International* similarly recognized that e-mail between employees talking about a memo received from the general counsel was privileged.¹²⁰

In *IBM v. Comdisco*,¹²¹ an e-mail from a manager to an account representative discussing legal advice was held privileged, except to the extent that it discussed matters clearly meant to be communicated outside the company. One author commented:

As lawyers serving as corporate counsel likely know, an all-too-common result of e-mail communication is the ease with which sometimes sensitive or privileged messages are forwarded to numerous individuals. Such was the case in *Comdisco*. However, the court concluded that the privilege was not destroyed where those copied had "a need to know the information in the memo to perform their duties."¹²²

However, the 2003 case *United States v. Stewart*¹²³ held that a defendant waived the privilege when she forwarded an e-mail from her lawyer to her daughter.¹²⁴ Considering the ease of duplication and forwarding of e-mails, such a ruling regarding a close family member might be more closely scrutinized. The e-mail, however, was deemed protected by

¹¹⁸ *Id.*

¹¹⁹ *AT&T Corp. v. Microsoft Corp.*, 2003 WL 21212614, at *4 (N.D.Cal. 2003), *citing* *Upjohn v. United States*, 449 U.S. 383, 396 (1981).

¹²⁰ *In re: Santa Fe International Corp.*, 272 F.3d 705, 708 (5th Cir. 2001).

¹²¹ *IBM Corp. v. Comdisco*, No. 91-C-07-199, 1992 LEXIS 67 (Del. Super. Ct. March 11, 1992).

¹²² *Carpenter & Patterson*, *supra* note 19, at 66.

¹²³ 294 F.Supp.2d 490 (S.D.N.Y. 2003)

¹²⁴ *Id.* at 493; *United States v. Stewart*, 287 F.Supp.2d 464 (S.D.N.Y. 2003).

"Defendant's arguments regarding Stewart's intent and the sanctity of the family notwithstanding, the law in this Circuit is clear: apart from a few recognized exceptions, disclosure to third parties of attorney-client privileged materials results in a waiver of that privilege. No exception is applicable in this case."

the work product privilege.¹²⁵ *Wesley College v. Pitts* ruled similarly on an e-mail forwarded to several Wesley employees and its president's wife, although the court also noted that Wesley had already produced the same e-mail as evidence for another case and shown it to the one of Pitts' co-defendants there.¹²⁶ As a counterexample, *In Re Grand Jury Subpoenas*,¹²⁷ another 2003 case, extended the privilege to e-mails regarding legal strategies made directly between a defendant and a public relations firm hired by his lawyers. Some of the communications reviewed even involved the litigant's wife.¹²⁸

The 2003 case *Kintaro, Inc. v. Convio, Inc.*¹²⁹ is an electronic version of *Upjohn*. Here, an in-house counsel anticipated litigation and talked to a company vice-president about it. The latter in turn talked to the Vice-President for Sales, who in turn asked selected members of his sales force to prepare reports for the lawyer's use, and this was done via e-mail.¹³⁰ Elaborating on *Upjohn*, the decision upheld privilege using a five-point test:

- (1) the communication should have been made for the purpose of securing legal advice;
- (2) the employee making the communication should have done so at the direction of his corporate superior;
- (3) the superior made the request so that the corporation could secure legal advice;
- (4) the subject matter of the communication should have been within the scope of the employee's duties; and
- (5) the communication should not have been disseminated beyond those persons who need to know the information.¹³¹

¹²⁵ *United States v. Stewart*, 287 F.Supp.2d 461 (S.D.N.Y. 2003).

¹²⁶ *Wesley College v. Pitts*, 1997 WL 557554, at *2 (D.Del. 1997).

¹²⁷ *In re Grand Jury Subpoenas* dated March 24, 2003 Directed to (A) Grand Jury Witness Firm and (B) Grand Jury Witness, 265 F.Supp.2d 321 (S.D.N.Y. 2003).

¹²⁸ *Id.* at 324-27.

¹²⁹ 219 F.R.D. 503, 513-14 (S.D.Cal. 2003).

¹³⁰ *Id.*, citing *Upjohn Co. v. United States*, 449 U.S. 383, 390 (1981).

¹³¹ *Cuno, Inc. v. Pall Corp.*, 121 F.R.D. 198, 203 (E.D.N.Y. 1988).

Another 2003 case, *RLS Associates, LLC v. United Bank of Kuwait, PLC*¹³² made a similar ruling regarding e-mail from a lawyer to the client's agent.¹³³ Both cases explicitly cited *Upjohn*. In a related case, *Wyoming v. United States Department of Agriculture*¹³⁴ dealt with government records on compact disc or CD-ROMs. The decision noted that government agencies can assert the privilege, but records must have been kept confidential and circulated only among the necessary employees, such as those authorized to speak on the matters contained.¹³⁵

Further, courts should be more willing to retain the privilege in cases where attorney-client discussions were communicated to certain third parties. The American Fifth Circuit, for example, explicitly recognizes a "common legal interest" or "community of interest" extension of attorney-client privilege that applies to communications between actual or potential co-defendants and counsel.¹³⁶ This is not even new; its 1977 case *Wilson P. Abraham Construction Corp. v. Armco Steel Corp.*¹³⁷ explained that mutual confidences between co-defendants and their attorneys must be protected.¹³⁸ Its 1985 case *Hodges, Grant & Kaufmann v. United States*¹³⁹ extended the privilege to matters communicated to a third party that shared a legal interest in the subject discussed.¹⁴⁰ *In re Auclair*¹⁴¹ also extended the privilege to a group of potential co-defendants who consulted a lawyer together.¹⁴² The Fifth Circuit, it is noted, construes derivative protection of the privilege broadly.¹⁴³ A good example of this extension applies to lawyers retained by

¹³² 2003 WL 1563330 (S.D.N.Y. 2003).

¹³³ *Id.* at *4, *citing* *Upjohn*, 449 U.S. at 391.

¹³⁴ 239 F.Supp.2d 1219 (D.Wyoming 2002).

¹³⁵ *Id.* at 1230 (D.Wyoming 2002), *citing* *Lacefield v. United States*, 1993 WL 268392, at *3 (D.Colo. 1993).

¹³⁶ *In re: Santa Fe International Corp.*, 272 F.3d 705, 710 (5th Cir. 2001). *See* *Robinson v. Texas Automobile Dealers Association*, 214 F.R.D. 432, 443 (E.D. Tex. 2003); *Katz v. AT&T Corp.*, 191 F.R.D. 433, 436 (E.D.Pa. 2000); *In re LTV Securities Litigation*, 89 F.R.D. 595, 604 (N.D.Tex. 1981).

¹³⁷ 559 F.2d 250 (5th Cir. 1977).

¹³⁸ *Id.* at 253. The extension of the privilege was patterned after coordinated defenses in criminal cases. *Chahoon v. Commonwealth*, 62 Va. 822 (1871).

¹³⁹ 768 F.2d 719 (5th Cir. 1985).

¹⁴⁰ *Id.* at 721.

¹⁴¹ 961 F.2d 65 (5th Cir. 1992).

¹⁴² *Id.* at 69. *See* *In re LTV*, 89 F.R.D. at 604.

¹⁴³ *Robinson*, 214 F.R.D. at 440. "Broad construction' applies only to the distinction between direct protection of attorney statements and derivative protection. As a general matter of construction, the attorney-client privilege is to be interpreted 'within the narrowest possible limits consistent with the logic of its principle.'" *Id.* at 440

insurers to defend claims of their insured; privilege would naturally extend to the insurers as well.¹⁴⁴

Thus, the 2004 decision *Ross v. Uki Ltd.* deemed the privilege unwaived when e-mails were made to other lawyers involved in the litigation, to client representatives, and to that latter's secretaries. A copy of one e-mail was even furnished to an Uki employee, but the privilege was not dissolved because he was necessary for opening a bank account related to a loan transaction discussed by the lawyer. Another e-mail was forwarded to the director of another company involved in a transaction, with the expectation that confidentiality would be maintained.¹⁴⁵ The 2003 case *Robinson v. Texas Automobile Dealers Association*¹⁴⁶ would have ruled similarly on e-mail from an interest group's chief counsel, except the relation of one recipient to the legal matter discussed was not established, nor was it shown that he was a client.¹⁴⁷

To present still another aspect, the attorney-client privilege is strictly for legal-related communication, and no protection is granted when a lawyer is dispensing accounting¹⁴⁸ or simple business advice.¹⁴⁹ However, in today's increasingly complex litigation, a lawyer may be tasked not just to answer simple legal questions but to help formulate an overall strategy for the client

n.2. *Robinson*, a 2003 case, contains a good discussion of recent attorney-client and work product precedents used in electronic discovery cases.

¹⁴⁴ *Bovis Lend Lease, LMB, Inc. v. Seasons Contracting Corp.*, 2002 WL 31729693, at *3 n.5 (S.D.N.Y. 2002). "Courts in this circuit have also applied the 'common interest rule' to allow an insurer aligned in interest with the insured to have access to privileged communications between the insured and its counsel, without breach of the privilege. The common interest rule, however, does not itself give rise to a separate privilege. 'Rather, it is a limited exception to the general rule that the attorney-client privilege is waived when a protected communication is disclosed to a third party outside the attorney-client relationship.'"

¹⁴⁵ *Ross v. Uki Ltd.*, 2004 WL 67221, at *4-6 (S.D.N.Y. 2004).

¹⁴⁶ *Robinson*, 214 F.R.D. 432.

¹⁴⁷ *Id.* at 447.

¹⁴⁸ *Couch v. United States*, 409 U.S. 322, 335 (1973); *Olender v. United States*, 210 F.2d 795, 805-06 (9th Cir. 1954).

¹⁴⁹ *Rossi v. Blue Cross and Blue Shield of Greater New York*, 73 N.Y.2d 588, 592-93 (1989).

that may touch on accounting, taxation, or commercial matters.¹⁵⁰ Note it has been held:

The attorney-client privilege has also been extended to protect items such as research, notes, files and memoranda that are not themselves confidential communications, if disclosure would reveal the substance of any confidential communications between attorney and client that were made in the course of seeking or giving legal advice.¹⁵¹

Given the casual, free-flowing, and off-the-cuff nature of instant e-mail communications, one should argue for privilege if a message is somehow related to legal advice or a legal strategy, just not directly. Thus, the recent *Ross*, which involved numerous e-mails, held that documents discussing business aspects of various transactions remained privileged, since such discussion was clearly needed to lay the foundation for legal advice.¹⁵² The 2003 decision *TVT Records, Inc. v. The Island Def Jam Music Group*¹⁵³ considered an e-mail from a lawyer privileged even if it discussed business concerns because it had a legal character when read in context.¹⁵⁴ The relation must be clear even if not apparent from the document itself; in *United States v. ChevronTexaco, Corp.*,¹⁵⁵ the court noted that business-related e-mails could not be privileged simply because an attorney was a recipient.¹⁵⁶ Finally, the 2002 case *eSpeed, Inc. v. Chicago Board of Trade*¹⁵⁷ found that three e-mails between a lawyer and a company then involved in certain negotiations were not privileged because they outlined business negotiation points and the attached draft document was meant to be disclosed to the other party. The court, however, allowed one particular sentence in one e-mail to be redacted due to privilege.¹⁵⁸ In light of *TVT Records* and the nature of e-mail, one would caution that in other factual milieus, points of

¹⁵⁰ *Id.* at 594; *Stratagem Development Corp. v. Heron International N.V.*, 153 F.R.D. 535, 543 (S.D.N.Y. 1994). "But legal and business issues are often inextricably intertwined." *Robinson*, 214 F.R.D. at 446.

¹⁵¹ *Robinson*, 214 F.R.D. at 440, *citing* *Upjohn Co. v. United States*, 449 U.S. 383, 401 (1981).

¹⁵² *Ross*, 2004 WL 67221, at *3.

¹⁵³ 2003 WL 749801 (S.D.N.Y. 2003).

¹⁵⁴ *Id.* at *3. Relation to legal strategy must be clear, however, and a related decision rejected privilege for some e-mails that discussed purely business concerns. *TVT Records, Inc. v. The Island Def Jam Music Group*, 214 F.R.D. 143 (S.D.N.Y. 2003).

¹⁵⁵ 241 F.Supp.2d 1065 (N.D.Cal. 2002).

¹⁵⁶ *Id.* at 1075.

¹⁵⁷ 2002 WL 827099 (S.D.N.Y. 2002).

¹⁵⁸ *Id.* at *2-3.

confidential material might be inferred by an opponent from such an approach, especially if larger numbers of messages are involved.

The recent *In Re Grand Jury Subpoenas* explained why e-mails with a public relations firm retained in connection with litigation were likewise privileged:

[I]t is common ground that the privilege extends to communications involving consultants used by lawyers to assist in performing tasks that go beyond advising a client as to the law. For example, a client's confidential communications to a non-testifying expert retained by the lawyer to assist the lawyer in preparing the client's case... probably are privileged... [C]onsultants engaged by lawyers to advise them on matters such as whether the state of public opinion in a community makes a change of venue desirable, whether jurors from particular backgrounds are likely to be disposed favorably to the client, how a client should behave while testifying in order to impress jurors favorably and other matters routinely the stuff of jury and personal communication consultants come within the attorney-client privilege.¹⁵⁹

Robinson would have found e-mails regarding analysis of legislation and lobbying privileged, except confidentiality was not maintained.¹⁶⁰ Another 2003 case, however, rejected privilege for communications with a company employee who was a lawyer, because these were clearly not made in connection with legal advice. The American court noted that the lawyer in question was not licensed to practice in the United States.¹⁶¹

To note a final recent case, waiver of a certain subject or production of non-electronic materials may subject a client to more electronic discovery than expected, again because the use of e-mail means so much more communication is reduced to writing. In *Naquin v. Unocal Corp.*,¹⁶² the court found that the attachment of a privileged e-mail, inadvertently or not, to a position paper submitted to the Equal Employment Opportunity

¹⁵⁹ *In re Grand Jury Subpoenas* dated March 24, 2003 Directed to (A) Grand Jury Witness Firm and (B) Grand Jury Witness, 265 F.Supp.2d 321, 326 (S.D.N.Y. 2003).

¹⁶⁰ *Robinson v. Texas Automobile Dealers Association*, 214 F.R.D. 432, 446 (E.D. Tex. 2003), *citing* *Weissman v. Fruchtmann*, 1986 WL 15669, at *15 (S.D.N.Y. 1986).

¹⁶¹ *Gulf Islands Leasing, Inc. v. Bombardier Capital, Inc.*, 215 F.R.D. 466, 477 (S.D.N.Y. 2003).

¹⁶² 2002 WL 1837838 (E.D.La. 2002).

Commission waived privilege with respect to other e-mails related to the subjects that the attached e-mail discussed.¹⁶³

Again, although extending the privilege to the above communications is not new in itself, it is submitted that courts should exercise no hesitation in allowing the privilege amidst electronic discovery. Because the widespread use of e-mail makes these more accessible in written form to adverse parties, courts must ensure that the attorney-client privilege is not breached through a side entrance. Finally, the ease of duplicating e-mails and forwarding copies to parties other than lawyers or principal clients means that waiver should not be declared with undue haste against a party, especially when the supposed third party is clearly no stranger.

The goal to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice,"¹⁶⁴ in short, is realized when clients are allowed unfettered use of the full range of Internet communication.

B. THE CONFIDENTIALITY OF E-MAIL

The requisite of confidentiality in particular merits more discussion in an electronic context. As lawyers "embark on this 'information superhighway,'"¹⁶⁵ they must be aware of the possibility that e-mail, just like an ordinary letter or note, might be intercepted by a person who is not the intended recipient. Aside from simply making a wrong turn on the information superhighway and sending the e-mail to the wrong person, one is threatened by "hackers,"¹⁶⁶ both in the transmission of the message and its storage.

¹⁶³ *Id.* at *3-6.

¹⁶⁴ *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

¹⁶⁵ Amy Stevenson, *Making A Wrong Turn On The Information Superhighway: Electronic Mail, The Attorney-Client Privilege And Inadvertent Disclosure*, 26 CAP. U.L. REV. 347, 357 (1997).

¹⁶⁶ Among the computer savvy, the proper term for someone who breaks into other people's programs and computers with destructive or malicious intent is "cracker." Mary Micheletti, *Are You Protected?* at <http://www.jamespublishing.com/lawofficecomputing/Reviewsdata/on00/security.htm> (last visited Feb. 28, 2004). "A 1998 study by the Computer Security Institute found that 64 percent of companies polled reported information system security attacks, with the total financial losses from the 241 organizations that could put a dollar figure on

These individuals use software called "sniffers" to gain access to e-mail messages by searching for the sender's or recipient's address, then seize the message. The hacker can also configure his computer to resemble that of the intended recipient's, including its address. This is called "spoofing." A spoofer can intercept a message, concoct a false reply or doctor the original message, then send it to the original recipient.¹⁶⁷ In response to these, the United States passed laws which prohibited the use or disclosure of unlawfully intercepted communications.¹⁶⁸

Some writers argue that despite the danger posed by such online malcontents, computers handle thousand or even millions of messages in a day for thousands of different people.¹⁶⁹ Thus, "the odds of finding a needle in a haystack are greater than the odds that a computer hacker would successfully locate a particular message from a lawyer to a client."¹⁷⁰ Others opine that interception software, when placed in a strategic Internet location meaning on or near the respective networks of the lawyer and client, can capture individual messages, entire accounts, or both. This can be done without the knowledge of both the owner or the operator.¹⁷¹

Even discounting the dangers posed by hackers, lawyers should be wary of sending e-mails without the proper safeguards. The nature of transmission itself poses risks of intrusion. When a person sends an e-mail, it is first transmitted to the nearest routing computer or "station" between the sender and the recipient. The message travels from station to station until it reaches the recipient's computer, a process known as "store and forward."¹⁷²

This promotes efficiency in the communication, but reduces security.¹⁷³ Again, anyone with the skills who wants to search for e-mail

their lost information coming in at about \$138 million. And more recently, a July 2000 global survey of 4,900 IT professionals across 30 nations, conducted by InformationWeek Research, estimated that the cost to firms in the United States this year for viruses and computer hacking will amount to \$266 billion."

¹⁶⁷ Ben Delsa, *E-mail And The Attorney-Client Privilege: Simple E-mail in Confidence*, 59 LA. L. REV. 935, 948 (1999).

¹⁶⁸ Stevenson, *supra* note 165, at 354.

¹⁶⁹ Talton, *supra* note 45, at 282.

¹⁷⁰ Arthur Smith, *E-Mail and the Attorney-Client Privilege at* <http://www.abelaw.com/basl/lpm/email.htm> (last visited Feb. 28, 2004).

¹⁷¹ Masur, *supra* note 49, at 1155.

¹⁷² Thomas Watkins, *Ethics: Attorney Activity In The Internet*, 691 PLI/PAT 1331, 1345 citing William Matthews, *Encoded Confidences: Electronic Mail, the Internet and the Attorney-Client Privilege*, 45 KAN. L. REV. 273, 277-78 (1996).

¹⁷³ Talton, *supra* note 45, at 281.

between the sender and the recipient or on a particular subject matter, can search for, read, modify or delete a message before it even reaches the recipient.¹⁷⁴ "[U]nlike the postal mail, simple e-mail generally is not 'sealed' or secured, and can be accessed or viewed on intermediate computers between the sender and the recipient."¹⁷⁵ E-mail more closely resembles a postcard than to a sealed letter when it travels through electric networks. Others claim this is inaccurate; rather, e-mail resembles a "postcard that might be getting Xeroxed in every post office it might pass through."¹⁷⁶

Despite these problems, however, one argues that it is superficial to deem e-mail any less confidential than letters in the mail and phone conversations; older media are equally susceptible to interception. In American colonial times, Thomas Jefferson, Alexander Hamilton, and George Washington would sometimes write in code, since, as Ralph Waldo Emerson quipped, it was unlikely that "a bit of paper, containing our most secret thoughts, and protected only by a seal, should travel safely from one end of the world to the other, without anyone whose hands it had passed through having meddled with it." Benjamin Franklin had postal employees swear oaths not to pry into letters in the 1700s,¹⁷⁷ and three centuries later, the Philippine Constitution explicitly mandates the inviolability of the mails.¹⁷⁸

In the Information Age, writing letters in code is naturally more sophisticated, but the principle remains the same. Encryption methods were first developed during the World War II when the Germans and the Japanese developed a scheme of exchanging information through code machines, where messages could only be decoded using a device with identical settings. Fortunately for the Allies, these codes were deciphered by their "code breakers." After the War, computers made the use of complex encryption techniques practical enough for ordinary use.¹⁷⁹ Governments and private companies alike took advantage of this to protect confidential information.

Today, encryption is easily available for e-mail. A message or document to be transmitted online can be scrambled, and then unscrambled

¹⁷⁴ Watkins, *supra* note 172, at 1346.

¹⁷⁵ American Civil Liberties Union v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996).

¹⁷⁶ Talton, *supra* note 45, at 281.

¹⁷⁷ Daniel Solove, *The Origins and Growth of Information Privacy Law*, 748 PLI/PAT 29, 37 (2003).

¹⁷⁸ CONST. art. III, § 3(1).

¹⁷⁹ Brill, *supra* note 25, at 99.

only by the recipient with the right "key."¹⁸⁰ This revolutionary encryption system was developed in the 1970s, and uses very large prime numbers to create unique pairs of code keys. Each pair consists of a "public" and a "secret key." Parties can exchange public keys or even make these available through their websites. However, the messages made with this key can only be read using the secret key, which the owner sends to message recipients. This also assures the latter that the message truly came from the purported author.¹⁸¹

To blunt the possibility of leaks and to forestall any challenges to confidentiality in the context of privilege, lawyers must learn to use such technology,¹⁸² and it is not very difficult to do so. Nevertheless, the use of encryption technology does entail additional expenses, and demands that the client use it as well since protection on only one end of the communication is useless. Further, not all countries allow the use of encryption in e-mail, an issue in international correspondence.¹⁸³

Related to encryption is the digital signature, "a machine-generated series of bits which is encrypted with the document sender's private key. [It] appears as an undecipherable string of alphanumeric characters, and is unique for each document to which it is attached." Such an electronic precaution determines the authenticity of a message for its recipient. It can detect, for example, whether the message was altered by another person after the original sender applied his corresponding digital signature onto the document.¹⁸⁴

Finally, one notes that law firms face greater "insider threats" than interception of files by outside parties.¹⁸⁵ Thus, a lawyer must also establish that security precautions are taken internally. These may include measures as simple as screen passwords that prevent use of a computer while the lawyer goes on a coffee break or to the bathroom.

¹⁸⁰ *Id.* at 100; Watkins, *supra* note 172, at 1354.

¹⁸¹ Watkins, *supra* note 172, at 1354.

¹⁸² Stevenson, *supra* note 165, at 356.

