2011

You've got mail the study of the attorney-client privilege and the use of electronic mail

Justin W. McConnell
University of Central Florida

YOU'VE GOT MAIL: THE STUDY OF THE ATTORNEY-CLIENT PRIVILEGE AND THE USE OF ELECTRONIC MAIL

by

JUSTIN W. MCCONNELL

A thesis submitted in partial fulfillment of the requirements
for the Honors in the Major Program in Legal Studies
in the College of Health of Public Affairs
and in The Burnett Honors College
at the University of Central Florida
Orlando, Florida

Spring Term 2011

Thesis Chair: Dr. Kathy Cook

ABSTRACT

The prolific use of the internet and electronic mail within the legal profession presents novel challenges to the application of the attorney-client privilege; especially, in regards to protecting intended confidential communications relayed through e-mail. This thesis addresses the question of whether an attorney in Florida, through electronic mail use, can waive his client's right to the protections of the attorney-client privilege. After a review of current case law, law review articles, statutes, and texts, this thesis concluded that an attorney's communication through e-mail warrants a reasonable expectation of privacy, permitting the attorney to speak in reasonable confidence to clients through the web. However, attorneys, ethically, should consider the strong repercussions for using such a potentially transparent medium for communication.

By examining the relationship between current law, the application of the attorney-client privilege, and a reasonable expectation of privacy, this study provides a comprehensive analysis for attorneys concerned with electronic mail usage. Lastly, this thesis provides attorneys with best practices for their electronic mail communications.

DEDICATION

For my loving family, without their love and support, none of this would be possible.

And for or all my friends, thanks for making it all worthwhile. You kept me going when I couldn't have done so myself.

ACKNOWLEDGMENTS

I express sincere thanks and gratitude to my committee members, who have been especially gracious in providing insight, direction, and wisdom to make this project a reality. Special thanks to my thesis chair, Dr. Kathy Cook, for her continued dedication and guidance. Her unwavering support was the steady push I needed to succeed.

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER ONE: INTRODUCTION

In an instant, digital information can be sent around the world through a complex infrastructure of networks and computers. Computers share and communicate through a binary system of one's and zero's, transmitting data efficiently and quickly. Prior to the development of the internet and computer programs such as electronic mail, immediate global communication was restricted to costly international phone calls and overnight packages by airmail. Electronic mail and the internet have circumvented all traditional notions of how to communicate in a fast and cost-effective manner.

At the present, e-mail technology has so deeply penetrated our daily routines, we often fail to remember how we functioned without it. It's become a necessity for many. Yet, the developments in this fertile field for technological growth have only just begun. The increasing number of electronic mail providers and features adds more users each day. In 1994, it was estimated that nearly twenty-five million people used the Internet regularly.[1] Since then, that number has grown to nearly 2 billion, or approximately one-third of the world's population.[2] Each day more people, businesses, and professions rely on the web, and specifically electronic mail, to transmit information.

The legal profession is one that has been profoundly impacted by the use of electronic mail. Lawyers often communicate with fellow attorneys, judges, and clients using e-mail software. Communicating via electronic mail, instead of traditional mediums such as written letters and telephone conversations, allows attorneys to provide clients with more efficient and

[1] G. Burgess Allison, *At the Edge of the E-Frontier: An Introduction to the Internet*, 17 Pa. L. 12, 13 (1995)
[2] See http://www.internetworldstats.com/stats.htm

affordable legal assistance.[3] It also provides significant advantages over traditional mediums including increased speed, increased storage, reduced cost, and greater access.[4] More importantly, e-mail offers many attractive user features such as near-instantaneous delivery, the ability to see if messages are opened, and a wide selection of free and subscription-based software from which to choose. Many readers have an account with some of the popular free e-mail clients such as AOL, Yahoo, and Gmail. "The practice of law is [furthermore] dependent upon the rapid transmission of information and documents over geographical space…"[5]; electronic mail is not limited by physical boundaries, allowing messages to be sent and received from many different locations by the user. There are a myriad of circumstances where communicating electronically simply outcompetes other forms of communication. For example, an attorney waiting in a courtroom to be heard by a judge can send and receive e-mails, addressing client concerns without having to return to the office. There's no doubt electronic mail has revolutionized how attorneys communicate with their clients and others.

However, lawyers have expressed alarm over whether this new mode of communication is exposed to security or privacy threats. National media agencies have reported scams and security invasions of private, business, and government e-mail accounts. Usually, the negative repercussions of such attacks are small-scale, but they send an eerie message to lawyers: electronic mail may not be as safe as it is perceived to be.

---

[3] William L. Stephens, Jr. *Convenience vs. Confidentiality: An Evaluation of the Effects of Computer Technology on the Attorney-Client Privilege*, 35 Duq. L. Rev. 1011, 1012 (1997)
[4] Joshua M. 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, 1130 (1999)
[5] *Id.*

CNNMoney.com
A Service of CNN, Fortune & Money
Symbol Get Quo
Home | Business News | Markets | Personal Finance | Retirement | Technology

Mass e-mail breach: Just how bad is it?

Recommend 233 people recommend this. Be the first of your friends.

By David Goldman, staff writer April 6, 2011: 3:09 PM ET

NEW YORK (CNNMoney) -- It seems like every day for the past week, another dozen major companies have come out and said that they too have been affected by the **massive data breach** at e-mail marketing firm Epsilon.

Verizon (**VZ**, **Fortune 500**), Ritz Carlton, JCrew, Ann Taylor (**ANN**) and Victoria's Secret were among the most recent companies to tell customers that their e-mail addresses had ended up in the wrong hands.

Figure 1: CNN Article describing the recent data breach at the e-mail marketing firm, Epsilon.[6]

In particular, the use of e-mail has also raised the question of whether it's granted the same protections as other forms of communication in regards to the attorney-client privilege. Many attorneys are quick to add a signature line at the bottom of their e-mails which contains a similar warning as the one stated below:

> CAUTION: THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, forwarding, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately by e-mail or telephone, and delete the original message immediately. Thank you.[7]

[6] See http://money.cnn.com/2011/04/06/technology/epsilon_breach/index.htm
[7] See Yvette J. Liebesman, *The Potential Effects of United States v. Councilman on the Confidentiality of Attorney-Client E-Mail Communications*, 18 Geo. J. Legal Ethics 893 (2005)

In addition to a disclaimer located at the end of the message, some lawyers will also add a disclaimer in the subject line of the message, denoting its confidentiality.

The courts have already addressed how security and interception of communications between certain forms of communication, such as telephone calls, facsimile, and letters, shall be treated. Courts generally agree there is a reasonable expectation of privacy and confidentiality in telephone conversations, letters sent through the post office, and in facsimile transmissions. In contrast, because of the incredible speed at which the internet and electronic mail have developed, the courts and the legislature have lagged behind in adopting rules and regulations which specify what protections are granted to e-mail users. The United States Congress did enact protections of electronic modes of communication in 1986 under the Electronic Communications Privacy Act (ECPA).[8] This Act was designed to prohibit "all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials engaged in the investigation of specified types of major crimes after obtaining a court order." [9] The expectation of privacy affirmed through the Fourth Amendment was thus expanded by the ECPA statute to include electronic communications, and therefore affected the attorney-client privilege when communicating electronically. This statute, arguably, provides a reasonable expectation of privacy to electronic mail communications, which in turn was later used by state bar review committees in their evaluations of electronic mail use. [10]

Nevertheless, as technology is advancing at a faster pace than the legal community is able to adapt, the use of e-mail continues to present novel and controversial legal issues. Can these

[8] Electronic Communications Privacy Act, 18 U.S.C. § 2510-22 (1986)
[9] Liebesman, *supra* note 7, at 894
[10] Liebesman, *supra* note 7

unencrypted electronic mail communications between attorneys and their clients result in a waiver of the attorney-client privilege?

Currently, the American Bar Association (ABA) permits the use of unencrypted e-mail. In 1999, the ABA issued an official opinion that attorneys may use unencrypted e-mail without violating the Model Rules of Professional Conduct because the mode of transmission was found to afford a reasonable expectation of privacy from a technological and legal standpoint.[11] "This consensus, though, has developed without even one definitive court ruling—indeed, a court has never considered the issue of whether confidential e-mail communications are protected by the attorney-client privilege."[12] The goal of this thesis is to (1) pursue whether the current and common practice of using electronic mail to communicate with clients regarding confidential and privileged matters creates a legal waiver of the attorney-client privilege (2), whether the opinion issued by the American Bar Association is still valid, and (3) whether unencrypted electronic mail should be used for practical and legal reasons. After a thorough analysis of current law and practice in regard to e-mail, this thesis will make recommendations for the best practices of Florida attorneys in their use of electronic mail and the legal ramifications to which attorneys will be subjected.

CHAPTER TWO: ELECTRONIC MAIL

"You've got mail!" has become one of the most ubiquitous phrases in society. So much so, even a movie in 1998 titled "You've Got Mail" starring Tom Hanks and Meg Ryan was

[11] See ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99 (1999)
[12] Joseph W. Rand, *What would Learned Hand do?: Adapting to Technological Change and Protecting the Attorney-Client Privilege on the Internet*, 66 Brooklyn L. Rev. 361, 363 (2000)

released which recounted a love story that takes place on the internet using e-mail. Electronic mail has had a lasting impact on interaction and communication. Whereas at one time Americans would send billions of letters through the postal service, Americans now send billions of e-mail messages daily, compared to just 293 million pieces of first-class mail.[13] As more and more users go online, society is becoming accustomed to its habits of using e-mail as the standard means of communicating.

How Electronic Mail Functions

Electronic mail describes the function by which a person sends, and receives, messages, labeled as "mail," on a computer. It carries many of the same traits common to postal mail. Like postal mail, electronic messages need a location to be stored and received by the sender. This is usually labeled as the "inbox" or "mailbox" for most electronic mail clients. Electronic mail also requires an address to distinguish where the mail is sent and received. This, conveniently, is called an "e-mail address" consisting of a combination of text, numbers, and symbols followed by the "@," or "at" symbol, which is then followed by a domain name. Lastly, electronic mail bears semblance to a regular letter in that it contains a return address, subject line, date, and body.

Conversely, unlike postal mail, electronic mail is able to transmit more information than simple text. Today, although there are limitations, electronic messages can convey images, video, audio, and other forms of digital data. Postal mail is also tangible, meaning it can only be accessed in one physical space. E-mail, however, can be accessed globally through the internet,

[13] Michael R. Roberts, *Impacts of Email*, May 2010. <http://oak.ucc.nau.edu/mr/cte692/Module_6/impacts_of_email.html>

at any time and location. This may also be a potential limitation of electronic mail in the fact that without an internet connection, it cannot be accessed. Overall, despite its differences, electronic mail is a very comparable type of communication technology.

Two main categories separate how e-mails are sent. The first category describes e-mail sent through local area networks, "LAN" or "intranet". The second describes e-mails sent using the internet. Beginning with the first category, "[a] local area network is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. Rarely are LAN computers more than a mile apart."[14] LANs were first used in small law firms to share documents and information. For brevity and focused discussion, this thesis will not discuss LAN networking in regard to electronic mail. On the other hand, this thesis will focus on e-mail conveyed through the internet, as it poses a greater likelihood to compromise confidentiality and security.

In most cases, electronic mail is sent through the internet. Transmission through the internet utilizes a complex system of networks, routers, servers, and packetization across many different locations. Joseph Rand describes this process simply:

> [Networks forward] the e-mail through a 'router,' a device that analyzes the transmission, examines the various network points to which it could send the message next, and sends the message on the most efficient path based on its understanding of the state of the networks to which it is connected. In this process, the e-mail might go through up to a dozen separate routers on its way to its destination server, and it might be stored for a brief time on an immediate server while the router chooses a path for the next leg of its journey. During this time, the e-mail might also be broken down into chunks of information, or 'packets,' that might take different routes and get reassembled at the end of the journey.[15]

[14] See *Chapter 1: What is a Network?*, Florida Center for Instructional Technology College of Education, http://fcit.usf.edu/network/chap1/chap1.htm
[15] Rand, *supra* note 12, at 377

In many ways, these traits of electronic mail are, likewise, characteristic of the internet. Data is randomly, but efficiently, transferred between multiple routers and servers before arriving at a destination. "Anyone intercepting one of the packets en route to its recipient would be unable to decipher the complete message without the remainder of the packets."[16]

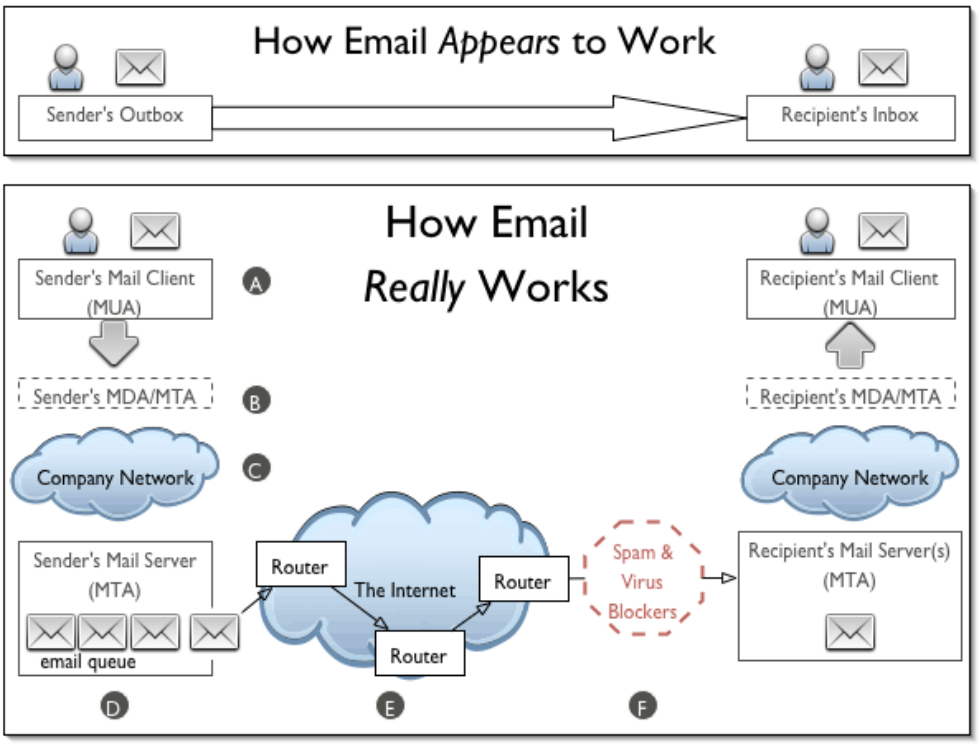

Figure 2: Diagram describing how e-mail travels between computers and networks.[17]

A useful analogy to this technology is driving. When traveling to a destination, there are often many different routes from which to choose. Despite some routes varying in duration and complexity, ultimately the driver will arrive at the predetermined destination and will usually

[16] David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 Geo. J. Legal Ethics 459, 464-69 (1998)
[17] See http://www.oasis-open.org/khelp/kmlm/user_help/html/images/howemailworks.png

have taken the most efficient route to get there. In contrast, however, to electronic data's ability to packetize, a driver and his vehicle cannot separate into multiple parts, travel concurrent routes simultaneously, and ultimately reassemble further down the road. This is a trait characteristic of the internet, known as "dynamic routing." When an e-mail is sent through the web, it's broken down into different, random packets. It's likely that no one part of the message will have traveled the exact same route to the destination.