¹⁸³ Delsa, *supra* note 167, at 956.

¹⁸⁴ Watkins, *supra* note 172, at 1355-56.

¹⁸⁵ Micheletti, *supra* note 166.

Proof of such measures is sufficient to thwart challenges to privilege on the basis of lack of confidentiality,¹⁸⁶ if made an issue, which appears unlikely in ordinary cases. One author noted:

Failure to use encryption to protect electronic mail communications may, in and of itself, indicate lack of intent or actual failure to maintain confidentiality. This is, however, a matter of unsettled law. No reported case addresses the effect of e-mail communication on the privilege. The closest that reported federal decisions have come to this issue is reviewing electronic mail sent over in-house or private networks, without considering issues unique to Internet-based communication. Some state ethics boards have found more limited protection for unencrypted electronic mail sent via the Internet. Iowa and South Carolina require express consent by the client to use of unencrypted e-mail, while Illinois treats electronic mail as an 'ordinary telephone call.' However, ethics panels in other states and the American Bar Association consider unencrypted electronic mail to be fully entitled to privileged treatment.¹⁸⁷

The presence of security measures, however, should be sufficient to establish an intent to maintain confidentiality and rebut allegations of its waiver.

C. DEALING WITH INADVERTENT DISCLOSURE

The sheer volume of electronic documents coupled with the ease of creating and transmitting copies has made the issue of inadvertent disclosure extremely important with respect to privilege.

Imagine this: A lawyer is bent over his computer, outlining a multimillion legal strategy using confidential information provided by his client. Instead of sending the memo to his partner, however, he mistakenly sends it to all the e-mail addresses stored in his computer, including the opposing counsel's. Since e-mail is near-instantaneous, aside from compromising the client's case, the lawyer seems to have irretrievably waived the attorney-client privilege – which, in the first place, is not his to waive.

The situation is not hypothetical, however:

¹⁸⁶ Discussions of cryptography may interest the mathematically-inclined. For example, legal articles on the subject discuss emerging techniques based on elliptical curves, and "quantum cryptography." Brill, *supra* note 25, at 102.

¹⁸⁷ Masur, *supra* note 49, at 1122-23.

[O]pposing counsel accidentally misdirected electronic communications and provided him with an unexpected edge. "I once got copies of e-mail from one partner to another in a disputed case, where they were discussing strategy and what they were going to tell me, versus what they could really do. It resulted in our getting a much better deal for our clients."¹⁸⁸

Aside from such extreme human errors, however, inadvertent disclosure of privileged material is inevitable. It is easily "accidentally produced when responding to a voluminous discovery request."¹⁸⁹ One only has to visualize the material potentially involved to understand why. An American Law Institute article depicted the scenario:

Large volumes of assorted, undifferentiated text files are difficult to screen for privilege. Computer search techniques may be used to roughly identify messages addressed to or authored by legal personnel, but the results of such searches will be far from precise. Manual review of the messages by people is time consuming and costly, as well as stupefyingly dull. While the seriousness of the consequences vary among the federal circuits, inadvertent production of privileged e-mail messages may result in the waiver of the privilege in part or in whole, against not only the immediate opponent but third parties as well.¹⁹⁰

The volume of discoverable electronic documents in a case defies imagination; the 2003 case *In re Worldcom, Inc. Securities Litigation*,¹⁹¹ for example, covered four *terabytes* worth of electronic documents, or 84 *million* pages worth, including 2.5 million pages of e-mail.¹⁹² Waiving sanctions for inadvertent disclosure would actually reduce the time and cost involved in electronic discovery.¹⁹³

¹⁸⁸ Micheletti, *supra* note 166. One famous horror story involves the pharmaceutical company Eli Lilly & Co. In June 2001, it accidentally released the e-mail addresses of 669 patients who had registered at their website to receive health related messages such as reminders to take medication. Michael Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 CHAP. L. REV. 39, 40 (2004).

¹⁸⁹ Delsa, *supra* note 167, at 953, citing Dorothea Beane, *Inadvertent Disclosure of Attorney-Client Privileged Material: Putting the Horse Back in the Barn*, 69 FLA. B.J. 67 (1995).

¹⁹⁰ Withers, *supra* note 9, at 748-49.

¹⁹¹ 2003 WL 22953645, (S.D.N.Y. 2003).

¹⁹² *Id.* at *3.

¹⁹³ Withers, *supra* note 9, at 749 & n.26. "Texas has a new rule that may serve as a model for such an agreement in other jurisdictions. Rule 193.3(d) of the Texas Rules of Civil Procedure, adopted in 1999, states, 'Privilege not waived by production. A party who produces material or information without intending to waive a claim of privilege

The time needed is considerable as well. In *Black v. United States*,¹⁹⁴ review of seized computers to help search for a fugitive was stalled because co-defendants might raise privilege. The defendants protested review by government lawyers not connected with the case, while the government protested the cost and time involved in hiring an independent outside party to perform the review. The court eventually ordered the defendant to produce printouts of the computer records for review by a judge, hardly a satisfactory compromise.¹⁹⁵ The 2003 case *Renda Marine, Inc. v. United States*¹⁹⁶ even featured a plaintiff who resisted not discovery itself, but the government's demand that it organize and label 38,000 pages of disclosed records.¹⁹⁷ These factual examples, incidentally, belie the impression that computers make discovery more convenient, cheaper and less cumbersome.¹⁹⁸ This is true on a per document basis, but the sheer number of documents often involved adds up to staggering totals.

The American Law Institute article recommended "creative negotiation" between parties, such as a prior agreement regarding such inadvertence endorsed as a court order.¹⁹⁹ Such agreements expediting discovery are already in use in the United States. The 2003 decision *United States v. Stewart*,²⁰⁰ for example, featured such an agreement in a securities fraud criminal case. Amidst disclosed materials, a government attorney

does not waive that claim under these rules or the Rules of Evidence if—within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made—the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.”

¹⁹⁴ 172 F.R.D. 511 (S.D. Fla. 1997).

¹⁹⁵ *Id.* at 515-16.

¹⁹⁶ 58 Fed.Cl. 57 (2003).

¹⁹⁷ *Id.* at 63.

¹⁹⁸ Watkins, *supra* note 172, at 197. “And when the discovery requests and orders come over the transom, the costs start to pile up quickly. Corporate information technology staffs are distracted from their core business assignments to assist lawyers and outside consultants to find data. Historic hard drives, floppy drives, tapes and other media are located and reviewed for electronic crumbs, incurring more costs in terms of business disruption and consultant's fees.” Redgrave & Hiser, *supra* note 28, at 206-207. “[T]he cost is not just the consultants' fee – it also includes the costs of lawyer review time, the production of non-relevant data, and the exposure of confidential and privileged materials to loss.” *Id.* at 209.

¹⁹⁹ Withers, *supra* note 9, at 749.

²⁰⁰ 294 F.Supp.2d 490 (S.D.N.Y. 2003).

found a copy of an e-mail from the defendant's lawyer that had been forwarded to the defendant's daughter. The attorney immediately stopped reviewing the materials and assured the court that she had not discussed the contents with colleagues. The e-mail was later held to be privileged as work product, though the lawyer was not disqualified by the case due to the less absolute nature of work product privilege.²⁰¹

Inadvertent disclosure remains problematic even in the United States given the relative youth of electronic discovery, and no single precedent resolves the issue. Existing precedents discuss ordinary mail; some of these retained the privilege if a lawyer took immediate steps to warn the opponent not to open the documents inadvertently sent to him, but such rules are suddenly obsolete in the face of e-mail's speed.

Courts use three different tests in ruling on waiver of privilege in case of inadvertent production.²⁰² These apply to work product as well as to the attorney-client privilege.

1. The strict test (waiver rule)

Some courts consider any disclosure an indication of "the lack of concern over confidentiality in the message,"²⁰³ since "[t]he amount of care taken to ensure confidentiality to the holder of the privilege reflects the importance of that confidentiality to the holder of the privilege."²⁰⁴ They hold that disclosure for any reason amounts to waiver,²⁰⁵ following Wigmore's view:

All *involuntary* disclosures, in particular, through the loss or theft of documents from the attorney's possession, are not protected by the privilege, on the principle... that, since the law has granted secrecy so far as its own process goes, it leaves to the client and attorney to take measures of caution sufficient to prevent being overheard by third

²⁰¹ *Id.* at 493-494.

²⁰² *Asian Vegetable Research and Development Center v. Institute of International Education*, 1995 WL 491491, at *6-7, (S.D.N.Y. 1995); *Meridian Mortgage Corp. v. Spivak*, 1992 WL 205640 (E.D.Pa. 1992); *Federal Deposit Insurance Co. v. Marine Midland Realty Credit Corp.*, 138 F.R.D. 479, 479-80 (D.C.Va. 1991). *Delsa*, *supra* note 167, at 953, *citing* *Beane*, *supra* note 189, at 68.

²⁰³ *Delsa*, *supra* note 167, at 954.

²⁰⁴ *In Re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989).

²⁰⁵ *In re Grand-Jury Proceedings*, 727 F.2d 1352, 1356 (4th Cir. 1984); *Wichita Land & Cattle Co. v. American Federal Bank*, F.S.B., 148 F.R.D. 456, 457 (D.D.C.1992); *State v. Vennard*, 159 Conn. 385, 270 A.2d 837, 849 (1970).

persons. The risk of insufficient precautions is upon the client. This principle applies equally to documents.²⁰⁶

In the 2002 case *Murphy Oil USA v. Fluor Daniel, Inc.*,²⁰⁷ the court compelled the defendant to produce relevant e-mail stored on backup tapes after Murphy argued that Fluor Daniel, Inc. had voluntarily produced one relating to the subject. The latter had already identified the disputed e-mail as privileged, but inadvertently produced it and the attached document. The court ruled that the inadvertent disclosure constituted waiver.²⁰⁸

In *Federal Deposit Insurance Corp. v. Singh*,²⁰⁹ the plaintiff's lawyer removed copies of a memo from a file made available to the defendant. The memo, however, was read by the defendant's lawyer while reviewing documents for discovery in the office of another lawyer for the plaintiff. The court held:

The purpose of the privilege is to protect the confidences of clients so they may freely discuss their legal concerns with counsel. However, when a document is disclosed, even inadvertently, it is no longer held in confidence despite the intentions of the party and thus, "the privilege is lost 'even if the disclosure is inadvertent.'"²¹⁰

In *In Re Sealed Case*,²¹¹ a defense contractor embroiled in a grand jury investigation for tax evasion resisted discovery of six documents. The government claimed that attorney-client privilege would be waived because they would eventually be disclosed for tax purposes, and the company learned that one had in fact been disclosed by its chief accounting officer to the Defense Contract Audit Agency during a routine audit of travel expenses.²¹² The court held:

Even assuming Company's disclosure was due to "bureaucratic error," which we take to be a euphemism that necessarily implies human error, that unfortunate lapse simply reveals that someone in the company and thereby Company itself (since it can only act through its employees) was careless with the confidentiality of its

²⁰⁶ *Berg Electronics, Inc. v. Molex, Inc.*, 875 F. Supp. 261, 262 (D.C. Del. 1995), quoting 8 WIGMORE, *supra* note 66, at 633, § 2325.

²⁰⁷ *Murphy Oil USA v. Fluor Daniel, Inc.*, No. 2:99-CV-03564 (E.D. La. Dec. 3, 2002).

²⁰⁸ Brill, *supra* note 25, at 167-68.

²⁰⁹ 140 F.R.D. 252 (D. Me. 1992).

²¹⁰ *Id.* at 253.

²¹¹ 877 F.2d 976 (D.C. Cir. 1989).

²¹² *Id.* at 977.

privileged communications... Short of court-compelled disclosure, or other equally extraordinary circumstances, we will not distinguish between various degrees of "voluntariness" in waivers of the attorney-client privilege. (internal citations omitted)²¹³

The appellate court then remanded the case to determine the extent of the subject matter covered by the waiver.

Summarizing the above representative cases, courts adopting the strict posture believe it encourages lawyers to employ effective precautions,²¹⁴ to treat confidential information "like jewels – if not crown jewels," "[o]therwise, there is a temptation to seek artificially to expand the content of privileged matter."²¹⁵ Further, once a third party obtains the information, the rationale is that confidentiality is lost and cannot be restored – "one cannot unring the bell;"²¹⁶ the "horse is out of the barn."²¹⁷ *Underwater Storage, Inc. v. United States Rubber Co.* even held that a document produced "entered the public domain."²¹⁸ Simply, "inadvertence is, after all, merely a euphemism for negligence, and certainly... one is expected to pay a price for one's negligence."²¹⁹

Critics argue that the strict test could have "a chilling effect" on lawyer-client communication,²²⁰ since the client knows that all confidentiality will be waived through any inadvertence by the lawyer. By penalizing the client this way, such strictness goes against the purpose of the privilege, to "ensure that a client remains free from apprehension that consultations with a legal advisor will be disclosed."²²¹

²¹³ *Id.* at 980.

²¹⁴ Stevenson, *supra* note 165, at 360.

²¹⁵ *In Re Sealed Case*, 877 F.2d at 980.

²¹⁶ *Federal Deposit Insurance Corp. v. Singh*, 140 F.R.D. 252, 253 (D. Me. 1992).

²¹⁷ *Hamilton v. Hamilton Steel Corp.*, 409 So. 2d 1111, 1114 (Fla. Dist. Ct. App. 1982).

²¹⁸ *Underwater Storage, Inc. v. United States Rubber Co.*, 314 F. Supp. 546, 549 (D.C. Cir. 1970).

²¹⁹ Stevenson, *supra* note 165, at 360, *quoting* *International Digital Systems v. Digital Equipment*, 120 F.R.D. 445, 450 (D. Mass. 1988).

²²⁰ Stevenson, *supra* note 165, at 360.

²²¹ *Berg Electronics, Inc. v. Molex, Inc.*, 875 F. Supp. 261, 262 (D.C. Del. 1995).

2. The lenient test (no waiver rule)

For courts that take the opposite extreme, mere inadvertence does not waive the privilege.²²² First, they hold that since the privilege belongs to the client, the lawyer cannot waive it.²²³ Second, since waiver is an intentional relinquishment by definition, inadvertent waiver is "inherently contradictory."²²⁴

Critics contend that such leniency "presents problems in discerning the client's intent." Likely, all clients would deny the intent to waive the privilege.²²⁵ *Underwater Storage, Inc. v. United States Rubber Co.*²²⁶ precisely held:

The plaintiff turned over to his attorney the documents to be produced. This letter was among them. The Court will not look behind this objective fact to determine whether the plaintiff really intended to have the letter examined. Nor will the Court hold that the inadvertence of counsel is not chargeable to his client.²²⁷

Indeed, a client would also lose a cause of action if a lawyer neglects to file the case before it prescribes, and lose an appeal if he fails to file notice on time. "It would be anomalous to treat the attorney-client privilege as more personal to the client than these rights, which are case-dispositive."²²⁸ Moreover, other implied waivers of attorney-client privilege exist despite lack of intent to waive it.²²⁹

Finally, this approach reduces the lawyer's incentive to protect confidential information since only the client is deemed responsible for

²²² *United States v. Zolin*, 809 F.2d 1411, 1417 (9th Cir. 1987); *Georgetown Manor, Inc. v. Ethan Allen, Inc.*, 753 F.Supp. 936, 938 (S.D.Fla. 1991); *In re Sealed Case*, 120 F.R.D. 66, 72 (N.D.Ill. 1988); Roberta Harding, *Waiver: A Comprehensive Analysis of a Consequence of Inadvertently Producing Documents Protected by the Attorney-Client Privilege*, 42 CATH. U.L. REV. 465, 472 (1993).

²²³ *Helman v. Murry's Steaks, Inc.*, 728 F.Supp. 1099, 1104 (D.Del. 1990).

²²⁴ *Bank Brussels Lambert v. Credit Lyonnais*, 160 F.R.D. 437, 442 (S.D.N.Y. 1995). See *Mendenhall v. Barber-Greene Co.*, 531 F.Supp. 951, 954 (N.D.Ill. 1982).

²²⁵ *Stevenson*, *supra* note 165, at 361.

²²⁶ 314 F. Supp. 546 (D.C. Cir. 1970).

²²⁷ *Id.* at 549.

²²⁸ *Bank Brussels Lambert v. Credit Lyonnais*, 160 F.R.D. 437, 442 (S.D.N.Y. 1995).

²²⁹ *Id.*, citing *In re von Bulow*, 828 F.2d 94, 101 (2nd Cir. 1987).

waiver.²³⁰ Some cases, it must be noted, do not even discuss the extremely lenient approach.²³¹

3. The middle of the road or balancing test (case by case approach)²³²

The majority of inadvertent disclosure cases, however, are decided with less absolute standards, on a case-to-case basis. "This analysis serves the purpose of the attorney client privilege, the protection of communications which the client fully intended would remain confidential, yet at the same time will not relieve those claiming the privilege of the consequences of their carelessness if the circumstances surrounding the disclosure do not clearly demonstrate that continued protection is warranted."²³³ Many recent cases consider this the most realistic approach because it recognizes the inevitability of errors,²³⁴ and considers it most faithful to the privilege's purpose.²³⁵

The Fifth Circuit's leading case *Allread v. City of Grenada* upheld a five-point multifactor analysis:

- (1) precautions taken to prevent inadvertent disclosure;
- (2) the time taken to rectify the error;
- (3) the scope of the discovery;
- (4) the extent of the disclosure; and

²³⁰ Bank Brussels Lambert, 160 F.R.D. at 442.

²³¹ See *Allread v. City of Grenada*, 988 F.2d 1425, 1434-35 (5th Cir. 1993).

²³² *United States v. Gangi*, 1 F.Supp.2d 256, 264 (S.D.N.Y. 1998).

²³³ *Allread*, 988 F.2d 1425 at 1434. See *Bank Brussels Lambert* 160 F.R.D. 437 at 442.

²³⁴ *Asian Vegetable Research and Development Center v. Institute of International Education*, 1995 WL 491491, at *7 (S.D.N.Y. 1995).

²³⁵ "This regimen best reconciles the principles underlying the attorney-client privilege with the realities of document production in complex litigation." *Bank Brussels Lambert*, 160 F.R.D. at 443. "The court finds the rule of law established by these cases that look to intent best serves the interests of the attorney-client privilege, as it protects the client from the apprehension that consultations with their legal advisors will be inadvertently disclosed and applies the privilege in a way that is predictable and certain." *Berg Electronics, Inc. v. Molex, Inc.*, 875 F. Supp. 261, 262 (D.C. Del. 1995). "[T]he fairest approach when considering different and individual circumstances surrounding inadvertent disclosure." *Stevenson*, *supra* note 165, at 363.

(5) the overriding issues of fairness²³⁶

No single factor is determinative; courts consider the five and weigh them accordingly.²³⁷ Thus, in the 2003 case *Ferko v. National Association for Stock Car Auto Racing*,²³⁸ the court found against waiver despite the inadvertent disclosure of two key documents:

(1) A team of attorneys sorted documents involved in discovery, and the two inadvertently disclosed were even marked "highly confidential."

(2) The plaintiff's lawyers were contacted four days after the mistake was made, and the documents were promptly returned.²³⁹

(3) The inadvertence was understandable given over 63,000 pages of documents were involved.²⁴⁰

(4) Two out of 63,000 pages is understandable, and this percentage is far less than that of other cases where waiver was not found.²⁴¹

(5) It is only fair to allow the privilege despite the disclosure, to encourage "full and frank communication." Moreover, the plaintiff has no inherent right in fairness to retain documents inadvertently disclosed.²⁴²

The 2002 case *Fleet Business Credit Corp. v. Hill City Oil Co.*²⁴³ obtained similar results using the *Alldread* framework:

²³⁶ *Alldread*, 988 F.2d at 1433, *citing* *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323 (N.D.Cal.1985).

²³⁷ *Delsa*, *supra* note 167, at 956.

²³⁸ *Ferko v. National Association for Stock Car Auto Racing, Inc.*, 218 F.R.D. 125 (E.D. Tex. 2003).

²³⁹ *See* *Myers v. City of Highland Village*, 212 F.R.D. 324, 327-328 (E.D.Tex.2003). In *Myers*, opposing counsel was notified three weeks later.

²⁴⁰ *See* *Lazar v. Mauney*, 192 F.R.D. 324, 330 (N.D.Ga.2000). *Lazar* involved 1,000 pages.

²⁴¹ *See* *Myers*, 212 F.R.D. at 327-28 (E.D.Tex.2003); *Lazar* 192 F.R.D. at 330; *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985).

²⁴² *Ferko*, 218 F.R.D. at 140-41 (E.D. Tex. 2003), *citing* *Alldread*, 988 F.2d at 1434.

²⁴³ 2002 WL 31741282 (W.D.Tenn. 2002).

(1) Three attorneys and one paralegal reviewed the documents, isolated privileged ones, and tagged the others with pre-printed tabs. An outside copy service was employed to copy and number the latter documents.

(2) The error was discovered less than three months later, and the opposing lawyer was notified within days of the discovery.

(3) The inadvertence was understandable given over 16,000 pages of documents were involved.

(4) 30 out of 16,000 pages were disputed as inadvertently disclosed, "a relatively small, but acceptable margin of error."

(5) Finding the other requisites met, the court did not further discuss the fairness of finding that no waiver was made.²⁴⁴

The privilege is considered waived if the five-point test reveals gross negligence instead of inadvertence. In *Ciba-Geigy Corp. v. Sandoz Ltd.*,²⁴⁵ the defendant produced all documents from its database *without* conducting a privilege review. A seemingly flabbergasted court ruled:

[T]he party resisting a waiver argument must demonstrate that it undertook reasonable precautions to avoid inadvertent disclosures of privileged documents. Defendants have not, however, met this burden. The relatively small size of the document production at issue, the lack of time constraints, combined with defendants' own admissions that they failed, on two occasions, to conduct any privilege review prior to producing copies of the Oppikofer document, compel a finding of waiver in this case.²⁴⁶

The court even noted that the defendants' discovery time constraints were self-imposed, and that they failed to screen material even after the first case of "inadvertent" disclosure.

²⁴⁴ *Id.* at *3, *aff'd* In re Copper Market Anti-trust Litigation, 200 F.R.D. 213, 222 (S.D.N.Y. 2001).

²⁴⁵ 916 F. Supp. 404 (D.N.J. 1995).

²⁴⁶ *Id.* at 414.

Judging from the most recent cases, which contain detailed point-by-point *Allread* factual discussions, one makes two conclusions. First, inadvertent disclosure is not penalized as a general rule, especially when documents begin running to the thousands. Courts seem to even assume that it is inevitable. Second, the first prong is the most important, and so long as one establishes before the judge that one implemented a concrete, systematic method of privilege review, waiver is unlikely to be found. Omissions on this sole point are fatal, as evidenced by *Ciba-Geigy*. On the other hand, in the 2003 case *United States v. Rigas*,²⁴⁷ the court did not find waiver after precautions were sufficiently established. This was despite the fact that the inadvertence involved a transfer of files that was entirely foreseeable, although the expert called testified, "he had never witnessed such an occurrence in all his years of experience with technology-based litigation services."²⁴⁸ *Simon Property Group L.P. v. mySimon, Inc.*²⁴⁹ might have turned on this issue as the court found no evidence of concrete precautions aside from having a lawyer review the disclosed documents, which were not voluminous. However, the documents in *Simon Property* were inadvertently disclosed to an expert witness and not the opposing lawyer. Although the court would have deemed this waiver because the expert would have to be cross-examined, *in camera* inspection revealed the inadvertently disclosed material were irrelevant to the expert's testimony. Thus, it was still possible to "unring a bell."²⁵⁰

A concrete system, of course, may not outbalance a suspiciously higher number of disclosures that belie inadvertence. For example, *United States v. Keystone Sanitation Co.*²⁵¹ found waiver due to the extent and the number of disclosures, and that the interest of justice would not be served if the confidential information already disclosed was denied.

Critics of the *Allread* approach adhere to the strict interpretation, taking the latter line and arguing "there [is] no benefit in analyzing the reasonableness of the precautions taken."²⁵² The fact of inadvertence, for them, belies the reasonableness of the precautions. Again, however, the most recent decisions reject this simplistic argument in favor of allowing the

²⁴⁷ 281 F.Supp.2d 733 (S.D.N.Y. 2003).

²⁴⁸ *Id.* at 739.

²⁴⁹ 194 F.R.D. 644 (S.D. Ind. 2000).

²⁵⁰ *Id.* at 649.

²⁵¹ 885 F. Supp. 672 (M.D. Pa. 1994).

²⁵² *International Digital Systems v. Digital Equipment*, 120 F.R.D. 445, 445-48 (D. Mass. 1988).

attorney-client privilege when, for example, inadvertence is alleged for only two out of 63,000 pages of documents.

IV. THE WORK PRODUCT PRIVILEGE

A survey of Philippine jurisprudence shows that the phrase "work product" has appeared only in passing in *Fortune Corp. v. Court of Appeals*²⁵³ in 1994, and arguably only because Justice Narvasa cited from an American remedial law text. A survey of leading Evidence commentaries shows it is not even discussed.²⁵⁴ The sole exception is the 2004 vintage Remedial Law series of Professor Antonio Bautista – the Evidence volume devotes one page in the section on attorney-client privilege,²⁵⁵ while the Civil Procedure volume devotes one paragraph in the section on discovery.²⁵⁶

Thus, although work product has long been part of the University of the Philippines Evidence curriculum,²⁵⁷ its jurisprudential foundations are tenuous at best. It is fortunate that the foundations are nevertheless clear, because work product has become practically intertwined with invocations of attorney-client privilege in recent American electronic discovery cases. It is arguably more important because it more specifically pertains to the discovery and pretrial stage compared to the latter privilege²⁵⁸ -- "waiver of the protections afforded by the work product doctrine is a tactical litigation decision... the subsequent decision on whether or not to 'show your hand' is quintessential litigation strategy."²⁵⁹

Though the two are discussed together, the work product privilege is distinct from the attorney-client privilege. While the latter provides a cloak of protection to communication between lawyer and client to facilitate disclosure, the former protects the lawyer's "privacy in their work and for freedom from interference in the task of preparing the client's case for

²⁵³ *Fortune Corp. v. Court of Appeals*, G.R. No. 108119, Jan. 19, 1994.

²⁵⁴ See II FLORENZ REGALADO, REMEDIAL LAW COMPENDIUM 615-616 (2002); FRANCISCO, *supra* note 74, at 150-59.

²⁵⁵ ANTONIO BAUTISTA, BASIC EVIDENCE 71 (2004).

²⁵⁶ ANTONIO BAUTISTA, BASIC CIVIL PROCEDURE 127-28 (2003), *citing Hickman v. Taylor*, 329 U.S. 495 (1947).

²⁵⁷ Professor Bautista's new line of textbooks, for example, are based on his class outline. Other veteran faculty members such as Professor Rogelio Vinluan have long emphasized this lesser-cited privilege as well.

²⁵⁸ BAUTISTA, BASIC EVIDENCE, *supra* note 255, at 71.

²⁵⁹ *In re Columbia/HCA Healthcare Corp. Billing Practices Litigation*, 293 F.3d 289, 306-07 (6th Cir. 2002).

trial."²⁶⁰ It protects information not necessarily because it is confidential, but prevents other parties from peeking into the legal tactics unfolding in an attorney's mind via files and papers²⁶¹ prepared in anticipation of litigation.²⁶² The landmark case *Hickman v. Taylor*²⁶³ stated:

Were such materials open to opposing counsel on mere demand, much of what is now put down in writing would remain unwritten. An attorney's thoughts, heretofore inviolate, would not be his own. Inefficiency, unfairness and sharp practices would inevitably develop in the giving of legal advice and in the preparation of cases for trial.²⁶⁴

Thus, the work product privilege primarily allows lawyers to gather and study information unimpaired²⁶⁵ in a protected zone of privacy.²⁶⁶ It also discourages lawyers from using their opponents as unwitting aides, and ensures that "lawyers do not work with wits borrowed from their brother lawyers."²⁶⁷

The key distinction for electronic discovery, however, is the greater breadth of the work product doctrine.²⁶⁸ First, again, it is not limited to confidential information conveyed by a client during a professional relationship – "work product is protected *because* of its content, while attorney-client communication is protected *despite* its content."²⁶⁹ This was seen in *Hickman* itself, where an opposing lawyer was blocked from obtaining nonconfidential interviews made by his opponent on witnesses known and available to him. Thus, the privilege may apply to any material so long as it is raised against "an attempt to secure the production of written

²⁶⁰ MCCORMICK, *supra* note 65, §96, at 135.

²⁶¹ *Hickman* 329 U.S. at 510-11; *Dunn v. State Farm Fire & Casualty Company*, 927 F.2d 869, 875 (5th Cir. 1991).

²⁶² *Griffith v. Davis*, 161 F.R.D. 687, 699 (C.D.Cal. 1995).

²⁶³ 329 U.S. 495.

²⁶⁴ *Id.* at 511.

²⁶⁵ MCCORMICK, *supra* note 65, § 96, at 135.

²⁶⁶ *Hickman*, 329 U.S. at 511; *United States v. Nobles*, 422 U.S. 225, 238 (1975); *United States v. Adlman*, 134 F.3d 1194, 1196 (2nd Cir. 1998).

²⁶⁷ BAUTISTA, BASIC CIVIL PROCEDURE, *supra* note 256, at 128. "Discovery was hardly intended to enable a learned profession to perform its functions either without wits or on wits borrowed from the adversary." *Hickman*, 329 U.S. at 516 (Jackson, J., *concurring*).

²⁶⁸ *United States v. Nobles*, 422 U.S. 225, 238 n.11 (1975); *In re Worldcom, Inc. Securities Litigation*, 2003 WL 22953645, at *3 (S.D.N.Y. 2003), *aff'd* *National Education Training Group v. Skillsoft Corp.*, 1999 WL 378337, at *5 (S.D.N.Y. 1999).

²⁶⁹ *KW Muth Co. v. Bing-Lear Manufacturing Group, L.L.C.*, 2003 WL 23305864, at *12 (E.D.Mich. 2003).

statements and mental impressions contained in the files and the mind of the attorney."²⁷⁰ The confidential nature of the information itself is not so central as the pattern or organization revealed by its recording, and the latter can be revealed in notes regarding information readily available to the opponent through other means. The confidentiality that must be maintained, thus, pertains not to the information itself, but to the particular manner of recording in a document.²⁷¹

Second, as a result, it means that the work product privilege can be invoked independently by the lawyer, since it protects his privacy and not the client's.²⁷²

In seeming trade-off for this breadth, the work product privilege is much less absolute and provides only a qualified immunity.²⁷³

Where relevant and non-privileged facts remain hidden in an attorney's file and where production of those facts is essential to the preparation of one's case, discovery may properly be had. Such written statements and documents might, under certain circumstances, be admissible in evidence or give clues as to the existence or location of relevant facts. Or they might be useful for purposes of impeachment or corroboration. And production might be justified where the witnesses are no longer available or can be reached only with difficulty.... But the general policy against invading the privacy of an attorney's course of preparation is so well recognized and so essential to an orderly working of our system of legal procedure that a burden rests on the one who would invade that privacy to establish adequate reasons to justify production through a subpoena or court order.²⁷⁴

As implied above, however, factual scenarios "showing absolute necessity to avoid hardship or injuries"²⁷⁵ are the exception, not the general rule. *Hickman* itself closed, "If there should be a rare situation justifying

²⁷⁰ *Hickman*, 329 U.S. at 509.

²⁷¹ BAUTISTA, BASIC EVIDENCE, *supra* note 255, at 71.

²⁷² *Id.* Of course, it cannot be asserted against the client. *Id.* See *United States v. Regan*, 281 F.Supp.2d 795, 805-06 (E.D. Va. 2003). "This privilege does not apply here because the documents are not the opinions or the impressions of Defendant's attorneys, made in connection with this case. The documents were created by the Defendant."

²⁷³ BAUTISTA, BASIC EVIDENCE, *supra* note 255, at 71.

²⁷⁴ *Hickman*, 329 U.S. at 512, cited in BAUTISTA, BASIC CIVIL PROCEDURE, *supra* note 256, at 127-28.

²⁷⁵ BAUTISTA, BASIC CIVIL PROCEDURE, *supra* note 256, at 128.

production of these matters, petitioner's case is not of that type." Moreover, the mental impressions themselves or "opinion work product" now enjoy heightened privilege;²⁷⁶ necessary facts which constitute "ordinary" or "fact work product" may be disclosed without producing the actual documents that would reveal the attorney's state of mind. This must be emphasized given how much easier it is now to backtrack along an opposing lawyer's electronic trail.

Examining the history of the work product privilege itself, it originated from an amendment recommended by the Advisory Committee on Federal Rules of Civil Procedure in 1946:

The court shall not order the production or inspection of any writing obtained or prepared by the adverse party, his attorney, surety, indemnitor, or agent in anticipation of litigation or in preparation for trial unless satisfied that denial of production or inspection will unfairly prejudice the party seeking the production or inspection in preparing his claim or defense or will cause him undue hardship or injustice. The court shall not order the production or inspection of any part of the writing that reflects an attorney's impressions, conclusions, opinions, or legal theories, or except as provided in Rule 35, the conclusion of an expert.²⁷⁷

The proposal was ignored until *Hickman* was decided by the United States Supreme Court the following year. Lower courts, however, had considerable disagreement interpreting the doctrine, until the Supreme Court amended its rules of procedure in 1970 to specify the privilege's scope.²⁷⁸ *Hickman* remains a brooding omnipresence, much cited and quoted by the courts, and in fact still governs discussion of the privilege.²⁷⁹

Though more loosely discussed in jurisprudence compared to the attorney-client privilege, the Federal Rules of Civil Procedure now provide three requisites for the work product privilege:

1. a document or tangible thing
2. prepared in anticipation of litigation and not made in the ordinary course of business

²⁷⁶ Murphy, *supra* note 57, at 1847; National Education Training Group v. Skillsoft Corp., 1999 WL 378337, at *6 (S.D.N.Y. 1999).

²⁷⁷ MCCORMICK, *supra* note 65, at 137.

²⁷⁸ *Id.*

²⁷⁹ *Upjohn Co. v. United States*, 449 US 383, 397-402 (1981).

3. prepared by or for a party, or by or for its representative, including an attorney, consultant, surety, indemnitor, insurer, or agent²⁸⁰

The burden of establishing these, as in the former privilege, rests on the party claiming it.²⁸¹

Finally, the work product privilege is subject to some of the attorney-client privilege's requirements. As discussed, the documents sought must have been kept confidential, even if the contents are not confidential material in themselves. The privilege is similarly subject to the crime-fraud exception.²⁸² The discussion on waiver²⁸³ and inadvertent disclosure is likewise squarely applicable, though it must be noted that the invocation of attorney-client privilege alone may be interpreted as a waiver of work product privilege, and vice-versa.²⁸⁴ "The Second Circuit has noted its preference that parties 'raise all objections at once, rather than in staggered batches, so that discovery does not become a 'game.'"²⁸⁵ Some courts are more flexible with inadvertence and examine the nature and willfulness of such an omission.²⁸⁶

²⁸⁰ *Ricoh Co., Ltd. v. Aeroflex, Inc.*, 219 F.R.D. 66, 68 (S.D.N.Y. 2003); *Goodyear Tire & Rubber Co. v. Kirk's Tire & Auto Servicecenter of Haverstraw, Inc.*, 2003 WL 22110281, at *4 (S.D.N.Y. 2003); *In re Honeywell International, Inc., Securities Litigation*, 2003 WL 22722961, at *3 (S.D.N.Y. 2003); *National Education Training Group v. Skillsoft Corp.*, 1999 WL 378337, at *5 (S.D.N.Y. 1999); *Compagnie Francaise d'Assurance Pour le Commerce Extérieur v. Phillips Petroleum Co.*, 105 F.R.D. 16, 41 (S.D.N.Y. 1984).

²⁸¹ *Resort of World, N.V. v. Clarendon American Insurance Co.*, 1997 WL 739586, at *1 (S.D.N.Y. 1997); *Von Bulow v. von Bulow*, 811 F.2d 136, 144 (2nd Cir. 1987).

²⁸² *In re John Doe*, 662 F.2d 1073, 1079 (4th Cir. 1981); *United States v. Regan*, 281 F.Supp.2d 795, 803 (E.D. Va. 2003).

²⁸³ *In re Columbia/HCA Healthcare Corp. Billing Practices Litigation*, 293 F.3d 289 (6th Cir. 2002); *Kintera, Inc. v. Convio, Inc.*, 219 F.R.D. 503, 511-12 (S.D.Cal. 2003).

²⁸⁴ *In re Honeywell*, 2003 WL 22722961, at *4; *Bowne, Inc. v. AmBase Corp.*, 150 F.R.D. 465, 489-90 (S.D.N.Y. 1993); *Carte Blanche PTE., Ltd. v. Diners Club International, Inc.*, 130 F.R.D. 28, 32 (S.D.N.Y. 1990).

²⁸⁵ *In re Honeywell*, 2003 WL 22722961, at *5, *citing In re DG Acquisition Corp.*, 151 F.3d 75, 81 (2nd Cir. 1998); *United States v. Bryan*, 339 U.S. 323, 331 (1950).

²⁸⁶ *In re Honeywell*, 2003 WL 22722961, at *5, *citing RMED International, Inc. v. Sloan's Supermarkets, Inc.*, 2003 WL 41996, at *3 (S.D.N.Y. 2003); *AFP Imaging Corp v. Philips Medizin Systems*, 1993 WL 541194, at *3 (S.D.N.Y. 1993).

V. APPLICATION OF THE WORK PRODUCT PRIVILEGE TO ELECTRONIC DOCUMENTS

This section discusses that the work product privilege must similarly be applied broadly, given the increased number of communications now electronically reduced to writing. Pushing its fringes outward, one sees its ready application to agents of attorneys aside from the attorneys themselves, communications by expert witnesses, and communications regarding matters that are arguably in anticipation of litigation.

The brief 2003 decision *Cruz v. Delapaz* dealt with two boxes of documents and offers a clear glimpse of the work product privilege's application in an ordinary proceeding:

[T]he documents consist mainly of handwritten and typewritten attorney notes, drafts of documents and letters, memoranda reflecting legal research and analysis, and emails regarding the 'sheetrock cases,' a term used to refer to this litigation. The documents that are related to litigation and not created as part of routine office procedure, and reveal the attorneys' mental impressions, are protected from disclosure by the work product doctrine. Most of the documents in these boxes fall into that category.

Some of the documents, on the other hand, are not protected by the work product privilege. Specifically, the boxes contain copies of court documents and court opinions, letters dealing with issues other than the impending litigation of the 'sheetrock cases,' copies of lab reports, and letters from opposing attorneys or from individuals outside the district attorney's office. Because there is no basis for claiming work product privilege as to these documents, they shall be produced to the Plaintiffs. Also, the file contains several documents relating to informants that bear dates of 1999 and 2000. The District Attorney's office has presented no evidence, by affidavit or otherwise, to show that litigation was anticipated at that time, and have asserted only the work product privilege. Because there is no evidence that the documents were created in anticipation of litigation, the work product privilege cannot apply. Also, the boxes contain copies of correspondence between the District Attorney's office and the Office of the Attorney General regarding Public Information Act requests, which are not covered by work product privilege.²⁸⁷

Work product, as noted, is broader than the attorney-client privilege because it is not restricted to confidential information, and may even be

²⁸⁷ *Cruz v. Delapaz*, 2003 WL 22415743, at *1 (N.D.Tex. 2003).

asserted by the lawyer independently of his client. Again, it is divided into two categories. "Ordinary" or "fact work product" refers to the nonprivileged facts such as the identity of witnesses discussed in *Hickman*, and is qualifiedly privileged in that its disclosure can be compelled if it can only be obtained elsewhere with great difficulty.²⁸⁸ "Opinion work product" or the attorney's mental impressions themselves, however, is held absolutely privileged in many jurisdictions²⁸⁹ and is deemed to cover "matters at the heart of the adversary system."²⁹⁰ Note that fact work product need not reflect mental impressions; *Kintaro, Inc. v. Convio, Inc.* held e-mailed witness statements privileged simply because they were collected in anticipation of litigation, irrespective of mental impressions revealed in the line of inquiry.²⁹¹

It should be apparent from a document whether it contains ordinary work product that an opponent should discover on his own. Taking a cue from *TVT Records, Inc. v. The Island Def Jam Music Group*, thus, the subtle expansion comes when one asserts that a seemingly innocuous, matter-of-fact communication nevertheless reveals a glimpse of the lawyer's state of mind, bringing the opinion work product privilege to bear. This was seen in *In re Honeywell International*,²⁹² where audit letters and litigation reports

²⁸⁸ *In re Grand Jury Proceedings*, 219 F.3d 175, 190-91 (2nd Cir. 2000); *United States v. Regan*, 281 F.Supp.2d 795, 803 (E.D. Va. 2003).

²⁸⁹ *Murphy*, *supra* note 57, at 1847. See *Upjohn Co. v. United States*, 449 U.S. 398, 402 (1981); *National Education Training Group v. Skillsoft Corp.*, 1999 WL 378337, at *5 (S.D.N.Y. 1999); *United States ex rel. Burroughs v. DeNardi Corp.*, 167 F.R.D. 680 (S.D. Cal. 1996); *Connolly Data Systems v. Victor Technologies*, 114 F.R.D. 89 (S.D. Cal. 1987).

There is no United States Supreme Court precedent on this point, but some circuit courts fall short of holding an absolute privilege. *Dale Cendali & Susan Rodihan, Electronic Discovery*, 755 PLI/PAT 615, 636 n.50 (2003). *Holmgren v. State Farm Mutual Automobile Insurance Co.*, 976 F.2d 573, 577 (9th Cir. 1992). "[O]pinion work product of insurer could be discovered and admitted in bad-faith insurance claim settlement case in which mental impressions of insurer were at issue and need for material was compelling." *Duplan Corp. v. Moulinage et Retorderie de Chavanoz*, 509 F.2d 730, 734 (4th Cir. 1974). "No showing of relevance, substantial need or undue hardship should justify compelled disclosure of an attorney's memo, impressions, conclusions, or legal theories."

²⁹⁰ *Blumenthal v. Drudge*, 186 F.R.D. 236, 241 (D.D.C. 1999).

²⁹¹ *Kintera, Inc. v. Convio, Inc.*, 219 F.R.D. 503, 509 (S.D. Cal. 2003). The opposing party was unable to show substantial need, since it could conduct depositions, and the mere impeachment value of the statements already collected by the other party was insufficient to overturn the privilege.

²⁹² *In re Honeywell International, Inc., Securities Litigation*, 2003 WL 22722961 (S.D.N.Y. 2003).

prepared by counsel but intended to assist in business decisionmaking were nevertheless privileged. "Where a document was created because of anticipated litigation, and would not have been prepared in substantially similar form but for the prospect of that litigation," it is covered by the work product rule.²⁹³ Again, this applies even to electronic documents concerning nonprivileged subject matter that would be beyond the scope of attorney-client privilege.

Looking at the cases discussed under attorney-client privilege, opinion work product might also be indirectly obtained through client recollections of what a lawyer told them, examining the facts of *Long v. Anderson University*, for example. This logical extension of the privilege has been recognized by the United States Supreme Court in *United States v. Nobles*.²⁹⁴

One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is therefore necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself.²⁹⁵

Further, there are cases where the privilege should not be deemed removed by disclosure to third parties,²⁹⁶ especially when this arises from common interest²⁹⁷ or for some other reason not inconsistent with the privilege.²⁹⁸ For example, in *Ferko v. National Association for Stock Car Auto Racing*, e-mail between the lawyers of the defendant and the nominal defendant in a stockholder derivative suit was deemed unprivileged even though the two had been sharing information regarding deposition issues. However, this was because the defendant failed to make more than blanket assertions of work product privilege, instead of establishing its requisites, not because common interest would not apply.²⁹⁹

One tricky aspect of the electronically expanded paper trail is correspondence with an expert witness. *Simon Property Group v. mySimon* dealt

²⁹³ *Id.* at *6, quoting *United States v. Adlman*, 134 F.3d 1194, 1995 (2nd Cir. 1998).

²⁹⁴ 422 U.S. 225 (1975).

²⁹⁵ *Id.* at 238-39.

²⁹⁶ *Adlman*, 134 F.3d at 1200 n.4.

²⁹⁷ *United States v. American Telephone and Telegraph Co.*, 642 F.2d 1285, 1298-99 (D.C.Cir. 1980).

²⁹⁸ *Granite Partners v. Bear, Stearns & Co. Inc.*, 184 F.R.D. 49, 55 (S.D.N.Y. 1999).

²⁹⁹ *Ferko v. National Association for Stock Car Auto Racing, Inc.*, 219 F.R.D. 396, 399, 402 (E.D. Tex. 2003).

with this issue, and outlined two approaches over the last decade. The first school of thought considers privilege waived as to matters disclosed to an expert witness, as comprehensively discussed in *Karn v. Ingersoll-Rand Co.*³⁰⁰ *Simon Property* summarized:

Magistrate Judge Cosbey... held that the requirements for disclosure of matters "considered" by a testifying expert in forming his or her opinions prevailed over any claim of work-product privilege, including claims that documents constituted "opinion" work-product... [H]e specifically rejected any distinction between documents that the expert "reviewed" and those that the expert "relied upon."³⁰¹

Other cases upheld such a view.³⁰² *Simon Property* itself upheld *Karn* in deciding against privilege for the correspondence it dealt with:

An intentional disclosure of opinion work-product to a testifying expert witness effectively waives the work-product privilege... [A]n attorney should not be permitted to give a testifying expert witness a detailed "road-map" for the desired testimony without also giving the opposing party an opportunity to discover that "map" and to cross-examine the expert about its effect on the expert's opinions in the case.³⁰³

Similarly, in the earlier *Bartley v. Isuzu Motors Ltd.*,³⁰⁴ a plaintiff in a product liability case hired an expert to create computer simulations of an accident. The court ruled that the defendant should be allowed to see all data fed and manipulated through the computer, and the entire thought process involved in the experiment.³⁰⁵

³⁰⁰ 168 F.R.D. 633, 637-41 (N.D.Ind. 1996).