Security Risks Associated with Electronic Mail Use

Commentators have referred to e-mail transmission as the electronic equivalent of a postcard.[18] Much like a misdirected postcard, electronic mail that is intentionally intercepted, or inadvertently sent to the wrong address, can be read by the unintended recipient. Additionally, like postcards, which can be read at any point in transit to their intended address, electronic mail transmissions are vulnerable en route to their destination.

Interception of an electronic message, in transit though, is certainly more fiction than fact. To accomplish the interception of an electronic message, all "packets" of transmitted data must be captured. This makes the actual transmission of electronic mail very difficult to intercept. Even if a would-be-criminal attempted to intercept a message sent from an electronic mail program, he likely wouldn't prove to be successful. The few packets that would be captured would only provide a few words or letters from the original message. Even simply being able to intercept an e-mail would be a difficult challenge in its own right. A hacker would have to know the exact location of where the message was departing from, where it was traveling

[18] Erik J. Heels, *Why Lawyers Should Get on the Internet: Research on and Legal Issues Raised by the Internet*, L. Prac. Mgmt., 25.

to, and in milliseconds be able to detect what specific journey between networks and routers the message was going to travel through. Considering the volume of electronic messages sent on a daily basis, the amount of data sent through any given network, and the minute timeframe, this may be an impossible task for any hacker to accomplish.

There is contention that this may not be true any longer. Whatever randomness was originally found in dynamic routing has diminished considerably as internet infrastructure has developed.[19] "From September to October, 1999, Joshua Masur, at the time a student at Columbia University, sent six different e-mail messages between his home computer and three remote computers and found little variety in the paths the messages took through the internet, much less variety than would be sufficient to provide security."[20] As the internet continues to grow and become increasingly standardized, e-mail which may have traveled a random route "might now take predictable, well-worn, and more easily monitored paths."[21] Predictable pathways, nonetheless, are always coupled with other issues like speed of transmission and the amount of data surrounding the transmission. It's unlikely the predictability of a message's route would substantially affect the ability to intercept the message.

A more realistic risk lies in administrative third-party access to e-mail messages. Due to the lack of many attorneys' technological expertise, it's a common practice for a network administrator to have omnipotent access to all computer accounts associated with a law firm. The administrator is able to make software changes, alter computer privileges, and access saved documents or information. The same is true for electronic mail accounts. When a technical error

[19] Rand, *supra* note 12.
[20] Masur, *supra* note 4, at 1147-48
[21] Rand, *supra* note 12, at 389.

occurs, the computer administrator is easily able to access the account and change settings, even remotely.

E-mails don't just travel though – they do eventually stop somewhere. This may be where the greater security risks are more of a concern. For beginners, most electronic mail account users are greeted with some sort of log-on screen. This is analogous to a gatekeeper. Only the individual with the information needed to access the account (usually a username and password) is able to gain entry. For the average user, this is usually sufficient to keep most anyone away. Lawyers beware: this is not the highest of security measures. Many people use simple, one or two word passwords. If we decide to be daring, we'll add some numbers, and maybe a symbol here or there. Overall, our passwords aren't too complicated. Unfortunately for those of us who rely on simple passwords, criminals and hackers are able to exploit our lack of password security and gain access to our accounts. Consider, too, how often most passwords are changed. Frequently, users will remain using the same password for extended periods of time. This increases the vulnerability of the account, as a hacker will have an extended period of time to decipher the account's password protection. Lastly, how many of the same e-mail accounts, online bank accounts, etc. use the same password? Is the same password for a social media network being used for banking information?

Chris Roosenraad, a leading computer industry expert in security and information technology, currently operates as the Director of Systems/Applications at Time Warner Cable, and the Vice Chair at the Messaging Anti-Abuse Working Group. He's formerly worked for a variety of internet and technology services companies, demonstrating a knowledgeable

commitment to the industry. Kindly, Mr. Roosenraad offered a wealth of valuable information concerning the topic of e-mail security in relation to this thesis.

Mr. Roosenraad identified several troubling features of electronic mail. First, he mentioned that there is a lack of password security for most e-mail users. He finds that the simplest way, overall, to gain unauthorized access to an electronic mail account "would be to get someone's password and hack into his mailbox."[22] While he expressed that the specific difficulty in doing so varies from situation to situation, he agreed it was very feasible and related it to a fault, not of technology, but of the "human being." Later, this concept will be discussed in more detail. Secondly, he identified a lack of sender verification. When an e-mail is transmitted to a recipient, there is no mechanism in place to verify the sender's identity. This poses a serious concern, as criminals and hackers are able to "spoof" e-mail identities and pretend to be someone, or something, they are not. If the recipient decides to reply, he may include private, confidential, or financial information to the false sender, resulting in clear harm. Finally, Mr. Roosenraad discussed e-mail messages' ability to be intercepted. Though he stressed intercepting messages is not a trivial task, it is always possible. In practice, however, there are much simpler ways to acquire information from an e-mail account in comparison to intercepting data. In his experience, he finds e-mail interception to be a rare occurrence. Interception he states is "difficult to do, and if you do something wrong while [intercepting information], chances are you just knocked something offline."[23] This, of course, would alert either the sender or recipient of the message to the presence of some sort of problem.

[22] Telephone Interview with Chris Roosenraad, Director of Systems/Applications, Time Warner Cable (Apr. 13, 2011).
[23] *Id.*

Mr. Roosenraad also addressed questions concerning the relative privacy of e-mail accounts and messages, as well as what are the best practices for lawyers utilizing electronic mail technology. When asked whether he, based on his expertise and experience, felt that there is a reasonable expectation of privacy in e-mail, he responded "No." He stated, "I know enough about how e-mail works to realize it's exposed to a lot of people behind the scenes. Now, most of those people don't care about your message, nor will read it, because they're decent people. The only way to keep that data private is to encrypt it."[24]

Overall, he concluded that the real issue isn't necessarily the technology, but the individual using it. He states that the "Achilles' heal [of technology] is the human being."[25] A very effective way to acquire information from a specific user is to socially engineer a method to do so. Mr. Roosenraad references the industry pseudonym for these attacks, called "spear-phishing". These attacks are very specific to one user. He describes why these attacks are so effective,

> It is such a tightly aimed message, that it's hard for anti-virus software to figure out. [The attack] may be completely transparent to the end recipient. It requires a fair bit of work, though. It's not something you're going to just do. However, [if] by seeing some of this information, you can make millions of dollars, then there's a strong incentive for you to do so.[26]

The recent technological attack on the Dallas-based online marketing firm, Epsilon, was mentioned as an example of a successful "spear-phishing" attack. By acquiring customer information, a hacker could spoof his appearance as a legitimate company, directing the recipient to navigate to a dangerous web-link.

---

[24] *Id.*
[25] *Id.*
[26] *Id.*

He does, however, disagree that technology has made the ability to acquire personal information, illegally, any easier. He states,

> It's not that technology makes this necessarily any easier; it just makes the methods of implementation different. What technology may make easier is the inadvertent "seeing" of the content by someone else. If you seal something inside an envelope, and then put that envelope inside a FedEx envelope, and then send that envelope to a law firm, someone has to go through a couple steps to actually see what the content is. If you just write out an e-mail and hit send, theoretically, an administrator on either side can read the message. They probably won't. They probably don't care. But technically, can they? Sure.[27]

The ability to inadvertently disclose information, electronically, is becoming increasingly less difficult.

In conclusion, Mr. Roosenraad explains criminal activity on the internet as a "chain of trust." He states, "The weakest link in the chain is most commonly the human being, at either end. The technology in between may allow you to do all these sneaky technical things, but it's probably going to be a lot simpler to go after one of the human beings in the equation."[28] He shared the following cartoon to visually describe his point:

[27] *Id.*
[28] *Id.*

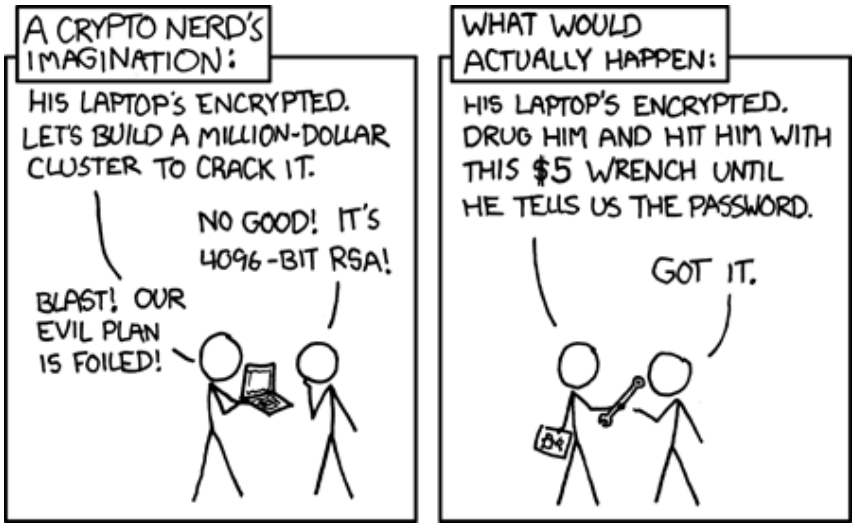

Figure 3: Cartoon demonstrating the technological, Achilles' heal.[29]

No-Encryption Standard

Encryption is an unfamiliar technology to many. The average computer user, or attorney, does not often utilize it. It operates by converting text, or other information, into unintelligible code during transmission.[30] The information is then decrypted once it reaches its destination, becoming intelligible to the recipient. It helps ensure confidentiality, and security, which standard transmissions cannot.

When e-mail first developed, encryption technology was not a commonly incorporated feature. During the period of rising e-mail popularity, encryption technology was cumbersome to use and expensive. "The two technologies had not developed at the same rate of speed, resulting in commercial applications of e-mail that far outpaced available encryption methods."[31]

[29] See http://www.xkcd.org/538/
[30] Ryan A. Murr, *Note, Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR, and Their Successors*, 34 San Diego L. Rev. 1401, 1405 (1997)
[31] Rand, *supra* note 12.

During the late 1990s, requiring attorneys to use encryption for attorney-client e-mails might have been viewed as an unnecessary and burdensome expense.

Today, encryption technology is a standard security measure used by many websites and online stores. Often, it's so simple to utilize, one may have failed to ever notice it. When traveling to an online banking portal or online store, the normal "http" has been replaced by an "https." HTTPS stands for "Hypertext Transfer Protocol Secure" and provides encryption of data transmitted to and from the website. When a user connects to a website via HTTPS, the website encrypts the session with a digital certificate. Digital certificates can be described as,

> …essentially a digital document that is issued by a trusted central authority and is used by the authority to validate a user's identity. Central, trusted authorities…are widely used on the internet to ensure that software from Microsoft, for example, is really from Microsoft, and not a virus in disguise.[32]

This approach is effective in preventing nefarious criminals from accessing sensitive information when it's being used to purchase an online product, for example.

Specifically encrypting electronic messages is more challenging, but very feasible. The additional protection encrypted e-mail messages provide would reasonably end any arguments regarding the dangers of electronic mail use. Even if a message, or any part or parts, were intercepted, the contents would be scrambled in unintelligible garble.

Generally, encrypted e-mail uses a lock-and-key approach. Both the sender and the recipient of a message must have access to the correct encryption key for the message to be decipherable. A common approach to this method is through the use of a public key. In a public key approach, there are two numeric program keys used: a private key and a public key. The sender of the message uses the public key. This key doesn't need to be closely guarded. With

[32] *Windows Server 2008: Unleashed*, 402 (2008)

the public key, the message is encrypted and sent to the recipient. The message can be intercepted or misdirected, but it is only accessible once it has been decrypted with the private key. The private key must be closely guarded and distributed in a secure fashion. The recipient with the private key is the only party that will be able to read the message.[33]

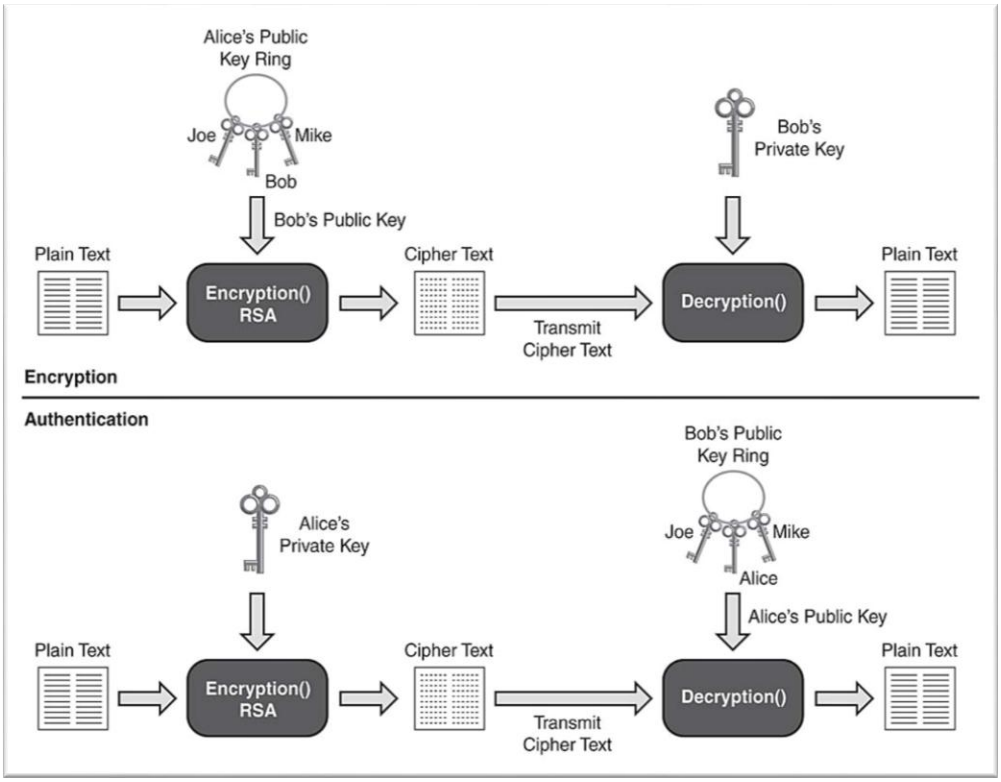

Figure 4: Diagram showing the public/private key encryption method.[34]

Applying this technology to a legal practice, a public key would be made available to a client. Any messages sent electronically to an attorney would be encrypted with the public key. The attorney would then decrypt the message with a private key, only available on the attorney's computer. This would ensure the confidentiality of all messages sent by the client and, even if

[33] *Id.*
[34] See http://www.networkworld.com/subnets/cisco/chapters/1587052423/graphics/02fig02.jpg

inadvertent disclosure did occur, would prevent messages from being read by unintended third parties.[35] When the attorney would transmit messages to a client, the use of the keys would alternate. The attorney would transmit the message, encrypting it with the public key. The client would receive the message, decrypting the message with the private key. For many reasons, including cost, lack of knowledge, or technological transition difficulties, the average attorney and legal practice does not utilize encryption standards in their electronic communications. In fact, because of the prevalence of older attorneys in today's practice, many may be unfamiliar altogether with the fundamental ideals of message encryption via computerized methods. This poses a great challenge when trying to make a fundamental shift in safer practices of communication mediums.

Document Transmission and Attachments

Electronic mail has the ability to transmit documents, in addition to the text of the original e-mail message. These documents are commonly referred to, and known as, electronic "attachments." When first developed, attachments were limited to simple text files and small pictures, those that are often created by document word processors or unsophisticated computer programs. The amount of data, which could be transmitted, was also restricted. This was due, in part, to the overall power and speed of computers, as well as the larger networking capabilities and infrastructure. As computers have gained the ability to process larger quantities of information, faster, and have acquired speedier connections to the internet, the limit on attachments has diminished substantially. A user can convey a word processing document as easily as a reasonably sized video file.

[35] *Id.* at 401

Overall, the use of attachments doesn't seem to pose any more or less of a risk, than e-mail messages, standalone, except in regards to metadata (a more comprehensive discussion on metadata will occur later in this thesis). Attached documents are equally likely to contain sensitive information an attorney wouldn't care to disclose to other parties. Such examples include drafted motions, memorandums, or case strategies. Accidentally communicating this information to the wrong parties may result in disastrous consequences, as would a confidential message to a client. Attorneys should exercise great discretion in what documents are sent by electronic mail. Unintentionally sending the document, by electronic message, to the wrong parties may result in severe consequences, both in practice and in legal consequences.

CHAPTER THREE: THE ATTORNEY-CLIENT PRIVILEGE

Before a discussion can take place, however, regarding the role of the attorney-client privilege and its relationship to e-mail, one must first ascertain a foundational understanding of the attorney-client privilege. The attorney client privilege has roots deep in history. "Of the now existing common law privileges, the attorney-client privilege is the oldest."[36] Historically, the privilege has been traced as far back as the Romans, where "attorneys were servants of those whose affairs they managed and under Roman law, could not testify for or against their masters since the relationship created a duty of loyalty."[37] This foundation in Roman law led to the later development and recognition of the attorney-client privilege throughout history. During the sovereignty of Queen Elizabeth I, English common law recognized a special relationship

[36] Sean M. O'Brien, *Extending the Attorney-Client Privilege: Do Internet E-Mail Communications Warrant a Reasonable Expectation of Privacy?*, 4 Suffolk J. Trial & App. Adv. 187, 193 (1999)
[37] Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B. U. J. Sci. & Tech. L. 1, 3-4 (2010).

between an attorney and client."[38] This relationship noted relative confidentiality in communications between attorney and client, as well as the importance for the client to be able to speak trustingly and honestly to his lawyer.

The United States Supreme Court formally recognized the attorney-client privilege in 1888.[39] Since that time, "most states have incorporated the attorney-client privilege into their evidence code and at least twenty state legislatures have codified the privilege."[40] At the federal level, the attorney-client privilege has been written into the Federal Rules of Evidence.[41] Today, the common law privilege has been expanded and is generally defined as:

> Where legal advice of any kind is sought from a professional legal advisor in his capacity as such, the communications relating to that purpose, made in confidence, by the client, are at his instance permanently protected from disclosure by himself or by the legal advisor, except the protection may be waived.[42]

Most jurisdictions' codification of the attorney-client privilege by statute[43] recognizes the modern purpose of the privilege. The statutes serve to promote the open conversation and free exchange of information between an attorney and client.[44] This exchange of information allows attorneys to establish rapport with their clients and build an open environment for case discussion and resolution. In a secondary and related purpose, these open and honest communications also allow for counsel to adequately prepare for litigation.[45] This enables the attorney to explore all possible defenses or legal remedies available to the client. In summary,

---

[38] Stephens, Jr., *supra* note 3, at 1011.
[39] *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888).
[40] O'Brien, *supra* note 36, at 193-194.
[41] Fed. R. Evid. 501.
[42] Masur *supra* note 4, at 1121.
[43] William P. Matthews, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 Kan. L. Rev. 273, 280 (1996).
[44] Hill, *supra* note 37, at 4.
[45] Charles W. Ehrhardt, *Florida Evidence*, 356 (2007)

courts have repeatedly recognized that the privilege granted to communications between an attorney and client is of special legal importance and that "…great care must be taken to ensure that the attorney-client privilege remains preserved."[46]

A Study of the Attorney-Client Privilege

Clients speak with their attorneys in many fashions. A client may meet with their attorney in person, communicate with him telephonically, or send messages by fax, mail, or e-mail. The communications consists of both oral and written communications. The law recognizes that both oral and written communications deserve protection under the attorney-client privilege.[47] Even physical actions, made by the client in order to convey meaning, can receive these same protections.[48] The privilege has broad authority in protecting many different mediums of communications between an attorney and his client.

Under original common law concepts, the attorney-client privilege protected only those communications originating from the client and directed to the attorney. Today, communications between an attorney and client as a whole, as well as communications among paralegals, employees of the attorney, and experts hired for case preparation, all share the protections of the privilege.[49] The privilege is interpreted in a broad sense. It protects communications made by individuals acting under the direction of an attorney, unless those communications are specifically waived.

Florida Statute § 90.502 "…codifies the attorney client privilege and generally provides that neither an attorney, nor a client, may be compelled to divulge confidential communications

[46] Stephens, Jr., *supra* note 3, at 1017
[47] See *Johnston v. State*, 497 So. 2d 863 (Fla. 1986); see also *Anderson v. State*, 297 So. 2d 871 (Fla. 2d DCA 1974)
[48] See *Keir v. State*, 11 So. 2d 886 (Fla. 1943)
[49] FLA. STAT. § 90.502(1)(c)(1) (2011)

between a lawyer and client which were made during the rendition of legal services."[50] This remains consistent with, and adopts the philosophy of, both the common law and modern interpretation of the privilege. Furthermore, the attorney-client privilege is an absolute privilege, meaning that the "privilege is not subject to any balancing test and cannot be discovered by a showing of need, undue hardship, or some other competing interest."[51] However, the "burden of establishing that a communication is protected by the attorney-client privilege is upon the party asserting it."[52]

One important concept relating to the attorney client privilege is that of waiver. "The most common waiver of a privilege occurs by voluntary disclosure of the protected communication."[53] For example, if a client voluntarily disclosed confidential information to an acquaintance, and it was later discovered by opposing counsel, or the court, that this disclosure occurred, the legal protections of the attorney-client privilege for the confidential information communicated may no longer apply. Waiver of the attorney-client privilege eliminates the protected nature of the communication between the attorney and client. This voluntary disclosure can affect the entirety of the communication or "…any significant part of the matter or communication."[54] Simply referring to a particular subject matter of a conversation may also constitute waiver.

---

[50] Ehrhardt, *supra* note 45, at 359; see also FLA. STAT. § 90.502 (2011)
[51] Ehrhardt, *supra* note 45, at 357; see also *National Sec. Fire & Cas. Co. v. Dunn*, 705 So. 2d 605, 608 (Fla. 5th DCA 1997).
[52] Ehrhardt, *supra* note 45, at 357; see also *Leithauser v. Harrison*, 168 So. 2d 95 (Fla. 2d DCA 1964); *Nationwide Mut. Fire Ins. Co. v. Harmon*, 580 So. 2d 192, 192-193 (Fla. 4th DCA 1991).
[53] The Florida Bar, *Evidence in Florida*, p. 4-8 (2002); see also *St. Paul Fire & Insurance Co. v. Welsh*, 501 So. 2d 54 (Fla. 4th DCA 1987).
[54] *Id.*; see also FLA. STAT. § 90.507 (2011)

If the communication, however, is "…by a client to a person assisting a lawyer in the rendition of the professional services, [then] no waiver occurs."[55] This occurs frequently as attorneys will often have their clients seek out the services and assistance of various experts. This assistance may occur during trial preparation, or, as part of the information needed to adequately render a legal opinion. For example, a certified paralegal will often assist a lawyer by preparing case documents and gathering information from the client. The 'disclosure' of client and case information to the paralegal would remain within the protections of the attorney-client privilege.

A waiver of the privilege can also be made in the more traditional sense of the word "waiver". If the client, through written documentation, agrees to allow communications to be relayed to third parties, the agreement will constitute as a waiver.[56] It's worth noting that there are other exceptions, similar to the attorney-client privilege. Some of these include the work product privilege, husband-wife privilege, accountant-client privilege, etc. This thesis is only concerned with the concept of waiver in relation to the attorney-client privilege.

An attorney cannot waive the privilege on behalf of his client.[57] In *Smith v. Armour Pharmaceutical Co.*, the defendant's attorney inadvertently disclosed a memorandum. Although the document was widely circulated (and published in several newspapers), the United States Southern District Court of Florida held that the document and client retained the legal protections of the attorney-client privilege. The court found that,

---

[55] Ehrhardt, *supra* note 45, at 395; see also *International Tel. & Tel. Corp. v. United Tel. Co. of Florida*, 60 F.R.D. 117 (M.D. Fla. 1973).
[56] The Florida Bar, *Evidence in Florida*, p. 4-8 (2002); see also *Saenz v. Alexander*, 584 So. 2d 1061 (Fla. 1st DCA 1991).
[57] *Schetter v. Schetter*, 239 So. 2d 51, 52 (Fla. 4th DCA 1970).

> …[T]he contents of the document are no longer confidential is different from ruling that, in legal terms, the client holding the privilege has lost the privilege because someone else disclosed the document to the public. In Florida, for a privileged document to lose that status, it must be found that [the client] intentionally waived his rights.[58]

The *Smith* court also cited *Georgetown Manor, Inc. v. Ethan Allen, Inc*., in its opinion, quoting "Although confidentiality can never be restored to a document already disclosed, a court can repair much of the damage done by [the] disclosure by preventing or restricting the use of the document at trial."[59] This once again reaffirmed the legal position that a client retains the right to disclose, or not disclose, confidential information. It also acknowledged that while information may be circulated to the client's detriment, there are remedies in the courtroom to help assist the client in retaining whatever legal protections remain.

At the end of the *Smith* opinion, the court makes one final analogy that is useful in understanding the Florida courts' philosophy in allowing a client to be the only individual to waive the privilege:

> …[W]hat if a confidential memorandum is stolen from an attorney's office and subsequently published in newspapers across the country? Clearly, the client should not be held to have waived the attorney-client privilege. The fact that the contents of a privileged document have become widely known is insufficient by itself to eliminate the privilege that covers the document. Although in practical terms the document has lost any semblance of confidentiality, the court in legal terms must recognize that the client has not intentionally waived the privilege. The law is clear; it is only the client who has the power to waive the attorney-client privilege. To hold that public circulation eliminates the privilege would, in effect, give any individual who secured a privileged document the power to waive the attorney-client privilege by simply having the contents widely recounted in newspaper reports.[60]

---

[58] *Smith v. Armour Pharmaceutical Co*., 838 F. Supp. 1573, 1575 (S.D. Fla. 1993).
[59] *Georgetown Manor, Inc. v. Ethan Allen, Inc*., 753 F. Supp. 936, 938 (S.D. Fla. 1991).
[60] *Smith v. Armour*, *supra* note 58, at 1577

These cases, as well as the current view of the law, sufficiently demonstrate that the client is the sole bearer of the rights to the privilege. While documents or conversations may lose any sense of confidentiality in the public sphere, as in the example of the *Smith* case, the client still maintains the legal right to exercise the protections of the attorney-client privilege. The attorney, or another, cannot waive the client's legal rights to the attorney-client privilege, since he is not the holder of the privilege.

It's important to address the expectation of privacy in relation to the attorney-client privilege and waiver. The general rule is that testimony of a third party who overhears a confidential communication is admissible.[61] However, a client does not waive the protections of the privilege if, for example, an "…unknown eavesdropper overhears the communication [which was] intended to be confidential."[62] As evidenced in the cases below, the Florida courts have held that if a reasonable expectation of privacy did not exist, or attorneys and their clients should have reasonably known an expectation of privacy did not exist in their communications, then the communication is no longer protected by the privilege.