³⁰¹ *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 644, 646-47 (S.D. Ind. 2000).

³⁰² *Id.*, citing *Lamonds v. General Motors Corp.*, 180 F.R.D. 302, 305-06 (W.D.Va. 1998); *Musselman v. Phillips*, 176 F.R.D. 194, 199-202 (D.Md. 1997); *B.C.F. Oil Refining, Inc. v. Consolidated Edison Co. of New York*, 171 F.R.D. 57, 64-67 (S.D.N.Y. 1997); *Barna v. United States*, 1997 WL 417847, at *2-3 (N.D.Ill. 1997); 8 CHARLES WRIGHT ET AL., *FEDERAL PRACTICE AND PROCEDURE* § 2016.2, 252 (2nd ed. 1994).

³⁰³ *Simon Property Group*, 194 F.R.D. at 647.

³⁰⁴ 151 F.R.D. 659 (D. Colo. 1993).

³⁰⁵ *Id.* at 660.

The second school of thought, however, holds that the need to disclose the basis of the expert witness' testimony does not override the privilege granted over opinion work product.³⁰⁶

It must be noted, however, that *Simon Property* refused to even allow redaction of work product protected components of the material disclosed to their expert, because the court believed an amendment to their Rule 26 barred even this. Given the potential volume of electronic records and the lack of an explicit rule in the Philippines to date, it is submitted that there should be a distinction between material "reviewed" and "relied on" for discovery purposes. Peripheral documents such as daily or supplemental e-mail correspondence between the lawyer and expert might arguably remain privileged and deemed not "relied upon," or at least treated on a case to case basis, given the oftentimes casual nature of e-mail. The actual computer data in *Bartley*, for example, and daily correspondence between the expert and a lawyer should be treated differently. One approach taken in other cases was to find waiver of fact work product, but not opinion work product.³⁰⁷ Such easily conducted correspondence might contribute little more factual evidence for the opponent's case, but may yield stray mental impressions.

Another tricky relationship in jurisprudence is that of an insurer's employees and the insured. In the 2003 decision *Benton v. Brookfield Properties*, the court withheld privilege from an e-mail prepared by an insurer's engineer following the collapse of an elevator at a construction site, which killed two workers. He made this immediately after he traveled to the site to investigate the cause of the collapse. The defendant's lawyers were also on site, but they did not talk to the engineer. The court held:

An insurance company's decision whether to afford coverage is part of its normal business decision-making and does not constitute work-product even though the insurance company may face the prospect that if coverage is denied, the insured will commence litigation against it. Still less can work-product immunity be invoked in a case in which the insurer is not a party, and the work done was undertaken immediately following the assertedly insurable event in

³⁰⁶ *Nexus Products Co. v. CVS New York, Inc.*, 188 F.R.D. 7, 9-11 (D.Mass. 1999); *Magee v. Paul Revere Life Insurance Co.*, 172 F.R.D. 627, 642-43 (E.D.N.Y. 1997).

³⁰⁷ *Haworth, Inc. v. Herman Miller, Inc.*, 162 F.R.D. 289, 294-96 (W.D. Mich. 1995); *All West Pet Supply Co. v. Hill's Pet Products Division, Colgate-Palmolive Co.*, 152 F.R.D. 634, 638-39 (D.Kan. 1993).

order to assist the insurer in determining whether to cover the expected claim.³⁰⁸

First, such an absolute rule seems to deter communication between the insurer and its own client; even assuming it is the best policy, it is submitted that one should at least consider factors such as the length and quality of the parties' relationship, and the expectation of honoring the claim. Second, with the greater amount of communication left in writing, such a policy becomes unduly harsh against parties that may well become co-defendants. If such insured parties can be hoisted by their petards, they may well demand that insurers leave nothing in writing until they decide to honor a claim, never mind the aid e-mail lends, which is the evil *Hickman* precisely intended to bar. Note that the recent *Ricoh Co., Ltd. v. Aeroflex, Inc.*,³⁰⁹ drew the line regarding parties covered. It rejected a claim of privilege over e-mails between the employee of another of the lawyer's clients uninvolved in the litigation and a witness likewise not a party.³¹⁰

Discussing another aspect, one must not forget to concretely establish that the documents were prepared in anticipation of litigation, or there are arguably no mental impressions regarding litigation to protect. In *United States v. Connors*,³¹¹ for example, a defendant charged with conspiracy to smuggle Cuban cigars into the United States failed to establish work product protection over electronic records seized from his home since there was no trial yet at the time of seizure, and it did not appear that they were prepared for litigation for some other reason.³¹² In *Cruz v. Delapaz*, the court excluded from privilege routine communication with the Office of the Attorney General and those relating to informants before any litigation could have been anticipated. With respect to the latter, the court held that

³⁰⁸ *Benton v. Brookfield Properties Corp.*, 2003 WL 21749602, at *2-3 (S.D.N.Y. 2003), citing *Weber v. Paduano*, 2003 WL 161340, at *4, 6-8 (S.D.N.Y. 2003); *525 Fulton Street Holding Corp. v. Mission National Insurance Co.*, 1984 WL 591, at *3-4 (S.D.N.Y. 1984); *Fine v. Bellefont Insurance Co.*, 91 F.R.D. 420, 422 (S.D.N.Y. 1981).

³⁰⁹ 219 F.R.D. 66 (S.D.N.Y. 2003).

³¹⁰ *Id.* at 68. "Movants suggest that the privilege attaches because the e-mail exchange 'was initiated at the request of [defendants' and Synopsys] shared counsel.' The argument, I gather, is that because Howrey Simon asked the employee of its client Synopsys - which is not a party to this action - to initiate an e-mail exchange with a witness who is also not a party to this action, the e-mails exchanged by the two non-parties magically fall within the work product privilege. This, I assume, is defendants' way of trying to circumvent the rule that a non-party witness is not entitled to assert the work product privilege."

³¹¹ *United States v. Connors*, 2002 WL 1359427 (N.D. Ill. 2002).

³¹² *Id.* at *15.

privilege was asserted without establishing connection to any litigation.³¹³ Finally, *Benton* held that an e-mail by an insurer's employee after visiting an accident site is part of routine business and not in anticipation of legislation, though it is submitted that this is questionable.³¹⁴ Parenthetically, the 2003 case *United States v. Bell*³¹⁵ brings this point home. In discussing privilege over material related to a defendant's "National Institute for Taxation Education" web site, it stated:

Bell is not a lawyer. Bell did not create the subject work product at the direction of a lawyer or in consultation with a lawyer. He sells his "clients" absurd tax advice, which puts these clients in jeopardy of legal sanction. The work product doctrine is an evidentiary privilege and must be strictly construed.³¹⁶

Jurisprudence, however, has particularly upheld that litigation-related systems and routines may contain possible stray mental impressions and should be protected by the privilege. In an electronic context, the participation of a lawyer in the design or functioning of an electronic litigation support database or similar recordkeeping system suffices. In *Hoffman v. United Telecommunications, Inc.*,³¹⁷ for example, the court rejected an interrogatory that requested "detailed information regarding the setup"³¹⁸ of the defendant's litigation support system because it went beyond regarding about the existence of a particular fact or file and into the defendant's very plan for discovery. Similarly, *Lawyers Title Insurance v. U.S.F. & G.*³¹⁹ blocked inquiries regarding the defendant's computer system ostensibly to help the plaintiff frame more accurate discovery requests, because it would reveal confidential methods of processing and storing data.

Third party intervention, however, makes a difference. In *Santiago v. Miles*,³²⁰ the court extended the privilege to printouts from a computer program co-developed by a correction facility's counsel that showed job assignments were distributed in a racially discriminatory manner in the facility. However, a second set of printouts that had been modified, sent to another official during routine business, and never seen by the lawyer was

³¹³ *Cruz v. Delapaz*, 2003 WL 22415743, at *1 (N.D. Tex. 2003).

³¹⁴ *Benton*, 2003 WL 21749602, at *2.

³¹⁵ 217 F.R.D. 335 (M.D. Penn. 2003).

³¹⁶ *Id.*

³¹⁷ 117 F.R.D. 436 (D. Kan. 1987).

³¹⁸ *Id.* at 439.

³¹⁹ *Lawyers Title Ins. Co. v. U.S.F. & G.*, 122 F.R.D. 567 (N.D. Cal. 1988).

³²⁰ F.R.D. 636 (W.D.N.Y. 1988).

held outside the scope of the privilege.³²¹ Finally, the input or thought process of the lawyer involved must be established, given the ease of automating document retrieval today. The 2003 case *Moye, O'Brien, O'Rourke, Hogan & Pickert v. National Railroad Passenger Corp.*³²² ruled against privilege because the litigation database prepared consisted largely of photographic computer scans of existing documents, and no special indexing was asserted.

Lastly, it is important to note that the confidentiality of the documents, again not necessarily the contents, must still be established to claim the work product privilege. The claim of privilege was rejected in *In re Worldcom, Inc. Securities Litigation*, for example, because the contested electronic record was held to be a mere summary of funds, an accounting that inevitably would have been created and disclosed at some point.³²³ It would have been different had they somehow held some confidential opinion, such as projections regarding tax consequences. In *Bank of America v. Terra Nova Insurance*,³²⁴ documents collected by an investigator, including an e-mail by an insurance agent suspected of fraud stating he was contemplating suicide, were deemed unprivileged because they had already been disclosed to the government in the hopes of forestalling an investigation.³²⁵ In such cases, unless there is a concrete agreement regarding confidentiality, the disclosure "substantially" or "materially" increases the likelihood that an adversary will obtain the information" since the government itself may prosecute or make the material public.³²⁶ In *Kintera Inc. v. Convio Inc.*, the disclosure of substantial portions of contested documents on the party's web site clearly dissolved their privileged status.³²⁷ The court found the party a "sophisticated, well-counseled party" who

³²¹ *Id.* at 637-40.

³²² 2003 WL 21146674, at *16 (M.D.Fla. 2003).

³²³ *In re Worldcom, Inc. Securities Litigation*, 2003 WL 22953645, at *3 (S.D.N.Y. 2003).

³²⁴ 212 F.R.D. 166 (S.D.N.Y. 2002).

³²⁵ *Id.* at 168, 172.

³²⁶ *Id.* at 170, citing *GAF Corp. v. Eastman Kodak Co.*, 85 F.R.D. 46, 51-52 (S.D.N.Y. 1979); *ECDC Environmental v. New York Marine & General Insurance Co.*, 1998 WL 614478, at *4 (S.D.N.Y. 1998); *U.S. Information Systems, Inc. v. International Board of Electrical Workers, Local Union No. 3*, 2002 WL 31296430, at *3 (S.D.N.Y. 2002).

³²⁷ *Kintera, Inc. v. Convio, Inc.*, 219 F.R.D. 503, 512-13 (S.D.Cal. 2003).

intentionally disclosed the information 'in an act calculated to advance that party's commercial interests.'"³²⁸

VI. INSUFFICIENCY OF THE ATTORNEY-CLIENT AND WORK PRODUCT PRIVILEGES

This section discusses that when privilege finds no application, the only aspect of the remaining *Hickman* prongs that has concrete benchmarks in jurisprudence is the cost of discovery, and is not an issue in every case. Aside from these, matters such as irrelevance and bad faith are largely left to the judge's discretion. The discussion concludes that one must turn to the evolving fundamental right to privacy for more complete protection against electronic discovery.

After an exhaustive review of recent jurisprudence, one can see subtle actual and potential expansion of the attorney-client and work product privileges as applied to pervasively used e-mail and other electronic documents. However, one also sees that whatever breadth privilege possesses pales before the clearly broader application of electronic discovery in general.

First of all, privilege may only be invoked in very specific situations, when specific requisites are established. Barring, for example, a laptop computer containing a doctor's patient records, privilege may generally be invoked only when one's lawyer is involved in the communications. Second, even when they are properly invoked, privileges are seen as exceptions to a general rule. The burden is always on the party claiming it, and their application is always strictly construed against that party.³²⁹ One notes that decisions have far more often discussed the financial burden caused by an overbroad discovery order than they have the emotional intrusion caused by having adverse parties sift through one's daily, idle e-mail use.

Reviewing the *Hickman* and *Republic v. Sandiganbayan* framework once again, discovery is limited when it:

1. "is being used in bad faith or in such a manner as to annoy, embarrass or oppress the person subject to the inquiry"

³²⁸ *Id.* at 513, quoting *Electro Scientific Indus. v. Gen. Scanning, Inc.*, 175 F.R.D. 539 (N.D.Cal. 1997).

³²⁹ Moyer, 2003 WL 21146674, at *13.

2. "touches upon the irrelevant"
3. "encroaches upon the recognized domains of privilege"³³⁰

Thus, outside the situations where privilege is proper, one is left with the first two, which are matters of a trial judge's discretion. Bad faith, for example, is never presumed and the party alleging it must establish it. One might also argue that discovery is precisely the time to gauge what are relevant and irrelevant, and having material produced does not equate to admissibility as evidence later at trial.

Cost of production, including the time needed by the opposing party or his personnel, is the single practical, concrete articulation of these first two grounds.³³¹ The party on defense is entitled to argue that "the burden or expense of the proposed discovery outweighs its likely benefit," taking into consideration factors such as the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake, and the importance of the discovery itself in resolving the issues.³³² The scope of the costs involved were vividly demonstrated in *In re Worldcom, Inc. Securities Litigation*, *Black v. United States*, and *Renda Marine v. United States*, but the actual use of cost as an objection to discovery was seen in *Rowe Entertainment v. William Morris Agency*, a case where black concert promoters claimed to be prejudiced by the booking practices of the defendant agencies.

Here, the William Morris Agency argued that retrieving its e-mail communications was technically impossible, or at least prohibitively expensive. First, backup copies prior to 1998 had been made with a program that was no longer commercially available, and an outside party hired to examine the data had in fact been unable to retrieve the e-mails. Second, a consultant estimated the cost of retrieving and processing the e-mails for 1998 and 1999 at almost ten *million* dollars. Third, it claimed its agents did not rely heavily on e-mail anyway; any e-mail deemed important at the time was printed out and filed, and its printed files had already been disclosed. Another agency, Monterey Peninsula Artists, Inc. estimated that 90% of its communications were done through telephone, fax, and other non-Internet modes. It further estimated that 50-70% of e-mails sent by it was to alert

³³⁰ *Hickman v. Taylor*, 329 U.S. 495, 500 (1947), *quoted in* *Republic v. Sandiganbayan*, G.R. No. 90478, Nov. 21, 1991.

³³¹ Meyer, *supra* note 19, at 952-53.

³³² *Heckman & Brydges*, *supra* note 7, at 156.

agents regarding received phone calls. Monterey added that the additional cost of reviewing retrieved e-mails for privilege would run to a quarter million dollars, at the rate of two e-mails per minute per paralegal, at USD150 per hour. The other two agencies involved made similar projections.³³³

Their arguments failed to convince the court as to relevance, since the figures indicated a significant volume of business communication done through e-mail. Further, it cited that about a third of electronic documents are never printed out, and the agencies never had a set policy regarding the retention of e-mails in their printed files.³³⁴ E-mails showing discriminatory attitudes were precisely those unlikely to be filed. What the court felt was more significant was the issue of allocating the cost burden, and it summarized a criteria for this:

- (1) the specificity of the discovery requests;
- (2) the likelihood of discovering critical information;
- (3) the availability of such information from other sources;
- (4) the purposes for which the responding party maintains the requested data;
- (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production;
- (7) the relative ability of each party to control costs and its incentive to do so; and
- (8) the resources available to each party.³³⁵

After a comprehensive explanation of each point and review of the facts related to each, the court granted discovery to the extent that the

³³³ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 424-26 (S.D.N.Y. 2002).

³³⁴ *Id.* at 428, citing Corinne Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L.REV. 257, 259 (2000).

³³⁵ *Rowe Entertainment*, 205 F.R.D. at 429.

requesting party would bear the cost.³³⁶ Again, the court noted that the costs involved were not limited to the fees of computer consultants, but included less tangible ones such as the employee time diverted from regular business and the risk of inadvertently disclosing privileged information.³³⁷ *Rowe*, finally, is also important for its repudiation of an earlier line of thinking, which holds that such costs of production should be borne by the producing party, because they are "an ordinary and foreseeable risk" in storing documents electronically,³³⁸ following the earlier *McPeck v. Ashcroft*.³³⁹ However, *Rowe* also emphasized that the requesting party should not bear the costs in every case, either, since these are traditionally borne by the producing party, and it would be inequitable to poor litigants.³⁴⁰

If the costs are not as dramatic as those involved in such large-scale commercial litigation, then one is left to argue irrelevance or bad faith, as in

³³⁶ *Id.* at 433. A party seeking to use the cost argument against electronic discovery is well advised to begin its research with a review of *Rowe*. The lengthy eight-point discussion was reproduced verbatim in the PHILIPPINE LAW JOURNAL. Vistan, *supra* note 12, at 81-87.

³³⁷ *Id.* at 432. See Richard Agins, Comment, *An Argument for Expanding the Application of Rule 53(B) to Facilitate Reference of the Special Master in Electronic Data Discovery*, 23 PACE L. REV. 689 (2003); Robins, *Evidence at the Electronic Frontier*, *supra* note 19, at 232-33.

³³⁸ *Id.* at 429, quoting *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526, at *2 (N.D. Ill. 1995). "But even if this principle is unassailable in the context of paper records, it does not translate well into the realm of electronic data. The underlying assumption is that the party retaining information does so because that information is useful to it, as demonstrated by the fact that it is willing to bear the costs of retention. That party may therefore be expected to locate specific data, whether for its own needs or in response to a discovery request. With electronic media, however, the syllogism breaks down because the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it. And, even if data is retained for limited purposes, it is not necessarily amenable to discovery. Back-up tapes, for example, are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. Therefore, the organization of the data mirrors the computer's structure, not the human records management structure, if there is one." See *Daewoo Electronics Co. v. United States*, 650 F.Supp. 1003, 1006 (CIT 1986).

³³⁹ *McPeck v. Ashcroft*, 202 F.R.D. 31, 32 (D.D.C. 2001), quoted in *Rowe Entertainment*, 205 F.R.D. at 429. "The purpose of having a backup system and retaining the tapes was to permit recovery from a disaster, not archival preservation." See Withers, *supra* note 9, at 1085 (2001).

³⁴⁰ *Rowe Entertainment*, 205 F.R.D. at 429, citing Marnie Pulver, *Electronic Media Discovery: The Economic Benefit of Pay-Per-View*, 21 CARDOZO L.REV. 1379, 1424 (2000).

traditional discovery contests.³⁴¹ Even then and aside from the large discretion involved in weighing these, there are arguments unique to electronic evidence that expand the concept of relevance. For example, a party may request the original electronic storage device in an attempt to establish alteration or manipulation and impeach the paper records produced.³⁴² A court will likely allow this ground if the request is not particularly intrusive or burdensome.³⁴³ Another allowable angle is the reconstruction of files from the original hard drive or electronic storage device, especially if one alleges that the opposing party has been withholding or erasing documents. The landmark case *Playboy Enterprises, Inc. v. Welles*³⁴⁴ featured a court order for the reproduction of a "mirror image" of a party's entire hard drive precisely due to such allegations.³⁴⁵ *Playboy* also illustrated a third expansive ground, since the plaintiff sought e-mails that would show the defendant's state of mind. The case involved former "Playmate of the Year" Teri Welles' claim of emotional distress amidst Playboy Enterprises' trademark infringement suit against her.

Again, however, against the breadth of electronic discovery, there are very few concrete remedies, and one's protection relies mainly by the judge's discretion. To concretize these deficiencies on a less abstract, more human level, one might examine cases of electronic evidence that do not involve thousands of documents and large corporations. First, the New Jersey Supreme Court's *State v. Evers*³⁴⁶ described the electronic trail that led to William Evers' conviction for possession and transmission of child pornography over the Internet. The married, middle-class man with no criminal record opened a second Internet account for browsing child pornography websites. In 1999, in the chat room "NOxHAIRxYET," he transmitted images of a naked female child to fifty-one other users, one of whom was a California sheriff. Police obtained the account's billing information and traced it to Evers' wife. They seized the family computer's

³⁴¹ Meyer, *supra* note 19, at 951-52.

³⁴² Heckman & Brydges, *supra* note 7, at 158, citing *Williams v. Owens-Corning Illinois*, 665 F. 2d 918, 932-33 (9th Cir. 1982); *Fennell v. First Step Designs, Ltd.*, 83 F. 3d 526, 529 (1st Cir. 1996); *Momah v. Albert Einstein Medical Center*, 164 F.R.D. 412, 419. See Chris William Sanchirico, *Evidence Tampering*, 53 DUKE L.J. 1215, 1217, 1236 (2004).

³⁴³ Heckman & Brydges, *supra* note 7, at 159, citing Robins, *Computers and the Discovery of Evidence*, *supra* note 43, at 443.

³⁴⁴ 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

³⁴⁵ *Id.* at 1054-55.

³⁴⁶ 815 A.2d 432 (N.J. 2003).

hard drive and arrested Evers, who confessed on the spot.³⁴⁷ The Court commented:

[D]efendant readily admitted that he distributed the offending photographs for the express purpose of encouraging the recipients to reciprocate by sending him more child pornography in return. That is exactly the type of trafficking the Legislature meant to shut down in order to stop the demand for and perpetuation of the sexual exploitation of children. Defendant's so-called "bit player" role in the child pornography industry nevertheless brought him within the sweep of the second-degree crime of distribution and does not dispel the notion that his imprisonment would deter others from, in the trial judge's words, "perpetuat[ing] the growing market for... cyber-porn" by soliciting and disseminating child pornography.³⁴⁸

Second, the New York decision *People v. Jovanovic*³⁴⁹ dealt with discovery in a rape case. The defendant was indicted for kidnapping, aggravated sexual abuse, and sodomy, and subpoenaed all e-mails sent and received by the victim from her Columbia University account, which amounted to over 2,400 pages.³⁵⁰ The court conducted an *in camera* examination of the material, and released e-mail between the victim and the defendant, and two others with the name of the third party redacted. It ruled that the other e-mails would have no bearing on the case.³⁵¹ The court noted:

The Court can only conclude that the defendant's subpoena of the complainant's third party e-mails from Columbia University constitutes nothing more than a "discovery" subpoena – a fishing expedition to attempt to examine the e-mails in the hope that evidence or information helpful to the defense will be discovered, i.e., presumably information regarding the complainant's sexual history and/or proclivities. This is clearly an improper use of a *subpoena duces tecum*.³⁵²

Both cases demonstrate the use of electronic evidence, but *Jovanovic* is possibly the most atrocious fishing expedition seen in recent jurisprudence. Can a rape victim theoretically be subject to the indignity of

³⁴⁷ *Id.* at 437-38.