In *Mobley v. State*, defendant Autley Mobley argued that the "…trial court erred in limiting one of the defense counsel's cross examination of a State witness, Charles Bargman."[63] Mobley was attempting to elicit testimony made during a conversation between Bargman and his attorney inside a holding cell at the jail. Bargman testified that at the jail, the conversation he had with his attorney was "…strictly business and that he intended it to be confidential."[64] However, "…he conceded that he knew his conversation could be overheard by another inmate

[61] John Wigmore, *Wigmore on Evidence, Vol. VIII*, s2336 (1961)
[62] The Florida Bar, *Evidence in Florida*, p. 4-8 (2002)
[63] *Mobley v. State*, 409 So. 2d 1031, 1037-38 (Fla. 1982)
[64] *Id.* at 1038.

in the holding cell."[65] The Florida Supreme Court found that Bargman was capable of preventing his conversations from being overheard by using a private room in the jail. The court states,

> In the absence of any evidence that Bargman was purposely prevented from conferring with his attorney in private, we find he was capable of preventing others from overhearing his conversation with his lawyer. His failure to do so precludes him from asserting the attorney-client privilege. Therefore, the [trial] court had no basis for limiting appellant's sixth amendment right to confront their accusers.[66]

The decision in *Mobley* demonstrates that conversations of a client and attorney must afford a reasonable expectation of privacy. If, intentionally, conversations occur in an arena where the expectation of privacy is uncertain or clearly lacking, it will result in a waiver of the attorney-client privilege. The communication has been conveyed to a third party, thereby terminating the protections of the privilege.

Departing momentarily from the attorney-client privilege, while remaining within the realm of privileged communications, the earlier Florida Supreme Court in *Proffitt v. State*, dealt with a similar situation. In *Proffitt*, a third party overheard spoken conversations between a husband and wife. The court was asked to determine, specifically, whether the appellant, or his wife, should have known that their privileged communications were being overheard. The court found that it was readily discernable that the appellant and wife were aware of the third party's presence in their home and were not attempting to keep their voices at a level that could not be heard by others. The court finds,

> There is absolutely no testimony indicating that either the appellant or his wife made any attempt, no matter how little, to keep the conversation from being

[65] *Id.*
[66] *Id.*

> overheard. It is further clear from the testimony that conversations were readily discernible in other rooms and the appellant either knew or should have known that he was going to be overheard if he was speaking over a whisper. Therefore, the privileged character of the communication was lost when they were speaking in a manner and place where they had a reasonable chance of being overheard, and they knew of that possibility at that time.[67]

This finding reaffirms the decision of *Mobley*. In order for a conversation (or communication) to remain protected by the attorney-client privilege, there must be a reasonable expectation of privacy within the conversation. Speaking loudly, or in a public location, where a third party could reasonably overhear the substance of the communications constitutes a voluntary waiver of the legal protections of the privilege.

These cases present conclusions, which, are of special legal significance in Florida. First, the client will always be the bearer of the privilege. Attorney error or misconduct may occur in a case, harming the client, but ultimately the client will be afforded the legal protections of the attorney-client privilege if he did not voluntarily disclose confidential communications. Second, the case law establishes the important principle that one must have a reasonable expectation of privacy in his communications in order to be granted attorney-client privilege protection. As evidenced in the facts above, if one communicates information, where he knows or reasonably should know his communications are being overheard, those conversations will not be protected.

In relating these findings to the subject of this thesis, the latter poses significant concerns when studying the attorney-client privilege in relation to electronic mail use. Are electronic communications private? When information is communicated through the web, does the user know, or reasonably should he know, that the communication is being 'overheard' by a third party? How 'transparent' is electronic data sent through an electronic mail account? If in fact,

[67] See *Proffitt v. State*, 315 So. 2d 461 (Fla. 1975)

through further analysis, this thesis finds that there is not a reasonable expectation of privacy in electronic mail, confidential communications sent by this medium will not be afforded legal protection under this doctrine. In the next chapter, this thesis will discuss whether a reasonable expectation of privacy has been explicitly granted to e-mail communications, or if implicitly, a court could infer a reasonable expectation of privacy exists.

CHAPTER FOUR: EXPECTATION OF PRIVACY

Privacy has always been a very highly valued part of the American life and law. The Constitution of the United States is the primary source to protect the right to privacy. The Fourth Amendment of the Constitution establishes,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[68]

The framers of the Constitution wanted protection from unannounced, unwarranted invasions of their homes (as they had been subject to during British occupation). Since that time, the Fourth Amendment has continued to serve as the original and primary source establishing a form of privacy. Below, this thesis will analyze privacy in the contexts of the federal jurisdiction.

In a modern era, a debate ensued regarding how the Fourth Amendment affected searches of electronic mediums. The first notable case is *Olmstead v. United States*. During the National Prohibition Act, Roy Olmstead was convicted for unlawfully possessing, transporting, and selling alcohol. Evidence of Olmstead's involvement, and the larger conspiracy to sell and

[68] U.S. CONST. AMEND. IV

purchase alcohol, was gathered by four federal prohibition officers. Officers placed wiretaps along the telephone wires of Olmstead's residence and the large office building within which Olmstead worked. No trespasses were made to the defendant's property to place the wiretaps. Olmstead appealed the decisions of the lower federal courts on the basis that the evidence obtained by the federal officers was done so in violation of the Fourth Amendment of the U.S. Constitution. The Supreme Court held that the Fourth Amendment described searches "…of material things-the person, the house, his papers, or his effects."[69] It ultimately upheld Olmstead's conviction citing that "…the language of the [Fourth] amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[70]

The Supreme Court has since overturned the Olmstead doctrine. Though this case did not find a reasonable expectation of privacy to exist in telephonic communications, other cases afterwards established a fundamental expectation of privacy when communicating by telephone. It remains significant for being one of the first decisions to consider this issue.

After the Supreme Court's decision in the Olmstead case, Congress enacted the Federal Communications Act in 1934, forbidding anyone, unless authorized by the sender, to intercept a telephone message and directed that "no person" shall divulge or publish the message or its substance to "any person." It also barred testimony of federal agents concerning the substance of a defendant's interstate communications overheard by agents who had intercepted messages by

[69] *Olmstead v. U.S.*, 277 U.S. 438, 464 (1928)
[70] *Id.* at 465

tapping telephone wires. This legislation accepted the importance of recognizing a legal right to privacy in telephone conversations.

The Supreme Court, in *Nardone v. United States*, reaffirmed the restrictions created by Congress. Frank Nardone was indicted for the possession and distribution of alcohol. The original conviction was based on evidence obtained through telephone wiretapping by federal agents. In its review, the Supreme Court found that, except when sanctioned by a judge, no person could intercept a communication and subsequently disclose the contents of that communication. The Court held that the broad definition of the Act, stating "no person," prevented even federal agents from wiretapping telephone lines without a court-ordered subpoena.[71] The majority upheld the provisions of the Communications Act of 1934 by reversing and remanding the conviction of Frank Nardone. *Nardone* differs greatly from the decision in the *Olmstead* case. It affirmed that governments could not access communications to which they were not privy, establishing a reasonable expectation of privacy in telephone conversations.

In 1942, the Supreme Court encountered the first case involving electronic communication interception through a medium other than telephone lines. In *Goldman v. United States*, federal agents installed a listening apparatus in the wall adjacent to the office of defendant, Martin Goldman. The listening device was connected to earphones, but failed to operate correctly. The agents instead used a detectaphone, which when placed against Goldman's wall, could amplify the conversations emanating from inside. A stenographer recorded the conversations, which were later used as evidence against Goldman. The Supreme

[71] *Nardone v. U.S.*, 302 U.S. 379, 381 (1937)

Court found that the actions of the federal agents were not in violation of the Fourth Amendment, or the Communications Act of 1934.[72] They equated the use of the detectaphone to the actions of the federal agents in the Olmstead case. Most importantly, however, the Court, whether intentionally or unintentionally, overruled the rationale of Olmstead on the premise that conversations could not be seized.

In *Katz v. United States*, the Supreme Court issued one of the most important opinions to develop a right to privacy in electronic communication. Charles Katz was convicted of transmitting wagering information by telephone from Los Angeles, to Miami and Boston, in violation of a federal statute. Federal Bureau of Investigation agents were able to obtain the conversations made by Katz by attaching an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. The lower Court of Appeals affirmed Katz conviction, rejecting the position that there had been a violation of the Fourth Amendment, because "there was no physical entrance into the area occupied by the petitioner."[73] The *Katz* Court disagreed, holding,

> We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.[74]

Katz also established an important two-part test in determining whether a particular communication merits a reasonable degree of privacy:

---

[72] *Goldman v. U.S.*, 316 U.S. 129, 135 (1942)
[73] *Katz v. U.S.*, 389 U.S. 347, 348 (1967)
[74] *Id.* at 353

> …first that a person must 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 had 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.[75]

Katz remains as one of the most important cases for determining whether there is an expectation of privacy in any mode of communication. Its two-part test stands as a measure of reasonable privacy expectations in the home. It notes two important aspects of privacy: first, there must be a genuine expectation of privacy by the person asserting it, and second, it must be reasonable by societal norms. However, the Supreme Court failed to recognize what standard of society would be applied to this definition. Did it intend to define "society" as those people belonging to an individual city, state, or nation? Or, did the Court intend to define society as that which is within the jurisdiction of a court? In regards to electronic mail, this may pose a challenge, as electronic mail is a means of global communication.

During the same year, the Supreme Court also issued an opinion in *Berger v. State of N.Y.* In *Berger*, the Supreme Court held that the Fourth Amendment had been violated when a New York statute permitted New York State court judges to issue warrants for eavesdropping without proper judicial oversight. Justice Clark, in the majority opinion, cited *Lopez v. United States*, stating "…the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments."[76] The Berger

[75] *Id.* at 361
[76] *Lopez v. U.S.*, 373 U.S. 427, 441 (1963)

decision placed special emphasis on the potential for abuse of electronic surveillance equipment to overhear private conversations. The Justices also pointedly disagreed with law enforcement's claim that the ability to fight crime would be hindered by forbidding the use of eavesdropping equipment without probable cause. The Berger Court writes:

> …it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that without the use of such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and-what is more important-without attending illegality.[77]

The Court granted further protections to conversations and expanded the right to privacy once more.

In *The People v. Gregory Diaz*, the Supreme Court of California, on January 3rd, 2011, issued a divisive opinion regarding whether the Fourth Amendment to the United States Constitution permits law enforcement officers to conduct a warrantless search of a defendant's cell phone's text message folder, incident to a lawful arrest. Defendant, and appellant, Gregory Diaz, was involved in a controlled purchase of Ecstasy. A police informant, wired to transmit the defendant's conversations, purchased Ecstasy from a seller in the backseat of the defendant's vehicle. Shortly thereafter, the defendant was stopped and arrested for being a coconspirator in the sale of controlled substances. Ecstasy, marijuana, and a cell phone were seized from the defendant's person. The defendant was transferred to a police station.

There, Mr. Diaz was questioned regarding the drug transaction, in which he denied having any knowledge. After the interview, the arresting officer looked at the defendant's cell

[77] *Berger v. State of N.Y.*, 388 U.S. 41, 63 (1967)

phone's text message folder and discovered a message, which, according to the officer's training and experience, described the sale of Ecstasy. The police officer confronted the defendant regarding the message, thereafter prompting the defendant to admit his involvement in the sale.

The defendant asserted to the California Supreme Court, that although law enforcement is legally permitted to conduct an immediate search of a person following an arrest (as is found in *United States v. Chadwick*, 433 U.S. 1 (1977*), United States v. Robinson*, 414 U.S. 218 (1973), and *United States v. Edwards* 415 U.S. 800 (1974)), the "character" of a cell phone is not the equivalent of items traditionally seized by officers. The defendant argued that cell phones "contain quantities of personal data unrivaled by any conventional item of evidence traditionally considered to be 'immediately associated with the person of the arrestee,' such as an article of clothing, a wallet, or a crumpled cigarette box found in an arrestee's pocket," and, therefore, implicate heightened "privacy concerns."[78]

The majority of the *Diaz* court rejected the defendant's view that the validity of a warrantless search depends on the character of the searched item. The California Supreme Court cites *United States v. Ross*, stating,

> [A] constitutional distinction between 'worthy' and 'unworthy' containers would be improper. Even though such a distinction perhaps could evolve in a series of cases in which paper bags, locked trunks, lunch buckets, and orange crates were placed on one side of the line or the other, the central purpose of the Fourth Amendment forecloses such a distinction.[79]

The court also agreed with the decision in *New York v. Belton*, finding that whether or not a container can be searched does not depend on the arrestee's reasonable expectation of privacy in that container.

[78] *The People v. Diaz*, 51 Cal.4th 84, 94 (Cal. 2011)
[79] *United States v. Ross*, 456 U.S. 798, 825 (1982)

> [A]ny container…[in] the passenger compartment…may…be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.[80]

Lastly, the court found the defendant's argument unpersuasive that a cell phone's ability to store large amounts of personal data should be determinative. The court writes, "Even 'small spatial containers' that hold less information than cell phones may contain highly personal, intimate, and private information, such as photographs, letters, or diaries."[81]

The December 2010 decision of the United States Sixth Circuit Court of Appeals in *United States v. Warshak* now serves as the most important case affecting electronic mail and privacy. In 2001, Steven Warshak owned a number of companies selling herbal supplements. One of those was a company that sold herbal supplements targeted at 'male enhancement'. During several years of sales, Warshak and his employees engaged in questionable financial tactics, often fraudulently reporting credit card sales and customer information. In conjunction with a criminal investigation, the government seized roughly 27,000 private e-mails from Warshak's Internet Service Provider. From a culmination of evidence, including the e-mails acquired from law enforcement, Warshak was sentenced to prison and ordered to pay substantial fines.

Warshak appealed the conviction, arguing that the government did not have a warrant to acquire his private, e-mail messages. He argues that the government's warrantless seizure of his private e-mails is a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures. In its review of decisions like *Katz* and *Smith*, the Court of Appeals found that e-

[80] See *New York v. Belton*, 453 U.S. 454 (1981).
[81] *The People v. Diaz*, *supra* note 78, at 96.

mail accounts are afforded a reasonable expectation of privacy, analogous to those expectations found when communicating by telephone or through postal mail. The court writes,

> Given the fundamental similarities between e-mail and traditional forms of communication, it would defy common sense to afford e-mails lesser Fourth Amendment protection…As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call-unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP [Internet Service Provider] to surrender the contents of a subscriber's e-mails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.[82]

In summary, the *Warshak* case is the first to directly address whether an expectation of privacy exists in electronic mail communications. It sufficiently establishes a reasonable expectation of privacy in e-mail activity.

In summary, the cases presented here are binding on the federal judiciary, while some are further limited to an individual circuit (as evidenced by *Warshak*). Because this thesis is focused specifically on Florida courts, it's important to reaffirm that these federal cases are for reference, and persuasive, uses only. Florida courts will retain their discretion to adopt, or reject, the legal principles of the federal judiciary.

Whether an expectation of privacy is present plays a crucial role in determining whether the attorney-client privilege exists. "The privilege only extends to communications intended to remain confidential that are made under circumstances where a reasonable expectation of privacy exists."[83] If Florida judges adopted the two-part test, as described in *Katz,* or adopted the finding in the *Warshak* case, it is likely that a reasonable expectation of privacy would be

[82] *United States v. Warshak*, 631 F.3d 266, 285-286 (6th Cir. 2010)
[83] Sean M. O'Brien, *Extending the Attorney-Client Privilege: Do Internet E-Mail Communications Warrant A Reasonable Expectation of Privacy?,* 4 Suffolk J. Trial & App. Adv. 187, 192 (1999)

afforded to electronic mail communications between attorneys and their clients. This would permit attorneys to communicate electronically more comfortably, with less concern for the legal repercussions doing so.

CHAPTER FIVE: INADVERTENT DISCLOSURE

Courts drastically differ on their opinions and rationale regarding inadvertent disclosure of documents or information. In today's world of complex litigation and exchange of information cross-nationally or internationally, considerations by lawyers should be made with respect to how other jurisdictions view an attorney's request to keep inadvertently disclosed documents confidential. In many cases, lawyers will deal with clients and/or opposing counsel across state lines. Jurisdictions widely vary in their legal approach. This thesis has identified three main approaches: automatic waiver of the attorney-client privilege, whether the client intended to waive the attorney-client privilege, and a balancing test approach.

Automatic Waiver of the Attorney-Client Privilege

Some jurisdictions adopt the principle that one cannot un-ring a bell. This theory is rooted in the belief that if a confidential document is produced, even inadvertently, to another party outside of the intended communication, the veil of confidentiality is removed and the document is no longer confidential.

In *Federal Deposit Insurance Corporation v. Singh*, 140 F.R.D. 252 (D. Me. 1992), the United States District Court in Maine considered the inadvertent disclosure of a document sent by facsimile. The case facts describe a secretary, who in preparation for discovery removed all copies of a memorandum that was not to be submitted to opposing counsel. Accidentally,

however, the secretary faxed a copy of this privileged memorandum to opposing counsel when submitting other documents by facsimile. The plaintiff's attorney objected to its use in trial, on the legal grounds that the document was protected by the attorney-client privilege and work product immunity.

To the plaintiff's detriment, the District Court disagreed. The court held, and adopted the belief, that inadvertent disclosure does constitute a waiver because the privilege applies only to confidential communications. After disclosure, the information cannot be deemed confidential, regardless of the party's intentions. Citing the case, Chief Judge Gene Carter writes, "Once persons not within the ambit of the confidential relationship have knowledge of the communication, that knowledge cannot be undone. One cannot "un-ring" a bell."[84] Despite the plaintiff producing the document inadvertently to opposing counsel, the attorney-client privilege was waived when opposing counsel reviewed it.

In a similar approach, the United States District Court for the District of Columbia held in *Underwater Storage, Inc. v. United States Rubber Co.*, 314 F. Supp. 546 (D.D.C. 1970), that a letter, inadvertently disclosed, did not maintain attorney-client protections. In this case, a letter was inadvertently sent between the parties, which described patent solicitation services performed by the plaintiff's attorney. During deposition, the attorney, furthermore, refused to answer questions pertaining to the letter, arguing the document was subject to the protections of the attorney-client privilege. The court took a hardline approach to the argument. It found that it would not consider the intentions of the party producing the document as a test for confidentiality. It also did not attribute the inadvertent disclosure as chargeable to the client. In

[84] *Federal Deposit Insurance Corporation v. Singh*, 140 F.R.D. 252, 253 (D. Me. 1992)

a strict view of the attorney-client privilege, the court writes, "Once the document was produced for inspection, it entered the public domain. Its confidentiality was breached thereby destroying the basis for the continued existence of the privilege."[85] In this holding, it seems that any document or confidential material, if disclosed by a party intending to keep the information confidential, is subject to review if inadvertent disclosure occurs. This stern approach may be severely damaging to clients and attorneys, alike.

Again, a United States District Court, this time in Oklahoma, was faced with the question of whether inadvertent disclosure of documents abrogated the right of confidentiality under the attorney-client privilege. In *W.R. Grace & Co. v. Pullman, Inc.*, 446 F. Supp. 771 (W.D. Okla. 1976), an attorney inadvertently provided documents to opposing counsel during the production of documents. Despite the court ordering that many of the documents weren't subject to the protections of the attorney-client privilege, they found that the act of the defendant voluntarily producing documents to opposing counsel was sufficient to waive the privilege, regardless.[86]

Under this theory, lawyers and clients have few options in regard to the confidentiality of documents, which are produced inadvertently. These jurisdictions agree: the protection and confidentiality of a document is irrevocably breached upon its disclosure. In this bright-line approach to the confidentiality of documents, attorneys will be unable to convince a court to limit the use of documents that are produced accidentally. Applying this approach to modern habits of attorneys, it's very possible that a misplaced e-mail, disclosing litigation strategies or confidential documents, would enter the public domain for review.

[85] *Underwater Storage, Inc. v. U.S. Rubber Co.*, 314 F. Supp. 546, 549 (D.D.C. 1970)
[86] See *W.R. Grace & Co. v. Pullman, Inc.*, 446 F. Supp. 771 (W.D. Okla. 1976)

Client's Intent – Waiver of the Attorney Client Privilege

In contrast to the view of the jurisdictions above, some jurisdictions are not as strict when inadvertent disclosure occurs. Instead of a strict approach, whereby if disclosure occurs at all a document enters the public domain, some courts reason that inadvertent disclosure by an attorney, or his employees, does not necessarily warrant an automatic disregard for the attorney-client privilege. These jurisdictions find that the attorney-client privilege rests not with the attorney, but with the client. In this analysis, accidental disclosure by the attorney does not waive the client's right to the protections of the privilege.

The Superior Court of New Jersey, Law Division, in *Trilogy Communications, Inc. v. Excom Realty, Inc.*, 279 N.J. Super. 442 (Law Div. 1994), reviewed the inadvertent disclosure of a memorandum. The memo was purported to be confidential and was prepared for submission to Trilogy Communications, Inc. Prior to its submission, however, it was to be sent for review to a member of the defendant's general counsel. Before review of the document occurred, it was inadvertently sent, unsigned, to the plaintiff, Trilogy Communications, Inc. along with 5,500 other documents during a discovery request. Excom Reality, Inc. objected to its use in trial, claiming the document was confidential and intended to remain confidential under the attorney-client privilege.

The Superior Court of New Jersey, Law Division, held that the inadvertent disclosure of the document did not constitute a waiver of the attorney-client privilege. It rejected the old view of *Wigmore on Evidence*, which aligns with the view of the jurisdictions mentioned in the prior section, that the privilege is destroyed by any involuntary disclosure, including a mistaken one.[87]

[87] See *Trilogy Communications, Inc. v. Excom Realty, Inc.*, 279 N.J. Super. 442, 444 (Law Div. 1994)

Basing its decision in a more modern context, the court held that for important public policy reasons, and based on the legal principle that waiver imports the intentional relinquishment or abandonment of a known right[88], that the party charged with the waiver must have deliberately intended to relinquish it. Therefore, disclosure, which is accidental or inadvertent, does not necessarily permit the disclosure to be used by the opposing party for review, or at trial.

Other cases have similarly placed emphasis on the client's intent to waive his right to the attorney-client privilege and the confidentiality of documents. In a similar finding, the United States District Court, of the Northern District of Illinois, in *Mendenhall v. Barber-Greene Co.*, 531 F. Supp. 951 (N.D. Ill. 1982) held "…if we are serious about the attorney-client privilege and its relation to the client's welfare, we should require more than such negligence by counsel before the client can be deemed to have given up the privilege."[89] As the *Trilogy* case did, it too rejected the old, Wigmore strict responsibility doctrine, which would automatically allow for a document's review despite unintended disclosure.

While these cases emphasize the 'innocent client' and provide greater client protections, despite attorney negligence, disclosure can still have tremendously devastating effects. If, for example, a document submitted to an opposing party contained negotiation or litigation strategies, the consequences may be insurmountable. Yet, whereas the first grouping of cases did not provide any legal remedy for attorneys faced with inadvertently disclosed documents, these jurisdictions recognize a legal remedy for such accidental disclosure.

[88] Id. at 447
[89] See *Mendenhall v. Barber-Greene Co.*, 531 F. Supp. 951, 955 (N.D. Ill. 1982)

A Balancing Test

The third analysis commonly used by court systems is that of a balancing test. The courts weigh whether the inadvertent disclosure of a document, or information, will suffice as a valid waiver of the privilege based on the circumstances surrounding the disclosure. In this view, some jurisdictions have established tests to determine the effect of inadvertent disclosure on waivers.

The case of *Suburban Sew 'N Sweep Inc. v. Swiss Bernina, Inc*., 91 F.R.D. 254 (N.D. Ill. 1981), is a good example of the some courts' ability to weigh many factors in determining the effect of inadvertent disclosure on waiver. In this case, the plaintiffs suspected that the defendant was engaging in unlawful price discrimination and conspiring to restrain trade in violation of the Clayton Act and Sherman Antitrust Act. Attempting to substantiate their claims against the defendant, the plaintiffs began the practice of searching through the dumpster located behind the defendant's office complex. For nearly two years, this practice continued and resulted in the plaintiffs acquiring several hundred relevant documents. The documents were mostly handwritten drafts of memorandums sent to the defendant's corporate counsel.

During the course of the trial, the defendant's document disposal process was elicited. Initially, an employee of Swiss Bernina, Inc. would compose a handwritten draft of a confidential letter. Upon the mailing of the letter, the draft was disposed of in a wastebasket inside of the office. Later, an employee would empty the wastebasket into a dumpster located behind the Swiss Bernina, Inc. office building. The dumpster was owned solely by Swiss Bernina, Inc. and a company contracted with the defendant would empty its contents on a regular basis.

At trial, both parties agreed that defendants expected these documents to remain confidential. However, the magistrate in the court of original jurisdiction disagreed with the plaintiff's practice of taking documents from the defendant's privately owned dumpster, and prevented their admission into evidence.

On appeal, the United States District Court, for the Northern District of Illinois, weighed several factors in its determination of whether these practices constituted a waiver of the attorney-client privilege. The court cited the "modern trend," moving away from the strict standards of Wigmore's principle that inadvertent disclosure equals automatic waiver. However, in evaluating the arguments of both the plaintiff and defendant, the court analyzed the defendant's document retention strategies. It recognized that the defendant did not put the documents in a place for safekeeping and did not diligently attempt to safeguard their confidentiality. It focused on two considerations in its holding: "(1) the effect on uninhibited consultation between attorney and client [by] not allowing the privilege in these circumstances; and (2) the ability of the parties to the communication to protect against these disclosures." [90] In response to the first consideration, the District Court found that the likelihood of a party to risk the potential civil and criminal implications of rummaging through mounds of garbage, in the hopes of finding confidential information, does not sufficiently deter open and honest communication between attorneys and clients. For the second consideration, the court held that, "while requiring this degree of precaution may seem extreme, if the parties feel that the likelihood of disclosure is sufficiently great, the precautions may be justified, and it is within

[90] See *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91, F.R.D. 254, 260 (D.C.Ill. 1981)

their power to decide what precautions to take, and so to protect against disclosure."[91] With this ruling, the court applied a balancing test to weigh the interests of both the plaintiff and defendant. Finding in favor of the plaintiff, the court's reasoning established that though there were several considerations which were paramount to its justifications, the defendant ultimately carried the reasonable responsibility to ensure that confidential documents were protected in such a way to prevent their disclosure.

The United States District Court, for the Northern District of New York, in *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103 (S.D.N.Y. 1985) was presented a similar challenge: which interest would prevail in a case of inadvertent disclosure? The facts presented to the court described Lois Sportswear's requests for the production of documents by Levi Strauss & Co. Its request resulted in over thirty thousand documents produced by Levi Strauss. Inadvertently, in the large request for documents, the defendant produced twenty-two documents, which, it alleged, were protected by the work product doctrine and the attorney-client privilege.

Reviewing the case facts, the court determined that there were several factors that would assist it in resolving the issue of whether or not the release of the documents was a knowing waiver, or a simple mistake, later recognized and rectified.[92] The court cites the following elements as critical in its review of this issue: "…reasonableness of the precautions to prevent inadvertent disclosure, the time taken to rectify the error, the scope of the discovery[,]…the extent of the disclosure[,]…fairness and the protection of an appropriate privilege…"[93]

---

[91] *Id.*
[92] See *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co*., 104 F.R.D. 103, 105 (D.C.N.Y. 1985)
[93] *Id.*

The court relied heavily on the intent of Levi Strauss, rejecting too the Wigmore "strict responsibility" doctrine and analyzing more closely the intent of a disclosure. It found that although Levi Strauss had not adopted a regular practice of deeming documents confidential at the time of their origination, and that it did not have a thorough method to protect these documents, the intent of Levi Strauss to prevent these documents from being disclosed was sufficient to prevent their admission in trial. It ultimately upheld Levi Strauss' pre-trial motion to prevent the admission of the twenty-two documents into the record. This case further serves as an example that some courts are apt to view many factors in the consideration of whether inadvertent disclosure is admissible at trial and whether that disclosure is considered a known or unknown mistake.

Very similar to the case above, in *In re Grand Jury Investigation*, 142 F.R.D. 276 (M.D.N.C. 1992), a company was served with three grand jury subpoenas *duces tecum*. During the production of documents, in accordance with the subpoenas, the company produced over three-hundred thousand documents for the jury's review. The company inadvertently disclosed eighteen documents, which were protected by the attorney-client privilege. It sought a protective order from the United States District Court, for the Middle District of North Carolina, to prevent the documents' disclosure to the jury, alleging the documents were protected by the attorney-client privilege.