³⁴⁸ *Id.* at 458.

³⁴⁹ 676 N.Y.S.2d 392 (N.Y. 1997).

³⁵⁰ *Id.* at 392-93.

³⁵¹ *Id.* at 393, 396.

³⁵² *Id.* at 395.

having all her personal communications opened to the perusal by the accused before the trial? Apparently, yes, examining the decision.

First, no privilege could be asserted. The victim's e-mails were not confidential, and did not involve legal advice or mental impressions regarding legal strategies. Second, cost was not an issue. Columbia University readily produced diskettes containing the e-mails and forwarded these to the court. Third, although the court found impropriety and made no attempt to hide its disapproval of the discovery motion, one infers it did not find bad faith since it did not disallow the request altogether. In fact, the decision elaborated further and eventually restricted the production due to relevance, but even then it disclosed two e-mails between the victim and a third party.

Jovanovic ended:

The Court is also cognizant of the privacy rights of the complainant in the material subpoenaed, in light of the holding by the Court of Appeals in *People v. Williams*, 81 N.Y.2d 303... in which the Court of Appeals expressed the legitimate societal interest of affording protection to victims of alleged sexual crimes from unnecessary invasions of privacy and harassment. Communications between the complainant and third parties other than the defendant (which the Court has previously determined through its *in camera* review are not exculpatory) are not directly relevant to the defendant's case, since such have no bearing on the defendant's state of mind at the time the crime was allegedly committed.³⁵³

Thus, there is an additional implied standard, one that deals with discovery's degree of intrusion independent of cost and relevance. One wonders, however, if such a standard is applicable only in extreme cases, as in *Jovanovic* which was a rape case?

Eminent constitutionalist Fr. Joaquin Bernas, S.J. would say no; such a standard must apply. The Bill of Rights reads:

Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and *seizures of whatever nature and for any purpose* shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce,

³⁵³ *Id.*

and particularly describing the place to be searched and the persons or things to be seized. (emphasis added)³⁵⁴

Examining the wording in the 1987 Constitution, Fr. Bernas commented:

When it is realized that the power of the Supreme Court to issue rules of procedure is subject to the specific constitutional limitation that they shall not diminish substantive rights, it becomes clear that the application of Rule 27 must follow constitutional principles on search and seizure.³⁵⁵

Fr. Bernas, however, opines that the present Rule 27 nevertheless meets the minimum requirements of the right against unreasonable search as it requires probable cause and designation of the material sought.³⁵⁶ It would appear, then, that even the constitutional right referred to fails to furnish heightened protection in a *Jovanovic*.

However, the link to the right against unreasonable search also creates a link between Rule 27 and a more apt constitutional right: the right to privacy.

Privacy is gaining importance in cyberlaw today, and has been increasingly exalted in Constitutional Law. It is only beginning to receive attention, however, in Remedial Law. As one author noted, "Privacy is a condition that is much easier to violate, and thus, is much more difficult to establish and protect."³⁵⁷

VII. THE CONSTITUTIONAL RIGHT TO PRIVACY

This preliminary section discusses a more concrete framework for the right to privacy, one that has eluded Philippine academic discussion to date. Specifically, it first discusses what is called decisional privacy, which is the dominant concept in American jurisprudence and has close conceptual parallels to the work product privilege. It then discusses what is called informational privacy, which appears to be the dominant concept in

³⁵⁴ CONST. art. III, § 2.

³⁵⁵ JOAQUIN BERNAS, S.J., THE 1987 CONSTITUTION OF THE PHILIPPINES: A COMMENTARY 166 (1996).

³⁵⁶ *Id.* at 167.

³⁵⁷ Ronald Backes, *Freedom, Information, Security*, 10 SETON HALL CONST. L.J. 927 (2000), citing Thierry Olivier, *The Economic Espionage Act Of 1996: Are We Finally Taking Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 97-98 (1999).

Philippine jurisprudence and is the concept most conceptually relevant to discovery and evidence.

Individuals are granted the right to withhold information about themselves and build intangible walls to ward the public eye around personal information in the same way that what transpires inside the walls of one's home is generally regarded as private. More than this, however, it is submitted that individuals even have a right to relative anonymity, and that the State and discovery orders must respect this context of privacy.

A. DECISIONAL PRIVACY AND THE DUE PROCESS CLAUSE

The right to privacy, though not an explicit Constitutional right,³⁵⁸ is arguably the only one with a birthday. It made its debut through the landmark Warren-Brandeis article in Volume 4 of the *Harvard Law Review* in 1890.³⁵⁹ The original article, however, dealt with tort defenses a debutante might raise against overzealous paparazzi. The birth of the actual Constitutional right is less precisely marked, and there is arguably more than one date.

The landmark case *Whalen v. Roe*³⁶⁰ bifurcated the right to privacy into:

Decisional privacy: "the interest in independence in making certain kinds of important decisions"

Informational privacy: "the individual interest in avoiding disclosure of personal matters"³⁶¹

Later, after his appointment to the United States Supreme Court, Louis Brandeis's pen produced "the right to be let alone," that "most

³⁵⁸ *Roe v. Wade*, 410 U.S. 113, 152 (1973); *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, Jul. 23, 1998, *citing* *Griswold v. Connecticut*, 381 U.S. 479 (1965).

³⁵⁹ Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

³⁶⁰ *Whalen v. Roe*, 429 U.S. 589 (1977).

³⁶¹ *Id.* at 599-600, *citing* *Roe v. Wade*, 410 U.S. 113 (1973); *Doe v. Bolton*, 410 U.S. 179 (1973); *Loving v. Virginia*, 388 U.S. 1 (1967); *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Pierce v. Society of Sisters of the Holy Names of Jesus and Mary*, 268 U.S. 510 (1925); *Meyer v. Nebraska*, 262 U.S. 390 (1923); *Allgeyer v. Louisiana*, 165 U.S. 578 (1897).

comprehensive of rights and the right most valued by civilized men."³⁶² His famous dissent in *Olmstead*, however, does not frame the highest-profile line of American cases on privacy. Rather, these cases have carved an additional restraint on government authority into the Bill of Rights, one that arises from the Due Process Clause and specifically secures the liberty of an individual to make personal decisions without undue State interference.³⁶³

"Decisional privacy" arguably arose from a formidable line of decisions on sex,³⁶⁴ a sphere of conduct hardly as explicitly protected as speech and religion.³⁶⁵ The unwritten protection's first ramparts were raised in the 1920s, a period when the United States Supreme Court began reading substantive content into the Due Process Clause. *Meyer v. Nebraska*³⁶⁶ mapped out:

"No state ... shall deprive any person of life, liberty or property without due process of law."

While this court has not attempted to define with exactness the liberty thus guaranteed, the term has received much consideration and some of the included things have been definitely stated. Without doubt, it denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men.³⁶⁷

Applying this more holistic definition of liberty, *Meyer* struck down a law that forbade the use of non-English languages in schools, holding that it

³⁶² *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

³⁶³ *Whalen v. Roe*, 429 U.S. 589, 599 (1977).

³⁶⁴ "[A] right first explicitly recognized in an opinion holding unconstitutional a statute prohibiting the use of contraceptives, and most prominently vindicated in recent years in the contexts of contraception, and abortion." *Carey v. Population Services International*, 431 U.S. 678, 685 (1977).

³⁶⁵ Note, however, that while various constitutional protections parallel each other, the precise mechanisms of one may have no equivalent in another. See, e.g., *Lee v. Weisman*, 505 U.S. 577, 590 (1992). "Speech is protected by ensuring its full expression even when the government participates, for the very object of some of our most important speech is to persuade the government to adopt an idea as its own. The method for protecting freedom of worship and freedom of conscience in religious matters is quite the reverse."

³⁶⁶ 262 U.S. 390 (1923).

³⁶⁷ *Id.* at 399.

infringed on parents' liberty to direct their children's education, and in a way that inspired the Court to allude to the confinement of Spartan children in barracks.³⁶⁸ That same decade, *Pierce v. Society of Sisters*³⁶⁹ upheld the same Due Process right in striking down a requirement that all children attend only public schools.³⁷⁰

The word "privacy" was first explicitly used in *Griswold v. Connecticut*,³⁷¹ which described "a privacy older than the Bill of Rights."³⁷²

[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. (internal citation omitted)³⁷³

The Court, backpedaling from the stigma of *Lochner v. New York*³⁷⁴ and the "treacherous field"³⁷⁵ of substantive due process, declined to apply the Due Process Clause,³⁷⁶ and instead found penumbras of privacy in the

³⁶⁸ *Id.* at 400-03. "In order to submerge the individual and develop ideal citizens, Sparta assembled the males at seven into barracks and intrusted their subsequent education and training to official guardians. Although such measures have been deliberately approved by men of great genius their ideas touching the relation between individual and state were wholly different from those upon which our institutions rest; and it hardly will be affirmed that any Legislature could impose such restrictions upon the people of a state without doing violence to both letter and spirit of the Constitution." *Id.* at 403.

³⁶⁹ *Pierce v. Society of the Sisters of the Holy Name of Jesus and Mary*, 264 U.S. 510 (1925).

³⁷⁰ *Id.* at 534-35.

³⁷¹ 381 U.S. 479 (1965).

³⁷² *Id.* at 486.

³⁷³ *Id.* at 484.

³⁷⁴ 198 U.S. 45 (1905).

³⁷⁵ *Moore v. East Cleveland*, 431 U.S. 494, 502 (1977). "Substantive due process has at times been a treacherous field for this Court. There are risks when the judicial branch gives enhanced protection to certain substantive liberties without the guidance of the more specific provisions of the Bill of Rights. As the history of the *Lochner* era demonstrates, there is reason for concern lest the only limits to such judicial intervention become the predilections of those who happen at the time to be Members of this Court. That history counsels caution and restraint. But it does not counsel abandonment...."

³⁷⁶ *Griswold*, 381 U.S. at 481-82. "Coming to the merits, we are met with a wide range of questions that implicate the Due Process Clause of the Fourteenth Amendment. Overtones of some arguments suggest that *Lochner v. New York*, 198 U.S. 45, should be our guide. But we decline that invitation as we did in *West Coast Hotel Co. v. Parrish*, 300 U.S. 379; *Olsen v. Nebraska*, 313 U.S. 236; *Lincoln Union v. Northwestern Co.*,

freedom of speech, freedom of association, right against unreasonable search, right against self-incrimination, and the Ninth Amendment that reserved certain unenumerated rights to the people.³⁷⁷ Thus, *Griswold* struck down a statute that forbade the use of contraceptives by married couples:

Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.³⁷⁸

Despite this doctrinal *volte face*, two years later, *Loving v. Virginia*³⁷⁹ struck down a statute that forbade interracial marriage, this time on Due Process grounds:

The freedom to marry has long been recognized as one of the vital personal rights essential to the orderly pursuit of happiness by free men.

...To deny this fundamental freedom on so unsupportable a basis as the racial classifications embodied in these statutes... is surely to deprive all the State's citizens of liberty without due process of law.³⁸⁰

Six years after *Griswold*, *Boddie v. Connecticut*³⁸¹ ruled that Due Process prohibited a State from denying divorce proceedings to poor people, as these were an "exclusive precondition to the adjustment of a fundamental human relationship."³⁸² Twelve years after *Griswold*, *Moore v. East Cleveland*³⁸³ struck down a statute that limited occupation of houses to single "families" as it defined families, holding that Due Process protected "a private realm of family life which the State cannot enter."³⁸⁴ Finally, *Zablocki v. Redhail*³⁸⁵ cited *Griswold* as establishing that "the right to marry is part of the fundamental

335 U.S. 525; *Williamson v. Lee Optical Co.*, 348 U.S. 483; *Giboney v. Empire Storage Co.*, 336 U.S. 490. We do not sit as a super-legislature to determine the wisdom, need, and propriety of laws that touch economic problems, business affairs, or social conditions. This law, however, operates directly on an intimate relation of husband and wife and their physician's role in one aspect of that relation."

³⁷⁷ *Id.* at 484.

³⁷⁸ *Id.* at 485-86.

³⁷⁹ 388 U.S. 1 (1967).

³⁸⁰ *Id.* at 12.

³⁸¹ 401 U.S. 371 (1971).

³⁸² *Id.* at 382-83.

³⁸³ 431 U.S. 494 (1977).

³⁸⁴ *Id.* at 499.

³⁸⁵ 434 U.S. 374 (1978).

'right of privacy' implicit in the Fourteenth Amendment's Due Process Clause."³⁸⁶

In the rough decade after *Griswold*, only *Eisenstadt v. Baird*³⁸⁷ and its extension of the *Griswold* ruling on contraceptives to unmarried couples was explicitly founded on privacy and penumbras. Nevertheless, the language of *Eisenstadt* was precisely that of the decisional privacy later described in *Whalen v. Roe*.³⁸⁸

It is true that in *Griswold* the right of privacy in question inhered in the marital relationship. Yet the marital couple is not an independent entity... If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person.... (emphasis added)³⁸⁹

Moreover, the dissent precisely decried how the majority "hark back to the heyday of substantive due process."³⁹⁰

A year after *Eisenstadt*, however, the right to privacy and its spurned lover, *Meyer's* substantive due process, were reconciled in *Roe v. Wade*, which ruled:

This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.³⁹¹

³⁸⁶ *Id.* at 384.

³⁸⁷ 405 U.S. 438 (1972).

³⁸⁸ 429 U.S. 589, 599 (1977).

³⁸⁹ *Eisenstadt*, 405 U.S. at 453. See *Planned Parenthood of Southern Pa. v. Casey*, 505 U.S. 833, 897 (1992). "There was a time, not so long ago, when a different understanding of the family and of the Constitution prevailed. In *Bradwell v. State*, 16 Wall. 130 (1873), three Members of this Court reaffirmed the common law principle that a woman had no legal existence separate from her husband...."

³⁹⁰ *Eisenstadt*, 405 U.S. at 467 (Burger, C.J., *dissenting*). "[T]hese opinions seriously invade the constitutional prerogatives of the States and regrettably hark back to the heyday of substantive due process."

³⁹¹ *Roe v. Wade*, 410 U.S. 113, 153 (1973).

Citing *Whalen, Carey v. Population Services*³⁹² upheld the rationale of *Roe v. Wade*:

The decision whether or not to beget or bear a child is at the very heart of this cluster of constitutionally protected choices. That decision holds a particularly important place in the history of the right of privacy.... (internal citations omitted)³⁹³

Roe v. Wade was upheld all the way into the last decade, and was most emphatically reiterated in *Planned Parenthood v. Casey*,³⁹⁴ with only modification to its original trimester framework, which the Court deemed nonessential to *Roe v. Wade*'s central holding. *Planned Parenthood* underscored:

The woman's right to terminate her pregnancy before viability is the most central principle of *Roe v. Wade*. It is a rule of law and a component of liberty we cannot renounce.³⁹⁵

Finally, *Lawrence v. Texas*³⁹⁶ reiterated *Eisenstadt*'s emphasis on how privacy inheres in an individual, and extended the aegis of decisional privacy from childbirth, sexual intimacy, contraception and abortion to homosexual relationships:

The case does involve two adults... The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government.³⁹⁷

³⁹² 431 U.S. 678 (1977).

³⁹³ *Id.* at 685.

³⁹⁴ 505 U.S. 833.

³⁹⁵ *Id.* at 871. "The Court's duty in the present case is clear. In 1973, it confronted the already-divisive issue of governmental power to limit personal choice to undergo abortion, for which it provided a new resolution based on the due process guaranteed by the Fourteenth Amendment. Whether or not a new social consensus is developing on that issue, its divisiveness is no less today than in 1973, and pressure to overrule the decision, like pressure to retain it, has grown only more intense. A decision to overrule *Roe*'s essential holding under the existing circumstances would address error, if error there was, at the cost of both profound and unnecessary damage to the Court's legitimacy, and to the Nation's commitment to the rule of law." *Id.* at 868-869.

³⁹⁶ 539 U.S. 558 (2003)

³⁹⁷ *Id.* at 578. See Amicus Curiae Brief of Rights International in *X, Y and Z v. United Kingdom*, *The National Journal of Sexual Orientation Law*, at <http://www.ibiblio.org/gaylaw/issue5/transbre.html> (last visited Feb. 28, 2004). "[T]he right to privacy under Article 8 of the European Convention has been interpreted

This thought has found even broader application in England, which upheld transsexuals' right to marriage in 2003, although it did not explicitly use the word privacy:

Marriage is an institution, or relationship, deeply embedded in the religious and social culture of this country. ... There was a time when the reproductive functions of male and female were regarded as the primary *raison d'être* of marriage. ... For a long time now the emphasis has been different. Various expressed, there is much more emphasis now on the 'mutual society, help and comfort that the one ought to have of the other'.

Against this background there are those who urge that the special relationship of marriage should not now be confined to persons of the opposite sex. It should be possible for persons of the same sex to marry.³⁹⁸

A *Harvard Law Review* article quipped that decisional privacy "has little to do with privacy and nothing to do with the Constitution."³⁹⁹ It continued:

The right to privacy has everything to do with delineating the legitimate limits of governmental power. The right to privacy, like the natural law and substantive due process doctrines for which it is a late-blooming substitute, supposes that the very order of things in a free society may on certain occasions render intolerable a law that violates no express constitutional guarantee.⁴⁰⁰

Thus, one concludes that decisional privacy is a necessary or even implied outgrowth of Due Process that restrains government from intruding into certain personal decisions deemed fundamental in human experience, and not just those pertaining to sex, sexuality, and family life.

This brand of restraint has not been found in the short line of Philippine privacy jurisprudence, however. Indeed, a dramatic arrest of State

repeatedly by the European Court of Human Rights to extend to an adult's right to participate in private, consensual homosexual activity. See *Dudgeon v. United Kingdom*, 45 Eur. Ct. H.R. (ser. A) (1981) (protection extended to mutual masturbation, oral-genital contact, and anal intercourse between adult men); *Norris v. Ireland*, 142 Eur. Ct. H.R. (ser. A) (1988) (protection extended to anal intercourse between adult men); *Modinos v. Cyprus*, 259 Eur. Ct. H.R. (ser. A) (1993) (protection extended to carnal knowledge "against the order of nature").

³⁹⁸ *Bellinger v. Bellinger*, 2003 UKHL 21, ¶ 46-47.

³⁹⁹ *Jeb Rubinfeld, The Right to Privacy*, 102 HARV. L. REV. 737, 737 (1989).

⁴⁰⁰ *Id.*

action came in *Ople v. Torres*,⁴⁰¹ but this struck down a National ID system and no actual decisionmaking was directly restricted by it. This is possibly because the Philippine Court has not had an opportunity to pass on the kind of decisional privacy issues in the high-profile line of *Roe v. Wade* and *Lawrence*. However, in September 2004, *Duncan Ass'n of Detailman-PTGWO v. Glaxo Wellcome Philippines, Inc.*⁴⁰² upheld a company's right to prohibit an employee from having personal or marital relationships with a competitor's employee, over that employee's fundamental right to marry. The case has obvious parallels with Due Process and privacy cases such as *Loving v. Virginia*. On the other hand, this case involved a private employer's and not a government policy, and ruled that the prohibition was a valid management prerogative.⁴⁰³

The omission of decisional privacy from Philippine jurisprudence may be because *Roe v. Wade* is the line's most prominent case. Although its holding does not appear contrary to Philippine thinking since one can consider that the latter places a much higher premium on state interest with respect to the unborn, its result is an apparent constitutional taboo, that a jurist would prefer not to cite it in order to avoid misimpressions.

For whatever reason, then, although the Philippine Court traces its privacy rulings to American jurisprudence, the Philippine jurisprudential trail emphasizes another line of thought, one closer to Justice Brandeis. Because of this very different emphasis, the Philippine Court has come to emphasize not Due Process, but *Griswold* and its penumbras, an approach more apt to the issues of information disclosure it has so far discussed.

Any lawyer, however, should immediately recognize decisional privacy and its ready application in the Philippines. Aside from the fact that decisional privacy arises from Due Process, one notes the rationale of the attorney-client privilege:

⁴⁰¹ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, Jul. 23, 1998.

⁴⁰² G.R. No. 162994, Sep. 17, 2004. See Philip Tubeza, *High court 'rules' vs love*, PHIL. DAILY INQUIRER, Sep. 22, 2004, at A1.

⁴⁰³ See, however, Raul Pangalangan, *Passion for Reason: High court frowns upon Romeo and Juliet romances*, PHIL. DAILY INQUIRER, Sep. 24, 2004, at A14. "There are many ways to satisfy state action. It would have been easier here because the Constitution requires the state to respect the 'sanctity of family life' as the 'foundation of the nation,' etc. In light of this affirmative command, the Court's inaction is the state action. By tolerating intolerance, the Court becomes a willing accomplice."

In order to promote freedom of consultation of legal advisors by clients, the apprehension of compelled disclosure from the legal advisors must be removed.⁴⁰⁴

Similarly, *Hickman* explained the work product privilege:

In performing his various duties, however, it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference.⁴⁰⁵

This is precisely the language of decisional privacy, removed from its familiar context of sex and marriage.

B. THE PENUMBRAS AND INFORMATIONAL PRIVACY

The right to privacy was indubitably recognized in Philippine jurisprudence by *Morfe v. Mutuc*.⁴⁰⁶

The constitutional right to privacy has come into its own.

So it is likewise in our jurisdiction. The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection.⁴⁰⁷

Justice Enrique Fernando, writing *Morfe*, deemed the right to privacy so important that, "The right to be let alone is indeed the beginning of all freedom."⁴⁰⁸ Further, although leading Philippine cases such as *Morfe* and *Ople* quote *Griswold's* discussion on how privacy arises from certain fundamental rights, *Ople* went a step further and explicitly declared privacy itself a fundamental right:

[W]e prescind from the premise that the right to privacy is a *fundamental right* guaranteed by the Constitution, hence, it is the burden of government to show that A.O. No. 308 is justified by

⁴⁰⁴ 8 WIGMORE, *supra* note 66, at 545, § 2291, *quoted in* Regala v. Sandiganbayan, G.R. No. 105938, Sep. 20, 1996.

⁴⁰⁵ *Hickman v. Taylor*, 329 U.S. 495, 510-11 (1947).