Evidence demonstrated the company had a reasonable method to determine a document's responsiveness to the requirements set forth in the subpoenas. The court notes, "Responsive documents [to the subpoena] were further reviewed by a team member, in the presence of the senior team attorney (who has 'seven years experience in conducting large document productions

efforts'), to determine if they were privileged."[94] Documents, which were thought to be privileged, were referred to the senior attorney for final review. If a document was found to warrant attorney-client privilege protections, a red slip of paper was stapled to the document, designating it to be withheld from the document production. Finally, the documents, which were to be produced to the government, were organized according to the subpoenas, and all privileged documents were removed.

The District Court applied the balancing test in determining whether the attorney-client privilege had been waived by inadvertent disclosure. It applied a five-factor test in its determination. The court writes,

> …the test calls for the court to consider the following factors: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of the document productions; (2) the number of inadvertent disclosures; (3) the extent of the disclosure; (4) any delay and measures taken to rectify the disclosure; and (5) whether the overriding interests of justice would or would not be served by relieving a party of its error.[95]

The court purposefully failed to adopt one consistent method for reviewing inadvertent disclosure cases. Instead, it notes that each will be reviewed on a case-by-case basis. In its opinion, it finds that waivers do usually have to be intentional or knowing acts.[96] In conclusion, based on its review of the factors, the court found that the company had reasonable and adequate precautions in place to prevent the disclosure of protected documents. The company did not intend to release the specific, privileged documents to the government. Therefore, the documents would not be admitted for the jury's review.

[94] See *In re Grand Jury Investigation*, 142 F.R.D. 276, 277 (M.D.N.C. 1992)
[95] *Id.* at 278
[96] See Id. at 279

Florida Cases Regarding Inadvertent Disclosure of Documents

Generally, it appears Florida courts have adopted a "balancing test" approach in their determination of whether or not the inadvertent disclosure of information constitutes a waiver of the attorney-client privilege for protected documents. As will be described in more detail below, Florida Courts have looked to five criteria to determine whether inadvertent disclosure of privileged material constitutes a waiver of the privilege: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the number of inadvertent disclosures, (3) the extent of the disclosure, (4) the delay in measures taken to rectify the inadvertent disclosures, and (5) whether overriding interests of justice will be served by relieving the party of its error.

The Florida Supreme Court officially recognized the "relevant circumstances" test to determine if inadvertent disclosures would result in waiver in *Lightbourne v. McCollum*, 969 So. 2d 326 (Fla. 2007). In the *Lightbourne* case, the State inadvertently disclosed a memorandum to the defense. The Court analyzed the five-factor test, eventually finding the State had failed to take reasonable precautions to prevent inadvertent disclosure of the document, in violation of the first part of the five-factor test.[97]

In *Nova Southeastern University, Inc. v. Jacobson*, 25 So.3d 82, (Fla. 4th DCA 2009), Nova Southeastern University sought review by the Florida Fourth District Court of Appeals in light of a denied motion for protective order. The facts describe the defendant, while working at a middle school, receiving a facsimile transmission, which contained a letter from the law firm representing Nova Southeastern University (NOVA). Earlier, Patricia Jacobson had been fired from the University for "…failure to comply with an earlier written final warning and for

[97] *Lightbourne v. McCollum*, 969 So. 2d 326, 334 (Fla. 2007)

negligence and inefficiency, as well as other grounds."[98] Jacobson alleged that she had been terminated based on a disability and the University, therefore, took a course of conduct in order to justify her termination.

The letter sent in the facsimile transmission was authored by counsel for NOVA and was addressed to the head master of the school, the human resources department, and the director of the middle school. It described Jacobson and the termination stating that the university "…did not have enough performance issues to fire [Jacobson], and that it would have to be a business decision whether [Jacobson] was going to remain an employee of NSU."[99] At a deposition, the counsel for NOVA objected to the admission of testimony regarding the letter and claimed it was protected by the attorney-client privilege.

Counsel for NOVA highlighted their intentions to keep the letter confidential. The cover-sheet on the facsimile transmission stated that the letter was protected by the attorney-client privilege. Furthermore, NOVA filed affidavits from each of the parties to whom the letter was sent, indicating they didn't intend for third parties to see the communication.

The court weighed the five factors in determining whether the attorney-client privilege had been waived. It had the most difficulty in reaching a conclusion of whether reasonable precautions were taken to prevent inadvertent disclosure. In remanding the case to the trial court, the appellate court asked the judge to focus narrowly on several issues: "…whether the client knew or should have known that the letter sent by the attorney would be viewed by third parties. Whether the use of the fax machine to send the communication negates a claim that the matter was sent in confidence requires a fact-intensive determination." While a determination

[98] See *Nova Southeastern University, Inc. v. Jacobson*, 25 So.3d 82, 84 (Fla. 4th DCA 2009)
[99] *Id.*

was not made as to this issue, the court acknowledged and relied on use of circumstantial factors in reviewing how the disclosure did or did not affect the retention of the privilege.

At the District Court of Appeals, Third District, in *Abamar Housing and Development, Inc. v. Lisa Daly Lady Décor, Inc.*, 698 So. 2d 276 (Fla. 3d DCA 1997), the court was petitioned to quash a trial court order denying the plaintiff's motion for the return of specific documents, which were allegedly protected by the attorney-client privilege. The documents were inadvertently disclosed during a large document production. The plaintiffs had taken reasonable precautions to ensure that privileged documents were not released to the defense. Despite the production of approximately one hundred thousand documents, a lawyer and paralegal were assigned the arduous task of reviewing all the documents to be produced. Accidentally, twenty-three documents were produced which should have remained confidential.

In its analysis of the appeal, the Florida Third District Court of Appeals took the same five-factor test to determine whether the disclosure waived the attorney-client privilege. Based on the overall circumstances of the case, the defendant was ordered to return the documents and was not permitted to use the documents or reference them at trial.

Strikingly relevant to this thesis, the case of *Minakan v. Husted*, 27 So. 3d 695 (Fla. 4th DCA 2010) dealt directly with the access of e-mail messages and inadvertent disclosure. During a dissolution of marriage proceeding, the husband motioned for the disqualification of his former wife's attorney. The husband alleged that prior to the dissolution proceeding, the couple shared an e-mail account, where the password and access were jointly shared. However, shortly after the proceeding for dissolution began, the husband claimed he changed the password to the account to prevent access by his former wife. The wife was still able to access the e-mail

account after this password change, stating that she used the same password to login as she had always used.

During the time in which the wife continued to access the account, she became privy to messages between the husband and his attorney. In her review of the messages, she discovered a message that had been sent by the husband to his attorney. The wife interpreted this e-mail as evidence to defraud her in the dissolution proceeding. Quickly, she forwarded the message to her sister, which was later sent to the wife's attorney. Immediately, the wife's attorney recognized that the e-mail would potentially be subject to attorney-client privileges and sent the husband's counsel a letter returning the electronic message.

The case facts are truly unique, representing the only Florida appellate case found discussing the attorney-client privilege and misuse, or unintended disclosures, of electronic messages. Unfortunately for purposes of this research, the appellate court failed to make a finding as to the confidentiality of the e-mail message that was acquired by the wife and whether the husband acted in a manner, which demonstrates his intention to keep the document confidential. The court did, though, specify that the trial court was not to apply the five-factor test of inadvertent disclosure, as neither party alleged the disclosure was inadvertent.[100]

CHAPTER SIX: ANALOGIES TO OTHER MEDIA

Throughout more recent modern history, technology has swiftly changed for many professionals. Implementation of new devices, like fax machines and cordless telephones, brought with it a certain group of legal professionals that were fearful of the possible

[100] *Minakan v. Husted*, 27 So. 3d 695, 700 (Fla. 4th DCA 2010)

implications and dangers of using the new technology. Despite these fears, however, attorneys have consistently relied on these new forms of technology to communicate with their clients. Fax machines, cordless phones, and computers are mostly commonplace to all offices.

With each new office technology, concerns of privacy were adverted. In analyzing electronic mail and the new, similar concerns that are present currently, it's practical to report what the legal community's reaction to other technology has been. Below, this thesis will analyze other communication devices and their respective relationship to privacy concerns of electronic mail.

Facsimile

Fax machines were one of the first technological advancements to allow for the sending and receiving of physical documents over geographic space, without the use of hand delivery or postal service. The technology utilized existing phone lines to transmit data.

For many reasons, fax machines were quickly adopted. Similar to the improvements electronic mail has brought to the legal profession, fax machines offered many of the same attractive benefits. Documents could be sent quickly, cheaply, and almost instantly.

Fax machines are similar to electronic mail transmission in several respects. Like e-mail, fax machines are not restricted by geographic space. They transmit documents rapidly across large distances. Additionally, each fax machine has its own address: a telephone number. This is comparable to an e-mail address. It's a unique identifier, which allows the technology to appropriately convey information to the correct fax machine.

Dissimilarly, fax machines are generally not restricted to one user. Unlike an e-mail account, which can only be accessed by an individual username and password, fax machines

generally are purchased for whole office use. If a confidential document was sent by fax, one could not necessarily guarantee that only the claimed recipient of the document would have access to the information. This is a trend that is becoming decreasing true, however, as the cost of fax machines has decreased dramatically as the technology has been integrated into personal printers, computers, etc. Also, the increased use of electronic mail, where documents can be scanned and sent electronically, has decreased fax machine usage.

Facsimile transmission "…became affordable and widely used in the 1980's…"[101] and was at once under scrutiny for its effect on the attorney client privilege. Many courts faced with the issue agreed that a fax did not alter the nature of the privilege or the protections that it granted.[102] Lawyers were still cautioned to maintain client confidentiality when faxing materials as "careless use of a fax machine may result in inadvertent delivery of client information to the wrong person, triggering a dispute over availability of the attorney-client privilege and possible malpractice liability."[103]

Cordless Telephones

Cordless telephones operate by broadcasting radio waves in all directions. A cordless telephone communicates with a base station on a radio frequency. Both the incoming and outgoing conversations are relayed through this base station from the headset. The communications then transmit through the telephone lines to the party on the other end.

Because the conversation is openly broadcast, the radio waves aren't secure. Similar to a radio station, which you would tune into with a stereo, a cordless telephone conversation could

[101] Hill, *supra* note 37, at 8.
[102] David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 Tex. B.J. 104, 110 (1997)
[103] See ABA/BNA Lawyer's Manual on Professional Conduct: Electronic Communications Practice Guide, 55:401

be intercepted intentionally, or by mistake, with relative ease. [104] All that is required is to use another telephone or device, capable of receiving the same radio frequencies.

Like a postcard's ability to be read by any third party when in transit, cordless telephone conversations share similar properties. Any party in range of the cordless telephone base station, with a similar phone, would be able to overhear the conversation. Most cordless phones are limited in range, not extending much beyond the boundaries of a normal family home. From experience, when in an office building, vertical height, as well as the numerous walls and dividers found in office spaces, further limit the range.

The cordless telephone does not share many properties similar to electronic mail, but the concerns regarding their use are very similar. The open nature of cordless telephone conversations spurred debate and fears among legal professions. They were concerned one, that their conversations could be easily intercepted, and two, that these conversations would result in waivers of privilege.

The expectation of privacy using this technology in many ways diminished during the height of these concerns. Attorneys were increasingly aware of the ability to intercept cordless telephone conversations. Many avoided their use, communicating confidentially through landlines, or in person, instead. Legislatively, Congress granted the same protections to cordless phones as landline phones in 1994 through statutory changes of the Federal Wiretap Act.[105] It afforded a reasonable expectation of privacy in conversations, and provided a legal remedy for intentional interceptions. However, "it should be noted that some take the position that privacy

[104] Id.
[105] Hricik, *supra* note 16 , at 108.

is not assured on a cordless phone since federal law does not apply to mistakes, just intentional interceptions."[106]

Cellular Telephones

Cellular telephones operate, similarly to cordless phones, by transmitting radio signals to a base station receiver in a geographic space. The base station then routes the signals to other base stations, or local telephone companies, to deliver the call. Due to the nature of cellular radio signals, a receiver capable of receiving radio broadcast signals could be used to intercept cell phone conversations. Some bar committees urged lawyers to use cordless and cellular phones with caution. "Ethics opinions in several states indicated that communications conducted in this manner might not be considered confidential and might not be covered by the attorney-client privilege."[107]

The first cellular phones introduced into the market relied on analog radio signals to send and receive information. Analog radio functions by converting sounds into electrical signals. The electrical signals are then transmitted via carrier networks to the destination, where the electrical signals are converted into sound. Because analog radio signals are electrical signals, being sent and received in public airwaves, many raised concerns that communications could be easily intercepted, intentionally or by mistake.

Unlike that of analog cell phone technology, digital cellular service transforms sound into electronic data. The electronic data is made up of binary code, which is transmitted through carrier radio waves. Digital electronic communication is more difficult to intercept. Although a

[106] Hill, *supra* note 37, at 9.
[107] *Hill*, *supra* note 37, at 9

conversation could still be overheard using very sophisticated technology, for the most part, digital technology increased, to a greater degree, the expectation of privacy.

CHAPTER SEVEN: HOW THE ATTORNEY-CLIENT PRIVILEGE AND ELECTRONIC MAIL COLLIDE

As mentioned earlier, because of the importance of the attorney-client privilege and how it functions within our legal system, neither attorneys, nor clients, are typically required to disclose protected, confidential communications to another party outside of the privileged communication. "The attorney-client privilege is not absolute, [however,] but is subject to certain exceptions where the courts have determined that the privilege must give way to some other, competing policy."[108] Some of these exceptions include the fiduciary, crime-fraud, "at-issue", public policy, and waiver exceptions.[109] A fiduciary duty is a "duty of utmost good faith, trust, confidence, and candor owed by a fiduciary (such as a lawyer or corporate officer) to the beneficiary (such as a lawyer's client or a shareholder)."[110] The crime-fraud exception is the "doctrine that neither the attorney-client privilege nor the attorney-work-product privilege protects attorney-client communications that are in furtherance of a current or planned crime or fraud."[111] The "at-issue" waiver is defined as "an exemption from the attorney-client privilege, whereby a litigant is considered to have waived the privilege by taking a position that cannot be

[108] Vincent S. Walkowiak, *Attorney-Client Privilege in Civil Litigation: Protecting and Defending Confidentiality*, 232 (2004)
[109] *Id.* at 232-234
[110] *Black's Law Dictionary* (9th ed. 2009)
[111] *Id.*

effectively challenged without analyzing privileged information."[112] The public-policy exception provides protection for employees who blow the whistle on their employers' misconduct.[113] Lastly, waiver is "the voluntary relinquishment or abandonment – express or implied – of a legal right or advantage."[114] Once again, this thesis will only focus on the latter exception, 'waiver' and its role in relation to electronic mail use.

One circumstance, which may require an attorney or client to waive the protections of the attorney-privilege, arises when the content of their communications is conveyed to a third party. Disclosure to third parties can take place in many circumstances.[115] Such examples include when a client voluntarily disclosures case facts to another or a lawyer mistakenly provides a document in discovery containing case strategies. One potential danger of using e-mail is that disclosure to a third party can arise easily and unknowingly. Mere lack of technological expertise or a simple typographical mistake might cause disclosure. Clicking the "reply all" button instead of the "reply" button could potentially put protected communications in detriment. Or, a lawyer may inadvertently add opposing counsel on the recipient list when composing a new message, whereas the message was intended only for the attorney's client. In either scenario, a lawyer may jeopardize his client's case. After careful analysis of relevant case law, it's likely that in either scenario, if the lawyer was responsible for the disclosure, the communication will remain legally protected by the court. We've already learned that the client is the sole holder of the privilege. On the other hand, and in an equally likely scenario, if a client was to

[112] *Id.*
[113] Terry M. Dworkin & Elletta Sangrey Callahan, *Buying Silence*, 36 Am. Bus. L.J. 151, 173 (1998)
[114] *Black's Law Dictionary*, *supra* note 110
[115] Rand, *supra* note 12, at 362

inadvertently disclose a confidential e-mail intended only for his attorney through one of the mistakes just mentioned, the communication may be admissible at trial.

In a more sophisticated analysis, how does the expectation of privacy play a role in electronic mail? Except for the United States Sixth Circuit Court of Appeals in *United States v. Warshak*, no other court has established a legal expectation of privacy in electronic mail. When looking back to other developing technologies, such as facsimile, the courts were initially hesitant to grant such protection. Over time, the courts eventually found that there was a reasonable degree of privacy to be expected, and reminded lawyers in one way or another, that it was their obligation to protect the confidential communications of their clients. When the cellular telephone became popular, a similar scenario developed. Lawyers were cautioned in their use of the technology and advised to use more secure methods of communication when possible. In order to assert the protections of the attorney-client privilege, there must be a reasonable expectation of privacy in the communication that it will remain confidential or will only be disseminated to the intended individuals.

A lesser known, yet equally likely legal complication to the attorney-client privilege and electronic mail arises from something far less obvious to the common user: targeted advertisements and the use of third party e-mail clients. Many free consumer e-mail clients, such as Google's "Gmail", use targeted advertisements. They operate through computer software, which scans and "reads" e-mails to find key words that the software then determines may be related to advertisements offered by different companies.[116] These advertisements appear to the user by website links located at the top, bottom, or sides of the e-mail client window. Using a

[116] Google, *More on Gmail and Privacy*, http://mail.google.com/mail/help/about_privacy.html.

traditional legal approach, disclosing a privileged communication inadvertently or voluntarily constitutes as a waiver of the privilege. The obvious question that arises is whether sending e-mail that is subjected to targeted advertising constitutes as a waiver of that communication to a third party (advertisers)?

The last concern to address regarding the use of electronic mail arises in security. It's no surprise to those familiar with technology, and even to those that aren't, that electronic intruders (commonly referred to as hackers) seek to acquire notoriety, monetary gain, or information through exploits exposed in computer software. Banks, computers, governments, and the military have all been subject to hacking attacks, sometimes resulting in devastating consequences and embarrassing news coverage (see figure 5). Because of e-mail's prolific use and software-based construction, electronic mail has fallen victim to hacking, as well. A common user's electronic mail account may contain bank account information, addresses, phone numbers, credit card information, and passwords to countless online portals. Considering the harsh effects these attacks have on common users, attorneys are equally, if not more so, likely to be "damaged" by a malignant intruder. The question then becomes one of liability. "If lawyers have the reason to believe that communications between them and their clients are being intercepted, regardless of whether the privilege is preserved or not, an attorney may be liable."[117]

[117] Matthews, *supra* note 43, at 299.

CNN Home | Video | NewsPulse | U.S. | World | Politics | Justice | Entertainment | Tech |

CNN TV SCHEDULE ANCHORS & REPORTERS CONTACT US HLN

AM AMERICAN MORNING

November 29, 2010

WikiLeaks dump 'embarrassing' and damaging to U.S. relations, former govt. official says

Posted: 09:40 AM ET

Lexie Clinton - lclinton
Filed under: amFIX

(CNN) – A day after the whistleblower site WikiLeaks began publishing details from a massive collection of confidential U.S. diplomatic documents, the chorus of criticism from government leaders grew louder Monday. Top U.S. officials were quick to denounce the publication of the leaked documents Sunday. And the U.K.'s foreign office followed suit Monday, saying it condemned any release of classified documents. "They can damage national security, are not in the national interest and, as the U.S. [has] said, may put lives at risk," the office said in a statement.

The full set of documents includes 251,288 cables sent by American diplomats between the end of 1966 and February 2010, WikiLeaks said in a statement announcing the release. Of those, 8,017 originated from the office of the secretary of state, and more than 15,600 are classified as secret, WikiLeaks said.

Today on American Morning, John Roberts talks to James Rubin, former U.S. assistant Secretary of State, about how the information affects national security. Watch to find out why Rubin calls the documents a "broad-based attack on U.S. foreign policy."

Figure 5: WikiLeaks release of embassy cables was an embarrassing U.S. political dilemma.[118]

CHAPTER EIGHT: GOVERNMENT-IN-THE-SUNSHINE LAW

One additional aspect to consider in transmitting private information through electronic mail, especially in regards to attorneys, arises from those employed by municipalities, counties, or governmental agencies. Florida is one state, among several, which places a high emphasis on the public's right to access information produced by government officials. Even the Florida Constitution provides for the right of public information:

> Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records

[118] See http://amfix.blogs.cnn.com/2010/11/29/wikileaks-dump-%E2%80%98embarrassing%E2%80%99-and-damaging-to-u-s-relations-former-govt-official-says/?iref=allsearch

> exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution.[119]

The tradition of openness began in 1909, when the Florida Legislature voted to create Chapter 119 of the Florida Statutes, which has since become known as the "Public Records Law."[120] As new forms of media have developed, the statute has adapted from including traditional documents, such as papers and books, to new forms of media, like sound recordings and computer records. Regardless of the form of media, the general policy of the state, found in Chapter 119 of Florida Statutes provides, "It is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person. Providing access to public records is a duty of each agency."[121] However, the legislature has provided for several exemptions from this general rule, and right, as a matter of public policy.

Under Chapter 119.071, Florida Statutes describe general exemptions from the inspection or copying of public records. One such exemption provides for agency attorneys:

> A public record that was prepared by an agency attorney (including an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record) or prepared at the attorney's express direction, that reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and that was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or that was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings, is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until the conclusion of the litigation or adversarial administrative proceedings.[122]

[119] FLA. CONST. art. I, § 24
[120] See http://www.myflsunshine/sun.nsf/pages/Law
[121] FLA. STAT. § 119.01(1) (2011)
[122] FLA. STAT. § 119.071(1)(d)(1) (2011)

Under this provision, those records created by agency attorneys which reflect a mental impression, conclusion, litigation strategy, or legal theory of the attorney or agency are generally exempt from public records request. Interestingly, however, this statute only provides that these records are protected until the conclusion of the litigation or adversarial proceedings.

Amy Iennaco, Chief Assistant City Attorney for the City of Orlando, commented regarding the practices of the City Attorney's Office in relation to its document retention policies, as well as any security measures in place to ensure the confidentiality of e-mail messages. Currently, the City of Orlando does not utilize separate encryption software to transmit e-mail messages during the anticipation of litigation. Additionally, Mrs. Iennaco writes in reference to transmitting confidential information, "We do not have a specific written policy. There is a City e-mail policy, but it does not address the specific concern [of transmitting confidential information]."

Because of the City of Orlando's, City Attorney's Office, unique position that all records prepared in anticipation of litigation are no longer exempt from public records request at the conclusion of the litigation, Mrs. Iennaco was asked to offer her opinion regarding the use of e-mail disclaimers which state whether a particular message is confidential. She commented,

> Although e-mails we receive from outside counsel are often labeled 'confidential' in the subject line, and often contain disclaimers under the signatures, e-mails that I send usually do not. Because only work done in anticipation of litigation is exempt, and after the litigation is concluded it becomes public record, I do not want to give my in-house clients a false sense of security, so they think they can say whatever they like in their e-mails to me with impunity.

For many attorneys, this idea of purposefully omitting a warning of confidentiality statement, like was mentioned earlier, may seem counterintuitive. Perhaps, however, this

method of not instilling a false sense of security in e-mail messages deserves a closer look, given Mr. Roosenraad's comments.

CHAPTER NINE: ETHICAL CONSIDERATIONS

This thesis has addressed many of the legal and technical aspects of the attorney-client privilege, electronic mail use, waiver, and other relevant topics, but has yet to discuss the importance of ethical decision-making in light of these issues.

From a professional sense, placing a strong emphasis on the importance of practicing ethical behavior improves the credibility of the legal field and restores public trust in the profession. In the contexts of privileged documents and inadvertent disclosures, ethics continue to play a very important role. Attorneys are easily able to deceive, intentionally withhold documents and information, and override the interests of justice by engaging in unethical practices.

In a digital era, the importance of ethics takes a center role. For example, an attorney who receives an inadvertently sent e-mail from co-counsel could easily read the e-mail, delete it, store it, reproduce it, or use it to benefit his client. In fact, it may be only after the message is read that the attorney realizes the message was intended to be privileged, unless of course the subject line of the e-mail clearly indicates its confidentiality. What is the accepted ethical response to a misaddressed facsimile/e-mail, which contains privileged information? Dean Wigmore would argue that the document, by its receipt alone, is no longer subject to protection and therefore is free to be used by the receiving party. Other jurisdictions, like the Northern District of Illinois, argue that when information is clearly intended to remain confidential, it is

unethical to use the information to the sending party's detriment or receiving party's benefit.[123] Either way, the ethical dilemmas are thorny. There are several responses by the American Bar Association and The Florida Bar to these predicaments.

Inadvertent Disclosure – Perspective of Florida Bar

In legal practice, documents are exchanged between clients, attorneys, and the courts. On occasion, some documents are sent inadvertently to the incorrect parties. This can happen with misdirected e-mails and facsimiles, as well. In Ethics Opinion 93-3, the Professional Ethics Committee addresses the ethical responsibility of an attorney whom receives inadvertently disclosed documents. It states "…that an attorney, upon realizing or reasonably believing that he or she has received a document or documents that were inadvertently delivered, is ethically obligated to promptly notify the sender of the attorney's receipt of the documents. It is then up to the sender to take any further action."[124] As discussed in detail earlier, whether the inadvertent disclosure will affect the attorney-client privilege depends greatly upon both the jurisdiction and interpretation of the courts.

The Florida Supreme Court also has adopted an analogous rule governing ethical conduct of attorneys and their response to receipt of inadvertent documents. Rule 4-4.4(b) notes the attorney's responsibility to notify the sender of a received document when he knows or reasonably should know it was received in error.[125] Notice allows the sender to take protective measures. The Court does not require any more action aside from notifying the sending party, however. An attorney may choose to return an original document, delete e-mails, and discard

[123] *Mendenhall v. Barber-Greene Co, supra* note 89.
[124] See Fla. Bar Professional Ethics Committee, Formal Op. 93-3 (1994)
[125] Fla. Rules of Prof'l Conduct R. 4-4.4(b) (2006)

faxes, but ultimately, professional judgment and discretion will determine how an individual attorney will respond.

Deliberate Retrieval of Documents

Ethics Opinion 93-3 pertains directly to documents disclosed inadvertently, but does not wholly address an attorney's ethical duty to respond to documents that have been obtained wrongfully by the client.[126] In a matter brought for review before the Professional Ethics Committee, an attorney questioned what was the appropriate ethical response in a peculiar situation.[127] In writing the Committee, the attorney describes his client (a wife in a dissolution of marriage proceeding) retrieving documents from her husband in four, possibly unlawful, ways. One, she physically removed documents from the husband's office before and after the separation. Two, the wife gained access to the husband's office computer and e-mail account, thereafter printing and accessing financial records and communications sent between the husband and his attorney. Three, she accessed her husband's personal e-mail account where she continued to download and print more information. Lastly, four, the wife removed documents from the husband's vehicle which were believed to be privileged. This example is relevant to this thesis for its deliberate misuse of electronic mail. It also is applicable for its insight into lawyer conduct when dealing with wrongfully obtained information.

Rule 4-4.4(b), in comments, emphasizes that the rule fails to govern documents, which are given to a lawyer who knows or reasonably should know that the documents were obtained wrongfully. It only addresses the inadvertent disclosure of documents. While the Professional

[126] *Supra* note 124
[127] See Fla. Bar Professional Ethics Committee, Formal Op. 07-1 (2007)

Ethics Committee could not apply Rule 4-4.4(b) to the attorney's inquiry above, it found that other, relevant, rules applied.[128]

Rule 4-1.6 outlines guidelines for attorneys to follow when handling confidential information. Generally, confidential information cannot be disclosed without consent of the client, or if an exception applies. Most importantly, however, it protects confidential information, whatever the source.[129] The Committee writes, "Thus, under the rule, an attorney cannot voluntarily reveal any information relating to the representation of a client unless the client consents or an exception to the rule is applicable."[130] However, this rule applies indirectly to the scenario presented. The rule does not, narrowly enough, direct ethical conduct.

Other rules may be useful in finding a solution to this ethical dilemma. Rule 4-1.2(d) does not permit an attorney to assist a client in behavior which the attorney knows or reasonably should know is criminal or fraudulent.[131] Unauthorized access to data, e-mail accounts, and vehicle may be considered as criminal, fraudulent, or both. In a criminal proceeding, a court could demand the production of the 'stolen' documents, but this is a legal finding dependent upon substantive law and jurisdictional differences, more so than the findings of ethics committees.