⁴⁰⁶ G.R. No. 20387, 22 SCRA 424, Jan. 31, 1968.

⁴⁰⁷ *Id.* at 444.

⁴⁰⁸ *Id.* at 442, *quoting* Public Utilities Commission v. Pollak, 343 U. S. 451, 467 (1952) (Douglas, J., *dissenting*).

some compelling state interest and that it is narrowly drawn.
(emphasis added)⁴⁰⁹

Philippine cases, however, have not explicitly defined what privacy is, though they have discussed its scope. *Morfe* initially seemed to imply that the Philippine right to privacy is the decisional privacy of *Roe v. Wade* and *Lawrence*:

"The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen." This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state.⁴¹⁰

As discussed, however, Philippine jurisprudence never primarily shielded decisionmaking, and *Morfe*'s next sentences read:

In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector – protection, in other words, of the dignity and integrity of the individual – has become increasingly important as modern society has developed. All the forces of a technological age – industrialization, urbanization, and organization – operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society.⁴¹¹

This emphasis, instead, on dignity and a personal zone of seclusion was most emphatically reiterated by Justice Florida Ruth Romero in *Ople*:

What marks off man from a beast?

...Because of his sensibilities, emotions and feelings, he likewise possesses a sense of shame. In varying degrees as dictated by diverse cultures, he erects a wall between himself and the outside world wherein he can retreat in solitude, protecting himself from prying

⁴⁰⁹ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, Jul. 23, 1998.

⁴¹⁰ *Morfe*, 22 SCRA at 455, *quoted in Ople*, 293 SCRA at 155.

⁴¹¹ *Morfe*, 22 SCRA at 445, *quoted in Ople*, 293 SCRA at 155-156.

eyes and ears and their extensions, whether from individuals, or much later, from authoritarian intrusions.⁴¹²

Seemingly underscoring this personal zone, Justice Vicente Mendoza felt that the ID system taken up by *Ople* intruded not into privacy, but into freedom of thought and of conscience.⁴¹³

Again, *Whalen v. Roe* recognized two aspects of privacy:

The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.⁴¹⁴

The first, informational privacy, is the concept that has been emphasized in Philippine jurisprudence, and precisely the facet of the right to privacy that is becoming increasingly relevant in the Information Age. As Justice Reynato Puno ended the *Ople* decision:

The right to privacy is one of the most threatened rights of man living in a mass society... In the case at bar, the threat comes from the executive branch of government which by issuing A.O. No. 308 pressures the people to surrender their privacy by giving information about themselves on the pretext that it will facilitate delivery of basic services.⁴¹⁵

The right to informational privacy arises from the penumbras, and itself has two aspects: 1) the right of an individual not to have private information about himself disclosed; and 2) the right of an individual to live freely without surveillance and intrusion.⁴¹⁶ It must be emphasized that the latter protects against the very act of piercing Justice Romero's "retreat in solitude," *regardless of whether any information is actually disclosed.*

⁴¹² *Ople*, 239 SCRA at 171 (Romero, J., *concurring*). See *Fisher v. United States*, 425 U.S. 391, 416 (1976) (Brennan, J., *concurring in the result*), quoting *Murphy v. Waterfront Commission*, 378 U.S. 52, 55 (1964). "The privilege reflects 'our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'"

⁴¹³ *Ople*, 239 SCRA at 152 (Mendoza, J., *dissenting*).

⁴¹⁴ *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977).

⁴¹⁵ *Ople*, 239 SCRA at 170.

⁴¹⁶ *Whalen*, 429 U.S. at 599, n.24.

Because actual disclosure is not necessarily the operative violation against this aspect of privacy, the right in this sense becomes not one against disclosure, but one to peace of mind, analogous to that in Article 26 of the Civil Code.⁴¹⁷ It also follows from Justice Irene Cortes's concept of privacy:

Though a component part of the greater society in which he lives, the individual must of necessity reserve certain areas of his life to himself. To preserve his own identity, he has to maintain an inner self, safeguard his beliefs, and keep hidden certain thoughts, judgments and desires.⁴¹⁸

Further, Justice Cortes also wrote that man's moral nature is linked with a sense of privacy.⁴¹⁹

C. INFORMATIONAL PRIVACY AND THE RIGHT AGAINST UNREASONABLE SEARCH

Griswold was the first case to explicitly recognize the right to privacy, and it was the seeming crossroads of privacy doctrines before *Whalen*, where Due Process discussion met a summary of the penumbras privacy emerged from. *Morfe* first outlined the right to privacy by quoting *Griswold*:

Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in

⁴¹⁷ Antonio Carpio, *Intentional Torts in Philippine Law*, 47 PHIL. L.J. 650, 687-690 (1972); *Tenchavez v. Escano*, G.R. No. 19671, 17 SCRA 684, Jul. 26, 1966. CIVIL CODE, art. 26. "Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

- (1) Prying into the privacy of another's residence;
- (2) Meddling with or disturbing the private life or family relations of another;
- (3) Intriguing to cause another to be alienated from his friends;
- (4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition."

⁴¹⁸ IRENE CORTES, *THE CONSTITUTIONAL FOUNDATIONS OF PRIVACY* 1 (1970). This paper was adapted from the second lecture of the Albino Z. SyCip Lecture Series, delivered at the University of the Philippines College of Law on February 21 and 28, 1970.

⁴¹⁹ *Id.* at 3.

their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."⁴²⁰

*Lagunzad v. Vda. de Gonzales*⁴²¹ discussed a "right to privacy" without citing *Morfe*, and balanced it against the freedom of speech.⁴²² Continuing the *Morfe* line, *Ayer Productions, Ltd. v. Capulong*⁴²³ took *Morfe's* explicit recognition of privacy, but cautioned:

It was demonstrated sometime ago by the then Dean Irene R. Cortes that our law, constitutional and statutory, does include a right of privacy. It is left to case law, however, to mark out the precise scope and content of this right in differing types of particular situations.⁴²⁴

Later, *Ople* made its own Philippine constitutional accounting:

Sec. 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.

Sec. 2. The right of the people to be secure in their persons, houses papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Sec. 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

Sec. 6. The liberty of abode and of changing the same within the limits prescribed by law shall not be impaired except upon lawful

⁴²⁰ *Morfe v. Mutuc*, G.R. No. 20387, 822 SCRA 424, 444, Jan 31, 1960.

⁴²¹ G.R. No. 32066, 92 SCRA 476, Aug. 6, 1979.

⁴²² *Id.* at 488-89.

⁴²³ G.R. Nos. 82380, 160 SCRA 861, Apr. 22, 1988. *Lagunzad* and *Ayer* both discussed the balance between privacy and freedom of speech in the context of movies depicting public figures.

⁴²⁴ *Id.* at 870.

order of the court. Neither shall the right to travel be impaired except in the interest of national security, public safety, or public health as may be provided by law.

Sec. 8. The right of the people, including those employed in the public and private sectors, to form unions, associations, or societies for purposes not contrary to law shall not be abridged.

Sec. 17. No person shall be compelled to be a witness against himself.⁴²⁵

Ople further examined Philippine law from a broader perspective:

Zones of privacy are likewise recognized and protected in our laws. The Civil Code provides that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons" and punishes as actionable torts several acts by a person of meddling and prying into the privacy of another. It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another person, and recognizes the privacy of letters and other private communications. The Revised Penal Code makes a crime the violation of secrets by an officer, the revelation of trade and industrial secrets, and trespass to dwelling. Invasion of privacy is an offense in special laws like the Anti-Wiretapping Law, the Secrecy of Bank Deposits Act and the Intellectual Property Code. The Rules of Court on privileged communication likewise recognize the privacy of certain information.⁴²⁶

At its very inception, the right to privacy was already criticized as a "broad, abstract and ambiguous concept... [that can] easily be interpreted as a constitutional ban against many things."⁴²⁷ Thus, the Philippine conception of privacy is concretized by backtracking through *Ople's* parallel penumbras. One begins with the right to privacy's immortal articulation by Justice Brandeis himself in *Olmstead*:

The makers of our Constitution... recognized the significance of man's spiritual nature, of his feelings and of his intellect... They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual... must be deemed a

⁴²⁵ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, 156, Jul. 23, 1998, *quoting* CONST. art. III.

⁴²⁶ *Ople*, 239 SCRA at 157, Jul. 23, 1998.

⁴²⁷ *Griswold v. Connecticut*, 381 U.S. 479, 509 (1965) (Black, J., dissenting).

violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

...Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent.... The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding. (internal citations omitted)⁴²⁸

Gauging from *Griswold's* discussion,⁴²⁹ *Olmstead's* poetry, and the nature of informational privacy itself, the right's first set of roots are embedded in the bedrock of the right against unreasonable search and seizure. At the outset, however, it must be emphasized that this right is not identical to the right to privacy itself, as one key decision noted:

[T]he Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion.⁴³⁰

The right against unreasonable search arose from English law, as eloquently described by Lord Camden:

By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing, which is proved by every declaration in trespass where the defendant is called upon to answer for bruising the grass and even treading upon the soil. If he admits the fact, he is bound to

⁴²⁸ *Olmstead v. United States*, 277 US 438, 478-79 (1928) (Brandeis, J., *dissenting*), *quoted in* *Morfe v. Mutuc*, G.R. No. 20387, 22 SCRA 424, 442, Jan. 31, 1968; *Ople*, 239 SCRA at 153.

⁴²⁹ "The Fourth and Fifth Amendments were described in *Boyd v. United States* as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.' We recently referred in *Mapp v. Ohio*, to the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.'" *Griswold v. Connecticut*, 381 U.S. 479, 484-85 (1965).

⁴³⁰ *Katz v. United States*, 389 U.S. 347, 350-51 (1967); Orin Kerr, *The Fourth Amendment and New Technologies*, 102 MICH. L. REV. 801, 817-18, 838 (2004).

show, by way of justification, that some positive law has justified or excused him.⁴³¹

The constitutional right thus arose from property rights, but even the earliest property-centered images from Philippine jurisprudence reflected how the right against unreasonable search intertwines with the right to privacy:

[T]he humblest citizen or subject might shut the door of his humble cottage in the face of the monarch and defend his intrusion into that privacy which was regarded as sacred as any of the kingly prerogatives. The poorest and most humble citizen may bid defiance to all the powers of the state; the wind, the storm and the sunshine alike may enter through its weather-beaten parts, but the king may not enter against the owner's will.⁴³²

Searching for the Constitutional foundations of privacy, Justice Cortes pointed to the defining case *Boyd v. United States*.⁴³³ Quoting Lord Camden, Justice Joseph Bradley wrote:

The principles laid down in this opinion affect the very essence of constitutional liberty and security... It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property... Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment.⁴³⁴

An examination of jurisprudence in the PHILIPPINE LAW JOURNAL noted that Philippine search and seizure cases echoed this recognition of personal dignity, of Justice Romero's "sensibilities, emotions and feelings" and "sense of shame."⁴³⁵

It is hereby determined that the unreasonable search on the plaintiff's person and bag caused (sic) done recklessly and oppressively by the

⁴³¹ *Entick v Carrington and Three Other King's Messengers*, 19 How. St. Tr. 1029, quoted in *Boyd v. United States*, 116 U.S. 616, 627 (1886).

⁴³² *United States v. Arceo*, No. 1491, 3 Phil. 381, 384, Mar. 5, 1904.

⁴³³ CORTES, *supra* note 418, at 33.

⁴³⁴ *Boyd v. United States*, 116 U.S. 616, 630 (1886).

⁴³⁵ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, 171, Jul. 23, 1998, (Romero, J., concurring).

defendant, violated, impaired and undermined the plaintiff's liberty guaranteed by the Constitution, entitling her to moral and exemplary damages against the defendant. *The search has unduly subjected the plaintiff to intense humiliation and indignities and had consequently ridiculed and embarrassed publicly said plaintiff so gravely and immeasurably.*⁴³⁶ (emphasis added)

The constitutional protection of our people against unreasonable search and seizure is not merely a pleasing platitude. It vouchsafes our *right to privacy and dignity* against undesirable intrusions committed by any public officer or private individual.⁴³⁷ (emphasis added)

Landynski in his authoritative work (*Search and Seizure and the Supreme Court*, 1966) could fitly characterize this constitutional right as the embodiment of a 'spiritual concept: the belief that to value the privacy of home and person and to afford its constitutional protection against the long reach of government is *no less than to value human dignity*.... (internal citations omitted and emphasis added)⁴³⁸

Years after *Boyd*, the Court ruled in *Olmstead* that wiretapping by government agents did not violate the right against unreasonable search, because intercepting electronic telephone impulses involved no "seizure of his papers or his tangible material effects or an actual physical invasion of his house or curtilage" for the purpose of making a seizure;⁴³⁹ in short, no physical trespass beyond the constitutionally delineated boundaries. Justice Brandeis vehemently dissented:

Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping.⁴⁴⁰

⁴³⁶ *United States v. Reyes*, G.R. No. 79253, 219 SCRA 192, 201, Mar. 1, 1993, quoted in Oscar Franklin Tan, *Touch Me Not: Expanding Constitutional Frameworks to Challenge LTO-Required and Other Mandatory Drug Testing*, 76 PHIL. L.J. 618, 656 (2002).

⁴³⁷ *MHP Garments v. CA*, G.R. No. 86720, 236 SCRA 227, 229, Sept. 2, 1994, quoted in Tan, *supra* note 436, at 656.

⁴³⁸ *Villanueva v. Querubin*, G.R. No. 26177, 48 SCRA 345, 350, Dec. 27, 1972, quoted in *People v. Burgos*, G.R. No. 68955, Sept. 4, 1986; Tan, *supra* note 436, at 656.

⁴³⁹ *Olmstead v. United States*, 277 U.S. 438, 466 (1928).

⁴⁴⁰ *Id.* at 473-74 (Brandeis, J., *dissenting*).

His views proved too advanced for his day, but were eventually upheld in *Katz v. United States*.⁴⁴¹ Brushing aside the argument that the booth was made of transparent glass and thus not private, the Court noted "what he sought to exclude when he entered the booth was not the intruding eye — it was the uninvited ear."⁴⁴² It held:

[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.⁴⁴³

...

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.⁴⁴⁴

Justice John Marshall Harlan emphasized how the majority decision held that "electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment."⁴⁴⁵ Bringing the right to privacy to the fore, he articulated "people, not places" as:

[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.⁴⁴⁶

⁴⁴¹ 389 U.S. 347 (1967). However, *Katz* never explicitly cited the *Olmstead* dissent, though it did cite Brandeis's *Harvard Law Review* article. *Id.* at 350-51, cited in Kerr, *supra* note 430, at 817-18.

⁴⁴² *Katz*, 389 U.S. at 352, quoted in CORTES, *supra* note 418, at 43.

⁴⁴³ *Katz*, 389 U.S. at 351.

⁴⁴⁴ *Id.* at 359.

⁴⁴⁵ *Id.* at 360 (Harlan, J., concurring). Justice Harlan criticized *Olmstead* for "bad physics as well as bad law." *Id.* at 362.

⁴⁴⁶ *Id.* at 361. See Larry Downes, *Electronic Communications and the Plain View Exception: "More Bad Physics"*, 7 HARV. J.L. & TECH. 239 (1994).

The *Katz* test and its articulation of expectations of privacy was incorporated into *Ople*. Thus, Justice Harlan reasoned that a man expects privacy in his home, but not with respect to things he keeps in plain view or to conversations made in the open. Applying this to the facts in *Katz*, he argued that a man in a telephone booth does not ordinarily assume his call will be intercepted. *Ople* generalized this:

The factual circumstances of the case determines the reasonableness of the expectation. However, other factors, such as customs, physical surroundings and practices of a particular activity, may serve to create or diminish this expectation.⁴⁴⁷

Thus, it struck down the proposed national ID system, stating,

The measure of protection granted by the reasonable expectation diminishes as relevant technology becomes more widely accepted... A.O. No. 308 is so widely drawn that a minimum standard for a reasonable expectation of privacy, regardless of technology used, cannot be inferred from its provisions.⁴⁴⁸

The *Katz* test in *Ople* was later applied to an airport frisk in *People v. Johnson*⁴⁴⁹ that revealed packs of hidden drugs:

Persons may lose the protection of the search and seizure clause by exposure of their persons or property to the public in a manner reflecting a lack of subjective expectation of privacy, which expectation society is prepared to recognize as reasonable. Such recognition is implicit in airport security procedures... Should these procedures suggest the presence of suspicious objects, physical searches are conducted to determine what the objects are. There is little question that such searches are reasonable, given their minimal intrusiveness, the gravity of the safety interests involved, and the reduced privacy expectations associated with airline travel.⁴⁵⁰

Katz and *Johnson* were again explicitly upheld in the 2002 case *People v. Canton*, which involved a similar airport drug search.⁴⁵¹ Thus, taken together, *Katz*, *Ople*, *Johnson*, and *Canton* answer the question, "When does a search occur?" Even if a place is explicitly named in the Constitution such as a "house,"⁴⁵² it only occurs when "the individual manifested a subjective

⁴⁴⁷ G.R. No. 127685, 239 SCRA 143, 164, Jul. 23, 1998.

⁴⁴⁸ *Id.* at 164

⁴⁴⁹ G.R. No. 13881, 348 SCRA 526, Dec. 18, 2000.

⁴⁵⁰ *Id.* at 534.

⁴⁵¹ *People v. Canton*, G.R. No. 148825, 394 SCRA 478, Dec. 27, 2002.

⁴⁵² CONST. art. III, § 2.

expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable."⁴⁵³ The intrusion or search, as Dean Pacifico Agabin phrased, delves into one's "capacity to maintain aspects of one's life apart from public awareness" and "the control we have over information about ourselves,"⁴⁵⁴ which form the very core of informational privacy.

Various decisions have thus explored the levels of expectation in different "zones of privacy." For example, there is clearly a much decreased expectation in a general physical exam, while such is greatly increased in a comfort room.⁴⁵⁵ Moving vehicles are subject to a decreased expectation of privacy due to government regulation.⁴⁵⁶ The United States observed a "retreat from *Boyd*" since the 1980s, and a restricted interpretation of these interpretations. The school and the workplace, for example, were deemed to carry lesser expectations.⁴⁵⁷ *Florida v. Riley* ruled that there was no expectation of privacy violated when government authorities searching for marijuana plants flew over a greenhouse using a helicopter:

[H]elicopters are not bound by the lower limits of the navigable airspace allowed to other aircraft. Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more.⁴⁵⁸

Undisturbed in jurisprudence, however, is the "sanctity of privacy the law accords to the human abode,"⁴⁵⁹ "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."⁴⁶⁰ Finally, it is argued that the human body itself should enjoy the

⁴⁵³ *California v. Ciraolo*, 476 U. S. 207, 213 (1986).

⁴⁵⁴ Pacifico Agabin, *Integrating DNA Technology into the Judicial System*, available at http://www.supremecourt.gov/ph/CSJ/Dec_00/dna.htm (last visited Feb. 28, 2004).

⁴⁵⁵ Tan, *supra* note 436, at 681, 626.

⁴⁵⁶ *People v. Baula*, G.R. No. 132671, 344 SCRA 663, Nov. 15, 2000.

⁴⁵⁷ Solove, *supra* note 177, at 69, citing *New Jersey v. T.L.O.*, 469 U.S. 325 (1984); *O'Connor v. Ortega*, 480 U.S. 709 (1987).

⁴⁵⁸ *Florida v. Riley*, 488 U.S. 451 (1989).

⁴⁵⁹ *People v. Agoncillo*, G.R. No. 138983, 358 SCRA 178, May 23, 2001.

⁴⁶⁰ *Silverman v. United States*, 365 U.S. 505, 511 (1961). See *People v. Fabon*, G.R. No. 133226, 328 SCRA 302, Mar. 16, 2000; *People v. Sapinosa*, G.R. No. 122540, 328 SCRA 649, Mar. 22, 2000; *People vs. Paraiso*, G. R. No. 127840, 319 SCRA 422, Nov. 29, 1999; *Payton v. New York*, 445 U.S. 573, 601 (1980).

greatest expectation of privacy of all.⁴⁶¹ This is supported by the 1891 case *Union Pacific Railway Co. v. Botsford*⁴⁶² which held that forcing a female party in a civil action to submit to a surgical examination was an "indignity, an assault, and a trespass,"⁴⁶³ and the 1881 case *De May v. Roberts*, which considered it "shocking to our sense of right, justice and propriety" for a physician to allow a young man to witness his patient giving birth.⁴⁶⁴ Most compellingly, Justice Cortes wrote:

Surely the Constitution does not protect the individuals possessions — one's houses, papers and effects — more than the integrity of the human person.⁴⁶⁵

Most recently, the *Katz* test has been applied to evolving technological capabilities, to determine when a search is indeed a search. The recent decision *Kyllo v. United States*⁴⁶⁶ began by establishing that a visual inspection of a house's exterior cannot possibly be a search, even though *Katz* unbundled the definition from mindsets tied to property. However, it conceded that this is "not so simple" today:

[J]ust as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house — and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*.... Reversing that approach would leave the homeowner at the mercy of advancing technology — including imaging technology that could discern all human activity in the home.⁴⁶⁷

A four-point expanded *Katz* test is gleaned from *Kyllo*. This new test declares that a search takes place when:

- 1) Information is obtained through sense-enhancing technology.

⁴⁶¹ Tan, *supra* note 436, at 657-59, citing *Schmerber v. California*, 384 U.S. 757 (1967); *Guanzon v. de Villa*, G.R. No. 80508, Jan. 30, 1990. See, however, *Villafior v. Summers*, No. 16444, 41 Phil. 62, Sep. 8, 1920.

⁴⁶² 141 U.S. 250 (1891).

⁴⁶³ *Id.* at 252.

⁴⁶⁴ *De May v. Roberts*, 9 N.W. 146 (1881), cited in Solove, *supra* note 177, at 41.

⁴⁶⁵ CORTES, *supra* note 418, at 65. See, however, *Jacobsen v. United States*, 466 U.S. 109, 123 (1984).

⁴⁶⁶ 533 U.S. 27 (2001).

⁴⁶⁷ *Id.* at 33.

- 2) The information could not have been otherwise obtained without physical intrusion.
- 3) The intrusion is into a constitutionally protected area, following the *Katz* test.
- 4) The technology used is not in general public use.⁴⁶⁸

Arguing against its breadth, one author discussed the broad application of *Kyllo*:

Through enhanced technology such as electronic wiretaps and bugs, law enforcement agencies can listen to those with suspected terrorist ties. Rather than narcotics, dogs can be trained to locate bomb material. Trap and trace devices and pen registers can be used to capture source and addressee information for computer (e.g., e-mail) and telephone conversations. Other sense-enhancing devices "might detect the odor of deadly bacteria or chemicals for making a[n]... explosive."⁴⁶⁹

Reconciling *Kyllo* with precedents, another author concluded that *United States v. Knotts*⁴⁷⁰ arguably involved no violation when authorities placed a homing device on a defendant's car, because it remained in public roads and could have been observed without the device.⁴⁷¹ *Dow Chemical v. United States*⁴⁷² likewise involved no violation because authorities took aerial photographs with an expensive but commercially available mapmaking camera.⁴⁷³ Conversely, *United States v. Karo*⁴⁷⁴ found a violation because the homing device there was placed in a container that was tracked into a private home, which would normally not be open to surveillance. However, one also contends with doctrine on information already disclosed to third parties regardless of context, and *Smith v. Maryland*⁴⁷⁵ held that telephone users have no reasonable expectation of privacy over the lists of phone numbers they

⁴⁶⁸ *Id.* at 47.