The law is clear, though, in recognizing that attorneys, who receive evidence of a crime, must produce the evidence to a law enforcement agency. The attorney is not, however, obligated to disclose the source of the evidence and the prosecution is not able to introduce into trial how the evidence was acquired. This is demonstrated in *Quinones v. State* where the court writes,

---

[128] *Id.* at 4.
[129] Fla. Rules of Prof'l Conduct R. 4-1.6 (2006).
[130] *Supra* note 127, at 4.
[131] Fla. Rules of Prof'l Conduct R. 4-1.2(d) (2006).

"The overwhelming authority in the nation concludes that an attorney may not accept evidence of a crime unless he or she makes the same available to the prosecutor or the investigating law enforcement agency."[132] The finding was echoed too in *Anderson v. State*, which found that a lawyer acted responsibly when he surrendered a stolen dictaphone and calculator to the police.[133]

Rule 4-8.4(c) provides that a lawyer cannot engage in conduct, which involves dishonesty, or conduct that is considered prejudicial to the administration of justice.[134] Additionally, Rule 4-3.4(a) provides that a lawyer must not "unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act."[135] The Professional Ethics Committee of the Florida Bar refrained from making a definite decision to assist the petitioning attorney mentioned above. Yet, it can be reasonably inferred that the conduct the wife prescribed to is not in the interests of justice. Ethically, it will be the discretion of the attorney whether the documents obtained wrongfully by a client can, or should, be used in preparation of and during litigation. If the conduct of his client, however, involves conduct that is criminal in nature, the attorney should discuss the legal ramifications of his client's actions directly, possibly referring the client to the services of a criminal defense attorney. Finally, the receipt of the documents should be disclosed to the opposing party. This allows the opposing party to take corrective measures.

---

[132] *Quinones v. State*, 766 So. 2d 1165, 1172 n.8 (Fla. 3d DCA 2000)
[133] *Anderson v. State*, 297 So. 2d 871, 875 (Fla. 2d DCA 1974)
[134] Fla. Rules of Prof'l Conduct R. 4-8.4(c) (2006).
[135] Fla. Rules of Prof'l Conduct R. 4-3.4(a) (2006).

Though the Rules of Professional Conduct fail to adequately address ethical responses in these situations, an attorney should recognize the provisions that protect client confidentiality and the overall interests of justice. For electronic mail, which has been provided to an attorney by a client, the attorney should candidly discuss with his client what means were used to acquire the information. If criminal in nature, the attorney should refrain from further client representation and notify the opposing party of the documents or information, which have been obtained. Furthermore, in the interests of justice and fair trials, an attorney should recognize that allowing the use of wrongfully acquired information further incentivizes the client to once again participate in the behavior. Lastly, if the nature of the acquired information is confidential, an attorney may be sanctioned for disclosing confidential information without consent. Either way, it is ultimately the attorney's responsibility to discourage behavior by his client that does not abide by the laws or rules of ethical behavior.

Mining for Metadata

Metadata has taken a more recent spotlight in this ethics debate. An electronic document, such as a word processing document or e-mail, has hidden information, which can be retrieved by software or other intricate means. This is referred to as 'metadata'. The term is defined as "…information describing the history, tracking, or management of an electronic document."[136] Once an electronic document has been sent to another party, retrieval of this information could add additional insight into the case that the distributing party did not intend to disclose. In 2006,

[136] See *The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age,* Appendix F (The Sedona Conference Working Group Series, Sept. 2005 Series), http:// www.thesedonaconference.org

the Board of Governors of The Florida Bar directed the Professional Ethics Committee to review the ethical issues surrounding metadata retrieval.[137]

Metadata can reveal a wide range of information about a document. It can contain information about the author of the document, revisions made to the document, and comments by reviewers. Accessing this information could reveal materials the sending party did not intend to disclose. Or, metadata could include information, which is protected by the attorney-client privilege.[138]

The Committee was directed to analyze current Rules of Professional Conduct and make a determination as to how metadata is affected. As detailed before, an attorney is responsible to protect confidential client information. Likewise, in the transmission of electronic data, the duty to maintain confidentiality of information does not vanish. Therefore, the Committee found that lawyers must take reasonable steps to ensure that documents sent from the lawyer's office do not contain information, which is not intended to be disclosed.

Similarly, an attorney who receives electronic documents is directed to not engage in behavior that seeks to discover hidden information. If however, information is obtained inadvertently, in the form of metadata, the attorney must notify the opposing party of the receipt of the information.

Aside from these aspects of the law, attorneys are to engage in ethical decision-making on behalf of their clients and the legal profession. Lawyers are quick to adopt practices whereby costs are minimized and efficiency is maximized. After all, a law firm can greatly reduce its

[137] See Fla. Bar Professional Ethics Committee, Formal Op. 06-2 (2006)
[138] *Id.*

operating expenses by investing in electronic mail accounts to send and receive messages in exchange of frequent mailings, which would ordinarily require postage and paper products.

After a full review of the relevant case law affecting confidential communications sent using electronic mail, there is no clear answer describing how a judge or court would rule in a matter contesting whether an e-mail message was protected by the attorney-client privilege. Most of the current laws affecting this particular field of interest pertain to protecting other forms of communication. Similar cases may be persuasive, and may be able to be applied to electronic mail. However, a judge would be required to follow only those cases which are explicitly precedent.

Legal professionals should be aware of this predicament. Most wish to use the convenience of electronic mail to its full potential – conveying documents back-and-forth, communicating with clients extensively through e-mail, and posting information into the electronic world that is confidential.

CHAPTER TEN: CONCLUSION

Electronic mail certainly challenges the traditional notions of communication between attorneys and their clients. Attorneys can communicate instantly, efficiently, and at a greatly reduced cost. Though it is one of the most efficient ways of communicating, it is, perhaps, also one of the most transparent. Mr. Roosenraad's discussion on e-mail security presents a strong argument; concluding a reasonable expectation privacy exists in e-mail messaging may be ill founded. Moreover, the myriad of ways in which attorneys can cause disclosure of confidential client information using electronic mail is staggering. Whether it is striking the "reply all"

button, instead of the "reply" button, or unintentionally sending metadata in an attached document, information is being inadvertently sent. Though many lawyers wish to believe that communicating electronically is an unbreakably secure medium, one point is clear: disclosure can and will occur through electronic mail by attorneys.

The question then becomes, what are the repercussions of such disclosure? Though the American Bar Association has given their "stamp of approval" for electronic mail use, attorneys should reconsider their technological habits. Consider the wealth of information that is usually found within an e-mail account. Messages, images, documents, videos, sound recordings, etc. can all be transmitted and received from one e-mail. Entire case strategies may be discussed, in alternating messages, between clients and attorneys at a law firm via e-mails. The ease at which this information can be disclosed should be of alarming concern. Most e-mails, after the composition of the message, take mere minutes to be sent and received. There's little to no time to rectify an error after a message has been sent. Also, in the daily practice of an attorney, e-mail messages constitute a large portion of their daily tasks. With responses and messages to judges, judicial assistants, clients, and counsel, much time is dedicated to communication. It's not overreaching to say that mistakes will be made in the delivery of the e-mail messages. Most users don't have a secondary review system in place for a supervising attorney to review the message and recipients before a message is sent. In sum, while the technology offers incredible convenience, it is all too easy for an attorney to violate the attorney-client privilege.

From a strictly legal sense, electronic mail is likely to be granted the same protections as any other form of communication. Most would agree there is some reasonable expectation of privacy when transmitting messages using the internet. Florida Courts, likewise, have generally

found that when a reasonable expectation of privacy is present in a communication, the attorney-client privilege will attach to that communication. However, it's unclear whether the attorney-client privilege would attach to a communication when an attorney knows a third party is easily able to intercept his message, or is readily present. As discussed above, the courts have failed to grant the protection of the attorney-client privilege to conversations when the communication is known, or the person should have known, the conversation is capable of being overheard. Although a third party cannot "overhear" an electronic message, one can intercept one, intentionally or inadvertently. Because of the recent development of this technology, no court has yet to encounter a situation where case information is disclosed to a third party through electronic mail. In such a situation, will the court determine that the attorney should have known his communication reasonably could have been intercepted? Will the court require the attorney to use a higher level of security, such as encryption software, to further ensure confidentiality? Or, will the court find that a sufficient expectation of privacy is present in electronic mail communications to prevent waiver? These are all questions that remain unanswered. Unfortunately, I cannot provide the answers to what recourse any one particular judge would take.

From an ethical standpoint, there is cause for concern for any lawyer who uses electronic mail to communicate case information to a client on a regular basis. Attorneys are charged with providing their clients open and honest opinions and must take every precaution to ensure confidentiality. Because of the increasing availability and ease-of-use associated with encryption technology, attorneys should be looking to implement this protective software into their daily practice. Though the cost may be cumbersome at first, attorneys will gain greater protection for

their practice and their clients. No one disputes that the use of encryption technology will likely end the debate over whether or not electronic mail is a safe means to communicate information. However, for attorneys who choose to not adopt this protective standard, the burden then rests on those attorneys to inform their clients of the particular risks associated with communicating confidential information over the web. Or, attorneys should limit their conversations with clients over the internet by subject, and use a more well-researched and time-tested form of communication to communicate sensitive information, instead. Though this poses some concerns of efficiency and convenience, remember the court isn't going to accept "convenience" as an excuse for disclosing confidential communications.

This thesis makes several recommendations for attorneys who wish to utilize electronic mail in their daily practice. First, all attorneys should adopt some form of encryption technology. Though Mr. Roosenraad expressed hesitation that encryption technology, alone, would not eliminate all security threats, it is a much more secure method to transmit information. Furthermore, it would demonstrate to any court a clear expectation of privacy, on behalf of the attorney and client, when communicating electronic messages.

Two, when transmitting messages through electronic mail software, disable any "reply all" buttons. Or, require the software to display a dialogue box to the user, notifying him that the message is going to be sent to multiple recipients instead of one. Either method would assist in preventing the inadvertent disclosure of information to unintended parties. Similarly, disabling threaded conversations, like those found in Google's Gmail, would help in preventing the accidental disclosure of confidential information.

Three, attorneys should lobby for greater, and more specific, statutory protection when using electronic mail. A law, which recognizes a right to privacy in electronic messages, would remedy many of the legal complications electronic mail use is currently plagued by. Or, a more viable tactic may be to add specific provisions within the Florida Evidence Code attaching the attorney-client privilege to electronic mail communications. Either way, both methods would establish a legal basis and foundation to protect confidential communications sent through e-mail.

Four, lawyers should avoid the use of ad-generated electronic mail providers. It's unclear, both from a security perspective and legal perspective, whether targeted advertising would be considered disclosure to third parties. The information being obtained by these advertisements may be extremely personal data or indiscriminate usage statistics. In either scenario, safeguarding against this type of activity would prevent the disclosure of confidential information. As a solution, lawyers and law firms should purchase commercially available products that are not funded by advertising revenue.

Five, when transmitting documents by e-mail, attorneys should remove any possible metadata from their documents. Though ethically this information is not to be actively sought after by attorneys, for practical reasons, preventing disclosure of this information may save the attorney's client from embarrassing and damaging results. One tangible solution is to adopt metadata "scrubbing" software. This could prevent the inadvertent disclosure of confidential client data. Or, lawyers may be able to adopt a more secure document format, known to transmit and retain less metadata as a standard.

In summary, this thesis makes three important assertions. First, the use of electronic mail can result in the legal waiver of the attorney-client privilege. Case law has substantiated that when a reasonable expectation of privacy does not exist within a communication, or a party knows his communication can be overheard, then the protections of the attorney-client privilege do not attach to that communication. Without encryption technology, e-mail is too transparent to be considered "private" and there are many circumstances when electronic messages are in danger of being "overheard." Second, the opinion of the American Bar Association, permitting the use of electronic mail is invalid; the ABA fails to understand the technology of electronic mail. More than a decade after the original opinion permitting electronic mail use was issued, it's time for the ABA to reassess their stance on this communication medium and consult more qualified industry experts regarding its safety. Lastly, unencrypted e-mail should not be used for practical and legal reasons. E-mail messages, which are not encrypted, equate to the electronic version of a postcard. There are simply too many situations where either by administrative oversight, advertisers, interceptors, or inadvertent recipients, third parties are able to receive and read the content of e-mail messages. "You've got mail!" Now, just make sure to protect it.

APPENDIX: CASE LAW

APPENDIX: CASE LAW

Nationwide Mut. Fire Ins. Co. v. Harmon, 580 So. 2d 192 (Fla. 4th DCA 1991)

New York v. Belton, 453 U.S. 454 (1981)

Nova Southeastern University, Inc. v. Jacobson, 25 So. 3d 82 (Fla. 4th DCA 2009)

Olmstead v. U.S., 277 U.S. 438 (1928)

Proffitt v. State, 315 So. 2d 461 (Fla. 1975)

Quinones v. State, 766 So. 2d 1165 (Fla. 3d DCA 2000)

Saenz v. Alexander, 584 So. 2d 1061 (Fla. 1st DCA 1991)

Schetter v. Schetter, 239 So. 2d 51 (Fla. 4th DCA 1970)

Smith v. Armour Pharmaceutical Co., 838 F. Supp. 1573 (S.D. Fla. 1993)

St. Paul Fire & Insurance Co. v. Welsh, 501 So. 2d 54 (Fla. 4th DCA 1987)

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

The People v. Diaz, 51 Cal.4th 84 (Cal. 2011)

Trilogy Communications, Inc. v. Excom Realty, Inc., 279 N.J. Super. 442 (Law Div. 1994)

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)

Underwater Storage, Inc. v. U.S. Rubber Co., 314 F. Supp. 546 (D.D.C. 1970)

United States v. Chadwick, 433 U.S. 1 (1977*)*

United States v. Edwards 415 U.S. 800 (1974)

United States v. Robinson, 414 U.S. 218 (1973)

United States v. Ross, 456 U.S. 798, 825 (1982)

W.R. Grace & Co. v. Pullman, Inc., 446 F. Supp. 771 (W.D. Okla. 1976)