⁴⁶⁹ Nicholas Heydt, Note, *The Fourth Amendment Heats Up: The Constitutionality of Thermal Imaging and Sense-Enhancing Technology - Kyllo v. United States*, 29 WM. MITCHELL L. REV. 981, 1009-10 (2003).

⁴⁷⁰ 460 U.S. 276 (1983).

⁴⁷¹ *Id.* at 282, cited in Kerr, *supra* note 430, at 832-33; Amanda Froh, Note, *Rethinking Canine Sniffs: The Impact of Kyllo v. United States*, 26 SEATTLE U. L. REV. 337, 343-44 (2002).

⁴⁷² 476 U.S. 227 (1986).

⁴⁷³ *Id.* at 238, cited in Froh, *supra* note 471, at 345.

⁴⁷⁴ 468 U.S. 705 (1984).

⁴⁷⁵ 442 U.S. 735 (1979).

have dialed as these necessarily have to be disclosed to the telephone company.⁴⁷⁶ It is readily argued, of course, that the sheer volume of e-mail makes it far more difficult to track a particular individual's usage.

Looking over the requisites, one argues that more informational privacy violations are now possible with the Internet, arguably a sense-enhancing technology, using more advanced programs and techniques the ordinary user is unaware of. One argues that the Internet demands that *Katz* be taken to its final logical point, to a disassociation of expectations of privacy from place and zone altogether, and onto information itself.⁴⁷⁷

Certainly, this was echoed in *Ople*:

[T]he threat comes from the executive branch of government which by issuing A.O. No. 308 pressures the people to surrender their privacy by giving information about themselves on the pretext that it will facilitate delivery of basic services. Given the record-keeping power of the computer, only the indifferent fail to perceive the danger that A.O. No. 308 gives the government the power to compile a devastating dossier against unsuspecting citizens. It is timely to take note of the well-worded warning of Kalvin, Jr., "the disturbing result could be that everyone will live burdened by an unerasable record of his past and his limitations. In a way, the threat is that because of its record-keeping, the society will have lost its benign capacity to forget."⁴⁷⁸

The same sentiments were voiced in the original case on such a subject, *Whalen*, which *Ople* cited:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files... The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative

⁴⁷⁶ *Id.* at 742.

⁴⁷⁷ David Philips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 21-22 (2003); William deVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 306-07 (2003). See, e.g., *United States v. Hambrick*, 55 F.Supp.2d 504, 508 (E.D. Va. 1999). "Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis."

⁴⁷⁸ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, 170, Jul. 23, 1998.

procedures, evidence a proper concern with, and protection of, the individual's interest in privacy.⁴⁷⁹

Ople distinguished its facts from *Whalen*:

[T]he statute was narrowly drawn and contained numerous safeguards against indiscriminate disclosure. The statute laid down the procedure and requirements for the gathering, storage and retrieval of the information. It enumerated who were authorized to access the data. It also prohibited public disclosure of the data by imposing penalties for its violation. In view of these safeguards, the infringement of the patients' right to privacy was justified by a valid exercise of police power. As we discussed above, A.O. No. 308 lacks these vital safeguards.⁴⁸⁰

Examining this evolution, one thus argues that the traditional sanctity of the home grounded in informational privacy must now be overlaid onto personal information regarding one's life as well.

Again, the concept of place and the bounds marked by the walls of one's home are increasingly irrelevant because, for example, many bits of information are scattered throughout stray e-mails. It is not so much that this information must be kept confidential because it is important in the ordinary sense the minute details of one's life are often trivial. It is simply that a man needs to be able to hide a part of his life from public view in order to maintain a sense of personal integrity.

D. INFORMATIONAL PRIVACY AND THE RIGHT AGAINST SELF-INCRIMINATION

The right against self-incrimination is not discussed in depth in an informational privacy context because the intrusions it involves are much narrower than the right against unreasonable search, although the two were discussed together in *Boyd*, *Griswold*, and the *Olmstead* dissent. It comes into play mainly when prosecution is involved, and has a concrete doctrinal framework to afford protection in this narrow sphere. The right, however, is important in that it also reiterates the sacrosanct zone surrounding a person and his inherent dignity. As Justice William Brennan wrote:

⁴⁷⁹ *Whalen v. Roe*, 429 US 589, 606 (1977).

⁴⁸⁰ *Ople*, 239 at 167.

I do not join the Court's opinion... [because it is] but another step in the denigration of privacy principles settled nearly 100 years ago in *Boyd v. United States*.

...
Expressions are legion in opinions of this Court that the protection of personal privacy is a central purpose of the privilege against compelled self-incrimination. "[I]t is the invasion of [a person's] indefeasible right of personal security, personal liberty and private property" that "constitutes the essence of the offence" that violates the privilege. The privilege reflects "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" "It respects a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation." "The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." (internal citations omitted)⁴⁸¹

This is borne out by the right's history:

The doctrine that one accused of crime cannot be compelled to testify against himself is predicated upon principles of humanity and civil liberty. The maxim *Nemo tenetur seipsum accusare* had its origin in the protests against the abuses and manifestly unjust methods of interrogating accused persons in the inquisitorial Court of the Star Chamber. It was erected as an additional barrier for the protection of the people against the exercise of arbitrary power....⁴⁸²

So deeply did the iniquities of the ancient system impress themselves upon the minds of the American colonists that the states, with one accord, made a denial of the right to question an accused person a part of their fundamental law....⁴⁸³

However, the crux of the right goes against coercion by the government against an accused to confess against his free will,⁴⁸⁴ not to the "wall between himself and the outside world wherein he can retreat in solitude."⁴⁸⁵ This was seen in *Villaflores v. Summers*,⁴⁸⁶ which held that forcing a

⁴⁸¹ *Fisher v. United States*, 425 U.S. 391, 414, 416 (1976) (Brennan, J., *dissenting*), *citing* *Boyd v. United States*, 116 U.S. 616 (1886); *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965); *Katz v. United States*, 389 U.S. 347, 350 n. 5 (1967).

⁴⁸² *People v. Buscato*, G.R. No. 40639, 74 SCRA 30, 48 (1976), Nov. 23, 1976

⁴⁸³ *Id.*, *quoting* *Bram v. United States*, 168 U.S. 42.

⁴⁸⁴ *People v. Bagasala*, G.R. No. 26182, 39 SCRA 326 (1971), May 31, 1971; *United States v. Holt*, 218 U.S. 245 (1910).

⁴⁸⁵ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, 171 (1998), Jul. 23, 1998, (Romero, J., *concurring*).

woman to submit to a pregnancy test did not violate the right, since there was no "physical or moral compulsion to extort communications from him."⁴⁸⁷ Nevertheless, Justice George Malcolm wrote:

Fully conscious that we are resolving a most extreme case in a sense, which on first impression is a shock to one's sensibilities, we must nevertheless enforce the constitutional provision....

It is a reasonable presumption that in an examination by reputable and disinterested physicians due care will be taken not to use violence and not to embarrass the patient any more than is absolutely necessary. Indeed, no objection to the physical examination being made by the family doctor of the accused or by doctor of the same sex can be seen.⁴⁸⁸

E. INFORMATIONAL PRIVACY AND THE FREEDOMS OF SPEECH, OF ASSOCIATION AND OF ANONYMITY

At first blush, the rights to freedom of speech and association appear to have nothing to do with privacy. Examining the underpinnings of liberty, however, it becomes clear that they have everything to do with it. John Stuart Mill wrote that the pursuit of happiness necessarily involves the freedom of thought, "Over himself, over his own body and mind, the individual is supreme."⁴⁸⁹ His was a vision of the progressive enlightened development of a society,⁴⁹⁰ driven by the communication of thoughts of a social nature,⁴⁹¹ and according to Alexander Meiklejohn, this encompasses all elements of the arts, sciences and humanities that allow man to improve himself and his ability to govern himself.⁴⁹² Mill's development is achieved when these ideas compete in the community:

[W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate

⁴⁸⁶ G.R. No. 16444, 41 Phil. 62, Sept 8, 1920.

⁴⁸⁷ *Id.*, quoting *United States v. Holt*, 218 U. S. 245 (1910).

⁴⁸⁸ *Villafior*, 41 Phil. at 70.

⁴⁸⁹ JOHN STUART MILL, *On Liberty*, in *ESSENTIAL WORKS OF JOHN STUART MILL* 263 (Max Lerner ed., 1961).

⁴⁹⁰ George Wright, *Speech in Constitutional Sense*, in *THE FUTURE OF FREE SPEECH* LAW 8 (1990).

⁴⁹¹ *Id.* at 6.

⁴⁹² EDWIN BAKER, *HUMAN LIBERTY AND FREEDOM OF SPEECH* 26 (1989), citing Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUPREME CT. REV. 245, 256-57.

good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.⁴⁹³

Griswold outlined freedom of speech facets of privacy categorized under decisional privacy, and cited *Pierce* and *Meyer*. Justice Cortes likewise explored this line, citing *West Virginia Board of Education v. Barnette*,⁴⁹⁴ which enjoined a requirement for public school children to salute the flag.⁴⁹⁵

In the context of this market of ideas, however, the fullness of the “right to be let alone” is the right to speak anonymously. As the American Court held:

Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.⁴⁹⁶

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all....⁴⁹⁷

Simply, anonymity allows an individual to exchange thoughts in certain ways or regarding certain subjects that he would otherwise be unable to. Professor Michael Froomkin wrote, “The ability to protect a secret, to preserve one’s privacy, is a form of power.”⁴⁹⁸ The right to voice these thoughts necessarily requires the right to associate with others of like mind, to interact with them or to voice ideas collectively, and requires the same zone of elbow room. *NAACP v. Alabama*, for example, held that compelled disclosure of the National Association for the Advancement of Colored

⁴⁹³ *Abrams v. United States*, 250 US 616, 631 (1919) (Holmes, J. and Brandeis, J., dissenting), quoted in *Babst v. National Intelligence Board*, G.R. No. 62992, 132 SCRA 316, 345, Sep. 28, 1984 (Fernando, C.J., concurring).

⁴⁹⁴ 319 U.S. 625 (1943).

⁴⁹⁵ *CORTES*, *supra* note 418, at 35.

⁴⁹⁶ *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), citing *JOHN STUART MILL, On Liberty*, in *ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT* 1, 3-4 (R. McCallum ed., 1947).

⁴⁹⁷ *Talley v. California*, 362 US 60, 66 (1960).

⁴⁹⁸ Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1475 (2000).

Peoples' membership list would entail "the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association;"⁴⁹⁹ "the guarantee would be robbed of its significance if privacy in group association were not also recognized."⁵⁰⁰ *Griswold* considered this to mean, "the First Amendment has a penumbra where privacy is protected from governmental intrusion."⁵⁰¹

Modern life has led to other nuances in this zone of privacy surrounding associations. Today, the right to associate with a group is emasculated if stripped of the concurrent right to support it financially.⁵⁰² Thus, the American Court ruled:

A restriction on the amount of money a person or group can spend on political communication during a campaign necessarily reduces the quantity of expression by restricting the number of issues discussed, the depth of their exploration, and the size of the audience reached. This is because virtually every means of communicating ideas in today's mass society requires the expenditure of money.⁵⁰³

This, too, must be allowed with relative anonymity and without fear of undue publicity. The Constitution also shelters a right of expressive association. *Roberts v. United States Jaycees* held:

The Court has long recognized that, because the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State.... [T]he constitutional shelter afforded such relationships reflects the realization that individuals draw much of their emotional enrichment from close ties with others.⁵⁰⁴

⁴⁹⁹ *National Ass'n for the Advancement of Colored People v. Alabama*, 377 U.S. 288, 308 (1964).

⁵⁰⁰ *CORTES*, *supra* note 418, at 34.

⁵⁰¹ *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965).

⁵⁰² Emmanuel Gross, *The Influence of Terrorist Attacks on Human Rights in the United States: The Aftermath of September 11, 2001*, 28 N.C. J. INT'L L. & COM. REG. 1, 7 (2002), citing David Cole, *Hanging With the Wrong Crowd: Of Gangs, Terrorists, and the Right of Association*, 1999 SUP. CT. REV. 203, 248 (1999).

⁵⁰³ *Buckley v. Valeo*, 424 US 1, 20 (1976).

⁵⁰⁴ *Roberts v. United States Jaycees*, 468 U.S. 609, 619 (1984). *Roberts* is the leading case on "expressive association." *Boy Scouts of America v. Dale*, 000 U.S. 99-699, June 28, 2000. Here, the United States Supreme Court ruled that the Boy Scouts of America cannot be forced by the State to reinstate an assistant scoutmaster who was removed after it was discovered that he was a homosexual and gay rights activist. That would

Simply, men need to "retreat in solitude" to think, to speak, and to associate; they need that "private space in which a man may become and remain himself."⁵⁰⁵ Undue disclosures and intrusions into these likewise pierce the "wall between himself and the outside world" and deny "full protection in person and in property."⁵⁰⁶

Applying this evolution concretely to Remedial Law, it is submitted that a judge must be wary of unnecessarily tearing down this wall described by Brandeis and Warren, and lifting the fragile veil of anonymity that every individual is entitled to.

Note that this anonymity is not necessarily absolute; American privacy doctrine recognizes a concept called "practical obscurity."⁵⁰⁷ *Department of Justice v. Reporters Committee for Freedom of the Press* upheld an expectation of privacy in government compilations based on already public criminal records scattered throughout the country:

[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.⁵⁰⁸

The Court also distinguished that additional nonconviction data in the compilations was not generally available to the public, and that the information was not about the government itself, but merely information about citizens stored by the government.

amount to undue interference into an association's internal affairs by forcing it to accept a member it does not desire, a member whose presence would affect the group's ability to advocate certain public or private views.

⁵⁰⁵ CORTES, *supra* note 418, at 4.

⁵⁰⁶ Warren & Brandeis, *supra* note 359, at 193.

⁵⁰⁷ *Dept. of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 778 (1989). "The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of 'what the Government is up to,' the privacy interest protected by Exemption 7(C) is in fact at its apex while the FOIA-based public interest in disclosure is at its nadir."

⁵⁰⁸ *Id.* at 764.

More importantly, *Reporters* also held that privacy may still be expected over information *previously made public*, and rejected what it called a "cramped notion of personal privacy,"⁵⁰⁹ citing *Whalen*.⁵¹⁰ Similarly, *Air Force v. Rose*⁵¹¹ blocked outsiders' research into discipline summaries that had already been publicly posted on forty bulletin boards in the Air Force Academy campus, holding:

Despite the summaries' distribution within the Academy, many of this group with earlier access to summaries may never have identified a particular cadet, or may have wholly forgotten his encounter with Academy discipline. And the risk to the privacy interests of a former cadet, particularly one who has remained in the military, posed by his identification by otherwise unknowing former colleagues or instructors cannot be rejected as trivial.⁵¹²

Air Force refused to compel the government to release the summaries even with the names redacted, holding that anyone familiar with the Academy could readily identify the individuals concerned through other accompanying details.

A judge faced with a discovery request must similarly be able to appreciate this context granted to personal information. Although an opposing party is generally named in a lawsuit, the context of a right to relative anonymity must be appreciated to block undue probing. The example is, again, *Jovanovic*, where a rape suspect sought to unearth every detail regarding his victim's sex life.

VIII. APPLICATION OF THE CONSTITUTIONAL RIGHT TO PRIVACY

This final section will discuss how privacy rights are hardly discussed even in current American litigation, but will note that this is explained by many factors, such as the decreased expectation of privacy in the workplace and in work-related communication. It will then point to two small but important areas of jurisprudence where privacy has been lent more weight: first, Internet defamation cases concerning anonymous defendants; and second, *Playboy Enterprises, Inc. v. Welles*, which involved a self-employed defendant who used her home computer for business. It will then argue that

⁵⁰⁹ *Id.* at 762-63.

⁵¹⁰ *Id.* at 762, citing *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977).

⁵¹¹ 425 U.S. 352 (1976). Note that this doctrine is readily applicable in conjunction with *Ople*, which dealt with a government-maintained database of personal information.

⁵¹² *Id.* at 380-81 (1976), quoted in *Reporters*, 489 U.S. 749 at 768-69.

there is actually a spectrum of situations, and that the latter two represent the opposite end where privacy concerns are more significant, but that this end of the spectrum has not yet become visible in jurisprudence.

Again, *Ople v. Torres* ruled that not only is the right to privacy founded on a number of fundamental rights, it is itself a fundamental right.⁵¹³ Thus, when Fr. Bernas noted that the right against unreasonable search, which is a foundation of the right to privacy, must be applied to discovery,⁵¹⁴ this fundamental nature cannot be discounted.

There is a yawning chasm of difference in practice between the liberal spirit of Constitutional Law, however, and the investigative bent of Remedial Law. Simply, the latter still treats the right with skepticism and disbelief. For example, in the landmark Internet defamation case *Blumenthal v. Drudge*,⁵¹⁵ when a presidential aide sought to exclude documents from discovery citing privacy, the court merely footnoted:

No such privilege is generally recognized in this context, however, and defendant may not withhold any documents on this basis. With the exception of document numbers 25-28, which appear to be protected by the attorney-client privilege... the Court will compel production of these documents.⁵¹⁶

A footnote in the 2003 case *Green v. Bacc*⁵¹⁷ listed third parties' rights to privacy as one of several evidentiary privileges the responding party was claiming. However, whether this was applicable went undecided as the judge rejected the claims because they were blanket claims of privilege and the party failed to make particular allegations regarding the nature of any of the documents.⁵¹⁸ The 2003 case *United States v. Bell*⁵¹⁹ was more explicit:

There is no "right of privacy" privilege against discovery in civil cases. However, the court may take concerned individuals' privacy interests into consideration in determining whether a discovery request is oppressive or unreasonable... [T]he court does not believe that production of the unprivileged materials would be oppressive or

⁵¹³ *Ople v. Torres*, G.R. No. 127685, 239 SCRA 143, Jul. 23, 1998.

⁵¹⁴ BERNAS, *supra* note 355, at 166.

⁵¹⁵ 186 F.R.D. 236 (D.D.C. 1999).

⁵¹⁶ *Id.* at 244 n.10.

⁵¹⁷ 219 F.R.D. 485 (C.D. Cal. 2003).

⁵¹⁸ *Id.* at 491 n.22. "Defendant invokes the attorney-client privilege, the attorney work product doctrine, the official information privilege, and third parties' rights to privacy." See also Sanchirico, *supra* note 342, at 1239 n.93.

⁵¹⁹ 217 F.R.D. 335 (M.D. Penn. 2003).

unreasonable. Accordingly, the court finds Bell's right of privacy argument unpersuasive.⁵²⁰

Nevertheless, none of the abovedealt with e-mail or electronic evidence. However, *United States v. Hambrick*⁵²¹ ruled that an Internet provider's client has no expectation of privacy with respect to the billing information he discloses.⁵²² Still, this ruling may not be persuasive because it involved an Internet user who was charged with trying to entice a 14-year old boy to live with him, and the court emphasized that neither law nor his contract with the provider prohibited disclosure of his personal information to the government.

The problem is arguably one of mindset. First, as *Bell* notes, there is no explicit privilege that protects the right to privacy, unlike the attorney-client privilege which arguably arises from similar Constitutional fabric.⁵²³ The right, further, is not as familiar as others such as Due Process and Equal Protection such that a judge is expected to be cautious in safeguarding it. Thus, despite the fundamental nature of the right to privacy, it goes unrecognized, and becomes a straw man that falls before the general liberal treatment of discovery.

Second, very few electronic evidence cases have facts similar to *Jovanovic* where abuse is clear; privacy violations are less apparent in corporate litigation, for example. It is rarely correct to say that the right does not apply in a given context. Rather, the right to privacy may be deemed waived, there is a decreased expectation of privacy, or privacy is balanced against and is outweighed by a more compelling interest. Of course, a trial is a public event and what transpires in the court room is public property,⁵²⁴ and a litigant expects to have his affairs probed before the judge. Nevertheless, especially given the pervasiveness of electronic records, one should be able to argue that one does not enter court expecting every corner of his life to be scrutinized.

Again, given the right's fundamental nature, a balancing of interests should take place, and in extreme cases such as *Jovanovic*, the balance should

⁵²⁰ *Id.* at 343, citing *Hecht v. Pro-Football, Inc.* 46 F.R.D. 605, 607 (D.D.C. Circ. 1969); *United States v. Federation of Physicians and Dentists, Inc.*, 63 F.Supp.2d 475, 480 (D.Del. 1999).

⁵²¹ 55 F.Supp.2d 504 (E.D. Va. 1999).

⁵²² *Id.* at 508-09.

⁵²³ See BAUTISTA, BASIC EVIDENCE, *supra* note 255, at 61.

⁵²⁴ *Craig v. Harney*, 331 U.S. 367, 374 (1947).

swing hard enough that the burden should not even be on the victim to resist such an intrusive discovery order; and the judge should not even need to conduct an *in camera* inspection to realize this. Because "the right to be let alone" may be violated even without disclosure of information, having a judge poring over thousands of pages of one's personal e-mails to look for the details of one's sexual proclivities is almost as intrusive as having the rapist do it.

Even assuming judges have such a framework in mind, privacy loses the balance in many cases, and is quickly set aside. However, this is understandable given that most targets of discovery so far discussed are e-mails and records one makes in the course of business or made by one's employees. One is deemed to have a lower expectation of privacy in one's workplace,⁵²⁵ as this is the center of one's public life, on the opposite end of the spectrum from the home.

Further, there are specific reasons why employees have a decreased expectation of privacy with respect to work e-mail accounts. First, employers have legitimate interests in monitoring the workplace.⁵²⁶ They have a responsibility, for example, to police messages that constitute sexual harassment or pornography.⁵²⁷ In *Blakey v. Continental Airlines*,⁵²⁸ for example, the airline was sued by its first female captain for sexually explicit messages on the company's electronic bulletin board. In *Strauss v. Microsoft Corp.*,⁵²⁹ the corporation was sued by a female employee because the staff circulated sexually charged e-mails, such as a parodied play, "A Girl's Guide to Condoms." In *Coniglio v. City of Berwyn*,⁵³⁰ the city was sued by a female employee over a manager who viewed pornography from the Internet and printed it out in full view of female employees.

Monitoring Internet use is simply cheaper than incurring such lawsuits,⁵³¹ which goes to the second reason, namely that the employer owns

⁵²⁵ *O'Connor v. Ortega*, 480 U.S. 709, 715-17 (1987). This decision, however, emphasized that a decreased expectation is not the same as a nonexistent expectation.

⁵²⁶ *Id.* at 717. See Michael Rustad & Thomas Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 95 (2003).

⁵²⁷ Porter & Griffaton, *supra* note 54, at 67.

⁵²⁸ 751 A.2d 538 (N.J. 2000).

⁵²⁹ 814 F.Supp. 1186 (S.D. N.Y. 1993).

⁵³⁰ 2000 WL 967989 (N.D. Ill. 2000).

⁵³¹ Frank Morris, *The Electronic Platform: Email and Other Privacy Issues in the Workplace*, 20 NO. 8 COMPUTER & INTERNET LAW. 1, 1 (2003); Fernando Piera, *International*

the facilities. Thus, the fact that workers may be given individual accounts and password protection is not deemed to create any expectation of privacy.⁵³² This is true especially if the employer makes such clear in employee manuals and the like, but even employers with no explicit policies have been upheld in court.⁵³³

Third, monitoring is also a lesser evil compared to other liabilities, such as having copyright infringing material enter the company computers, or having employees send proprietary material to outside parties.⁵³⁴ To cite one especially striking example, the CEO of Cerner Corp. once threatened his staff via e-mail with layoffs and benefit freezes if productivity did not improve. Less than ten days later, the message was posted on the Internet and the company's stock price dropped.⁵³⁵ An employer also has an interest in detecting legally incriminating material that may later be subject to electronic discovery.

Finally, an employer simply needs to monitor the use of computer resources, from clogging due to large image or pornography files to viruses.⁵³⁶ Thus, today, about one-third of American workers with workplace Internet access are subject to monitoring, and employers can block them from certain web sites, read individual messages, and block messages with certain keywords.⁵³⁷

Nevertheless, *Rowe Entertainment v. William Morris Agency* stated:

To the degree the defendants seek to assert the privacy concerns of their employees, those interests are severely limited. Although personal communications of employees may be appear in hard copy as well as in electronic documents, the defendants made no effort to exclude personal messages from the search of paper records conducted by plaintiffs' counsel. Moreover, an employee who uses his or her employer's computer for personal communications

Electronic Commerce: Legal Framework at the Beginning of the XXI Century, 10-SUM CURRENTS: INT'L TRADE L.J. 8, 18 (2001).

⁵³² *Id.* at 3.

⁵³³ Mark Schreiber, *Employer E-Mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 84 (2000).

⁵³⁴ Porter & Griffaton, *supra* note 54, at 69.

⁵³⁵ Morris, *supra* note 531, at 5.

⁵³⁶ Matthew Finkin, *Information Technology and Worker's Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).

⁵³⁷ Charles Kerr et al., *Privacy - The Proliferating Legal Landscape*, 683 PLI/PAT 561, 752 (2002).

assumes some risk that they will be accessed by the employer or by others.⁵³⁸

This implies that a court might be willing to exclude employees' clearly personal e-mails, though it is unlikely an employer would go to the additional expense of filtering such e-mails along with privileged material.⁵³⁹ Nevertheless, the general rule remains a lack of reasonable expectations at work. The exceptions cover personal e-mail accounts of employees, though accessed at work. In *Fischer v. Mount Olive Lutheran Church*,⁵⁴⁰ a pastor guessed the password of and accessed such a personal account belonging to an employee he suspected of having multiple homosexual relationships. The court held that an expectation of privacy was possible. However, such personal accounts would likely be outside the scope of discovery, unless they belonged to impleaded employees.

Although privacy finds little application in the general work context, there are clearly scenarios where it has been used as the ground to resist discovery. The most common in present American jurisprudence are found in Internet defamation suits,⁵⁴¹ where the Internet provider has to be subpoenaed to obtain the identity of an anonymous user. Such suits may be serious matters, such as when Internet pranksters post rumors or claim to be employees, and affect small companies' stock prices. These incidents are called "cybersmears." These issues, incidentally, highlight the link between the right to privacy and the penumbras.

In 2000, Judge Joan Melvin sued an anonymous person who accused her on his website of lobbying the governor to appoint an unnamed lawyer to a vacancy in the judiciary. Through counsel, the anonymous defendant attempted to protect his identity during discovery. The Pennsylvania court denied this, recognizing a state interest in discouraging the defamation of public officers.⁵⁴²

Melvin v. Doe examined the inquiry using a threefold test. The defendant's identity must be:

⁵³⁸ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

⁵³⁹ *Marron*, *supra* note 56, at 922.

⁵⁴⁰ *Fischer v. Mount Olive Lutheran Church*, 2002 WL1306900 (W.D. Wis. 2002).

⁵⁴¹ It must be noted that these have become very important in American Internet jurisprudence. Online defamation cases, for example, accounted for 29% of punitive damages in Internet cases from 1992-2002. *Rustad*, *supra* note 188, at 47.

⁵⁴² *Melvin v. Doe*, 49 Pa. D. & C. 4th 449, 477 (2000).

- 1) material, relevant and necessary
- 2) unobtainable by other means
- 3) crucial to the plaintiff's case

The following year, 2TheMart.com tried to obtain the identities of twenty three anonymous users of a forum called "Silicon Investor," operated by Infospace. They had posted several unflattering comments; one who called himself "Truthseeker" called the company "a Ponzi scam that Charles Ponzi would be proud of" and accused the CEO of defrauding employees in the past. 2TheMart claimed that these messages had resulted in part of damage it was in turn being sued for by its shareholders. The Washington court considered a four-prong test:

- 1) the subpoena seeking the information was issued in good faith and not for any improper purpose,
- 2) the information sought relates to a core claim or defense,
- 3) the identifying information is directly and materially relevant to that claim or defense, and
- 4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.⁵⁴³

The court concluded that the company's motion sought to obtain material such as personal e-mails that had little relevance to the shareholder suit, and related to only one generalized claim out of twenty-seven affirmative defenses. Moreover, although the company alleged that the forum messages affected its stock prices, these were read by the public without knowing the identities of the authors. The company alleged that it needed to compare the authors' names with those of others who may have engaged in stock manipulation, but the allegation alone could not balance

⁵⁴³ John Doe v. 2TheMart.com, 140 F.Supp.2d 1088 (W.D. Wash. 2001), *citing* Columbia Ins. Co. v. Seescandy.Com, 185 F.R.D. 573, 578 (N.D.Cal. 1999); *In re* Subpoena Duces Tecum to America Online, Inc., 2000 WL 1210372, (Va. Cir. Ct. 2000).

against the right to free speech. The subpoena in the case was thus quashed.⁵⁴⁴

Less than three months later, a New Jersey Court ruled that Dendrite International could not obtain the identity of an anonymous Yahoo forum user. "John Doe No. 3" had accused its president of accounting misconduct and of trying to sell the uncompetitive company, but the court ruled that Dendrite had failed to prove a connection between the statements made and harm to the company. It noted, for example, that its stock price had actually increased on five out of eight days when Doe posted messages.⁵⁴⁵

Dendrite applied a different test:

- 1) The court should require notice to the defendant and an opportunity to be heard;
- 2) The court should require the plaintiff to set forth the exact statements that are the basis of its claim;
- 3) The court should receive evidence and determine not only whether the complaint would survive a motion to dismiss but whether plaintiff has submitted sufficient prima facie evidence to support its claim;
- 4) Assuming plaintiff has presented a prima facie claim, "the court must balance the defendant's First Amendment right of anonymous speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."⁵⁴⁶

⁵⁴⁴ See Richard Raysman & Peter Brown, *Discovering the Identity of Anonymous Internet Posters* (Sep. 11, 2001), available at <http://econ.law.harvard.edu/stjohns/anon-net.html>. This brief article from the *New York Law Journal* summarizes the various frameworks found in State cases from 2000 to 2001.

⁵⁴⁵ *Dendrite International v. Doe No. 3*, 342 N.J. Super. 134 (App. Div. 2001).

⁵⁴⁶ Michael Vogel, *Unmasking "John Doe" Defendants: The Case for Caution in the Creation of New Legal Standards*, at 2, at <http://www.cfp2002.org/proceedings/proceedings/vogel.pdf> (last visited Feb. 28, 2004).

Another New Jersey case, however, applied the *Dendrite* framework, but denied the anonymous defendant's motion to quash a similar subpoena. "Jean Doe aka moonshine_fr" posted messages on a Yahoo forum that identified her as "a worried employee" and described the alleged sales situation of the Immunomedics. The company showed a confidentiality agreement in its employment contracts and attempted to obtain moonshine's identity. The court ruled that Immunomedics had shown a *prima facie* cause of action for a breach of the agreement and stated:

Although anonymous speech on the Internet is protected, there must be an avenue for redress for those who are wronged. Individuals choosing to harm another or violate an agreement through speech on the Internet cannot hope to shield their identity and avoid punishment through invocation of the First Amendment.⁵⁴⁷

The latest case is slightly more complicated. In *La Societe Metro Cash & Carry France v. Time Warner Cable*,⁵⁴⁸ the plaintiff company that operated facilities in France traced a malicious e-mail to Time Warner's network and obtained a discovery order from a French court. The user was informed, and demanded no disclosure be made without an order from an American court. The plaintiff brought another action in Connecticut and the subscriber was permitted to litigate the privacy objection as Jane Doe, and even claimed self-incrimination and anonymous speech rights under the United States Constitution. However, after considering the privacy claim at length, the court applied *Doe v. 2theMart.com* and other cases, and granted discovery because the plaintiff had established probable cause and there was no other means of determining the defendant's identity.

Clearly, although the actual frameworks used are unsettled, American courts take privacy claims of anonymous defendants in these Internet defamation cases very seriously, and the balancing of interest applications are clear as crystal. Since June 1998, one or two lawsuits seeking to unmask forum users are filed each week in Santa Clara County, California, home of Yahoo! Inc.⁵⁴⁹ On one hand, higher bars for subpoenas in cyber-smear cases are hailed by libertarians. The defense attorney in 2TheMart, for

⁵⁴⁷ Immunomedics v. Jean Doe, 342 N.J. Super. 160, 167 (App. Div. 2001).

⁵⁴⁸ La Societe Metro Cash & Carry France v. Time Warner Cable, 2003 WL 22962857 (Conn. Super. 2003).

⁵⁴⁹ Blake Bell, *Dealing With the "Cybersmear"*, at n.8 (Apr. 19, 1999), available at <http://www6.law.com/ny/tech/041999t3.html>.

example, decried 2TheMart's actions as "a huge fishing expedition."⁵⁵⁰ A high bar for such subpoenas may be desirable to avoid a chilling effect⁵⁵¹ and to deter employers and companies who simply want to retaliate.⁵⁵² On the other hand, "although in many cases the battle between the anonymous poster and potential plaintiff is framed as one pitting the little, helpless individual, David, against the powerful, greedy corporate, Goliath, 'the reality is that sometimes the little guy is being a jerk.'"⁵⁵³ Too high a bar then makes redress illusory.⁵⁵⁴

The *Dendrite* test essentially asks a plaintiff to prove his allegations of libel before he is allowed to discover who he is suing, and this may not be possible without the defendant's identity. 2TheMart, for example, accused the anonymous forum users of manipulating its stock prices. If another company made the same accusation but further accused John Doe of being a competitor, it may need that competitor's trading records and other information to establish its *prima facie* case.⁵⁵⁵ In any case, in this line of

⁵⁵⁰ Stefanie Olsen, *Ruling seen as victory for online speech*, ¶ 10 (Apr. 20, 2001), at <http://news.com.com/2100-1023-256200.html?legacy=cnet>. "It's a huge fishing expedition," said Gelman, who represented the defendants. "Our Does weren't being sued. They weren't accused of being wrongdoers. They were just people who posted on a message board."

⁵⁵¹ John Doe v. 2TheMart.com, 140 F.Supp.2d 1088, 1093 (W.D. Wash. 2001).

⁵⁵² Jennifer O'Brien, *Putting a Face to a (Screen) Name: The First Amendment Implications of Compelling ISPs to Reveal the Identities of Anonymous Online Speakers in Online Defamation Cases*, 70 FORDHAM L. REV. 2745, 2766 (2002) citing Motion to Quash, Raytheon v. Does 1-21, No. 99-816 (Mass. Super. Ct. Middlesex County complaint filed Feb. 1, 1999). "Raytheon Co. sued twenty-one anonymous posters, alleging that their postings on a Yahoo! message board revealed confidential information about rumored mergers and acquisitions, divestitures, and defense contracts. After learning the identities of the posters by subpoenaing numerous ISPs, Raytheon dropped the suit against the defendants, many of whom turned out to be employees of the company who then quit their jobs or were sent for 'corporate counseling.' Unfortunately, Raytheon is just one example in a troubling line of cases in which corporations bring subpoenas to learn the identities of the anonymous posters, but then choose to forego judicial remedies." One of the John Does, in fact, turned out to be a vice-president. Bell, *supra* note 549, ¶ 20.

⁵⁵³ O'Brien, *supra* note 552, at 2766 quoting Mark Gibbs, *Responsible Anonymity and John Doe*, NETWORK WORLD, Jun. 28, 1999, ¶ 2 at <http://www.nwfusion.com/archive/1999b/0628gibbs.html>.

⁵⁵⁴ O'Brien, *supra* note 552, at 2747-48. She gives the example of "MadAl," a supposedly disgruntled employee of a retail manufacturer. MadAl accused his company's managers of incompetence and even of embezzling, and they resorted to trying to identify him by subpoenaing the ISP he used to connect to the Internet.

⁵⁵⁵ Vogel, *supra* note 546, at 3.

cases, it is clear that the trial judge's discretion is restricted by clear guidelines to balance interests, instead of allowing discovery outright.⁵⁵⁶

The most promising case to base a privacy objection on remains *Playboy*, however. Although this is often cited in infringement cases and for its detailed discovery order that involved creating a "mirror" copy of the defendant's hard drive, many overlook that *Welles* also featured a privacy claim that was taken very seriously by the court.⁵⁵⁷

The facts of *Welles* are subtly but significantly different from all the other cases discussed so far because 1981 "Playmate of the Year" Teri Welles was self-employed and used her personal computer for both business and personal e-mails.⁵⁵⁸ She admitted to deleting her e-mails immediately after reading them, despite a discovery order in the pending litigation, leading the plaintiff to ask to be allowed to recover the deleted e-mails. Welles' position was summarized by the court:

Defendant contends that her business will suffer financial losses due to the approximate four to eight hour shutdown required to recover information from the hard drive. Defendant also contends that any recovered e-mails between her and her attorneys are protected by attorney-client privilege. Lastly, Defendant contends that the copying of her hard drive would be an invasion of her privacy.⁵⁵⁹

The court's order deviated from the ones usually seen in such discovery cases:

Considering these factors, the Court determines that the need for the requested information outweighs the burden on Defendant. Defendant's privacy and attorney-client privilege will be protected pursuant to the protocol outlined below, and Defendant's counsel will have an opportunity to control and review all of the recovered e-mails, and produce to Plaintiff only those documents that are relevant, responsive, and non-privileged. Any outside expert retained

⁵⁵⁶ See Samtani Amil, *Cyberspace and the Law of Defamation: Developing a Workable Model*, C.T.L.R. 2001, 7(7), 180 (2001). Discussing the applicability of American cases to Singapore, the author noted, "A notable difference is the presence of the jury in the U.S. courts and its absence in Commonwealth courts. Though a judge presides in both legal systems, the judge in the U.S. plays a much diminished role vis-à-vis his Commonwealth counterpart."

⁵⁵⁷ Marron, *supra* note 56, at 921. Only one out of more than one hundred journal articles and none of the cases reviewed discussed this point regarding *Welles*.

⁵⁵⁸ *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999).

⁵⁵⁹ *Id.* at 1054.

to produce the "mirror image" will sign a protective order and will be acting as an Officer of the Court pursuant to this Order. Thus, this Court finds that Defendant's privacy and attorney-client communications will be sufficiently protected. Further, Plaintiff will pay the costs associated with the information recovery. Lastly, if the work, which will take approximately four to eight hours, is coordinated to accommodate Defendant's schedule as much as possible, the Court finds that the "down time" for Defendant's computer will result in minimal business interruption.⁵⁶⁰

In *Welles*, the court clearly recognized the privacy ground, since it ruled that the need for the information outweighed it, instead of dismissing the former outright, as in *Blumenthal*. Moreover, it took measures to safeguard Welles's privacy by allowing her lawyer to remove personal as well as privileged e-mails. It even explicitly ordered the plaintiff to "accommodate Defendant's schedule as much as possible." The key difference was Welles's self-employed status. First, this and her clear use of her computer for personal purposes gave her a clearly more significant expectation of privacy than an ordinary employee. Second, she owned the computer, and employer monitoring justifications did not apply to her. In short, she could not have a decreased expectation of privacy by virtue of being at the workplace, and the court perceived this difference.

Similar details apply to the anonymous defendants in the Internet cases, or at least potentially did, since one would be unsure of their circumstances. Thus, one begins to see that the right to privacy in the context of electronic discovery is actually found in a spectrum. The bulk of present decisions deal with commercial litigation where the business contexts and surrounding facts do not support privacy objections, but they are actually only one end of the scale. In the middle, one finds the anonymous defendant cases and *Playboy*, where a balancing of interests takes place. On the opposite pole, this author thus submits that one finds extreme cases such as *People v. Jovanovic* where the breadth and intrusiveness of discovery requests border on abuse. At this point, at least, such out-of-bounds discovery should no longer be treated liberally, and the burden should no longer be placed on the producing party.

As electronic discovery becomes more common and more closely integrated into the legal process, the other side of the spectrum will inevitably surface. Lawyers and judges alike should thus be ready to recognize more appropriate applications of the right to privacy, which is

⁵⁶⁰ *Id.* at 1055.

again explicitly held fundamental in the Philippines. At the very least, one can take *United States v. Bell's* stance and use privacy as a ground to claim that a discovery request is unreasonable and oppressive, but this sells the Constitutional foundations short.

One only has to think of a loved one raped and then subject to the indignity of having her e-mail being browsed by the suspected rapist.

CONCLUSION

Novelist Ayn Rand wrote:

So you think that money is the root of all evil? ... Have you ever asked what is the root of money?... Money is made possible only by the men who produce. Is that what you consider evil?⁵⁶¹

In the same way, it is sophomoric to assign notions of good to electronic discovery, and exhort lawyers to adopt an atmosphere of openness given the pervasiveness of electronic records. There are two sides to every litigation, and perhaps the goal should not be so much as truth as it should be mutual respect, given the new set of costs, burdens and intrusions that electronic discovery introduces. Amidst the wide-eyed wonder at the potentials, one should not forget that discovery is merely a tool and a process, with no mind or value judgments of its own, and it should be analyzed, wielded, and refereed critically.

If electronic discovery is the litigator's dream come true, then it must at the same time be his worst nightmare as well. Grafting *Rowe Entertainment v. William Morris Agency* and *Playboy Entertainment, Inc. v. Welles* onto *Hickman v. Taylor*, one draws up a rough plan for the possibilities of resisting electronic discovery:

1. The material requested is privileged.
2. The time and cost involved is prohibitive, and the requesting party should at least shoulder the costs.
3. The discovery request is overly broad and the material requested is irrelevant.

⁵⁶¹ AYN RAND, *ATLAS SHRUGGED* 382 (1957).

4. The discovery request is in bad faith or is meant to annoy, embarrass or oppress.
5. The discovery request violates the right to privacy.

Privilege is a simple first line of defense, though it is applicable only in particular situations, and is treated as the exception to the general rule. Aside from the familiar attorney-client privilege, the broader work product privilege which is only beginning to become recognized in the Philippines proves useful. Given the longer written trail people leave with e-mail use, one should argue to expand the application of privilege, lest opponents pierce them through documents at the periphery of the protections. One should also recognize the nuances of electronic communications, however, and learn, for example, how to maintain confidentiality in using these, and how to establish due diligence in conducting privilege reviews of material.

In cases with large numbers of documents, one may cite the burden of discovery and negotiate for narrower requests, or at least for cost shifting. This approach is straightforward using the *Rowe* framework. Barring these, one must argue irrelevance or bad faith, and establish these to the satisfaction of the judge. Outside *Rowe*, no widely-used guidelines exist for the multifarious factual scenarios these can be argued under, and the matters are left to the judge's discretion.

The emerging defense is the right to privacy. Decisional privacy arguably covers the attorney-client and work product privileges, but informational privacy is "the right to be let alone" itself. Although one expects in litigation that one will precisely not be let alone, some area's of one's life are arguably out of the bounds of a given litigation. At present, the bulk of electronic discovery cases involve workplace communication where the expectations of privacy are low, but one already sees exceptions to this with the Internet defamation cases, *Playboy v. Welles*, and *People v. Jovanovic*. As electronic discovery becomes more commonplace in litigation, the significance of the right to privacy should be clear, and courts should be conscious of potential *Jovanovics*.

The problem of an advocate of privacy, however, is the current judicial mindset that strongly leans towards treating discovery liberally. With the breadth of electronic discovery, this may no longer be appropriate in all cases. As one author writes:

Anecdotal evidence suggests that the present discovery rules are changing the way we use e-mail. Commentators have increasingly recommended extreme caution to companies in the use of e-mail, often citing broad discovery of e-mails and the inability to control the destruction of e-mails as key factors... Many commentators recommend companies not to allow e-mail to be used for personal purposes, others place restrictions on the type of communications that e-mail may be used for, and some warn that "if you wouldn't want the message published in a newspaper, don't write it in an e-mail" or encourage employers to "tell employees that if they are in doubt about whether to send an e-mail, they should ask themselves: 'How would I feel if this ended up in the hands of my worst enemy?'" Businesses are encouraged to inform employees not to use humor or sarcasm and to adopt document "retention" policies that employ special software to permanently delete e-mails as soon as they are read.⁵⁶²

In 1970, Justice Irene Cortes wrote:

The computer age is upon us. While the use of computers in this country is as yet limited, the need to provide protection to individual privacy against threats arising from computerization will have to be met. A legal framework will have to be established which, while recognizing the various ways in which the computer may be utilized, will also afford protection to privacy.⁵⁶³

She could not have known how true her words would ring today. Thus, again, there are two sides to every litigation. The playing field must be made fair and level. Otherwise, if one uses the court as the very tool to cast too wide a net, it may well be one's client caught in the next case.

Lawyers must set aside the uncritical wide-eyed wonder. Sometimes, perhaps, certain incredible things are best left unknown.

- o0o -

⁵⁶² Marron, *supra* note 56, at 923-24.

⁵⁶³ CORTES, *supra* note 418, at 12.