Spring 4-22-2003

"Compromised Counsel": The 2001 Patriot Act Policy & Its Effect on Attorney-Client Privilege for Lawyers Using E-mail to Communicate with Clients Online

Patrick J. O'Guinn, Sr.

"Compromised Counsel"

The 2001 Patriot Act Policy & Its Effect on Attorney-Client Privilege for Lawyers Using E-mail to Communicate with Clients Online

Patrick J. O'Guinn, Sr., JD

EMPA 396

Golden Gate University, San Francisco, CA

Dr. Jay Gonzalez

April 22, 2003

"Compromised Counsel"

The 2001 Patriot Act Policy & Its Effect on Attorney-Client Privilege for Lawyers Using E-mail to Communicate with Clients Online

INTRODUCTION

The 2001 USA Patriot Act poses a substantial risk of compromising or waiving the attorney client privilege for lawyers using electronic mail ("email") to communicate with their clients because of the Act's broadly sweeping message interception provisions and the untested "safe harbor" protections for intercepted attorney email communications.

This research paper will examine and seek to answer the following areas of inquiry.

1. Does the USA Patriot Act Policy compromise attorney client privilege when attorneys communicate with their clients using email online?

2. Do lawyers and clients waive their attorney-client privilege by using retail email providers to communicate, in light of the USA Patriot Act non-notice policy prohibitions?

3. Do existing USA Patriot Act policy provisions subject unsuspecting lawyers using email to potential civil and disciplinary sanctions for violation of attorney-client privilege and confidentiality rules?

One basic assumption underlying this research paper is that lawyers are increasingly using the internet to communicate with their busy clients online today (Pikowsky, 1999). This trend should be expected to continue well into the foreseeable

future as email becomes entrenched in our daily lives as a valuable practice tool for convenient and inexpensive client communication. A second underlying premise of this research is that it may be likely that few, if any, practicing lawyers have taken much time out of their busy schedules since October 2001, to seriously reflect upon recently enacted anti-terrorism legislation under the 2001 USA Patriot Act (Patriot Act).

It is against this background of analysis that real possibilities exist under the Patriot Act for the unknowing compromise or waiver of the attorney client privilege during the transmission of a lawyer's email messages, because of the newly established email interception authority granted to the government under the Patriot Act.

Busy lawyers today want to satisfy the needs of busy clients (Harris, p2), and it can be expected that the pragmatic considerations of legal representation will eventually give way to repeated client demands for the transmission of important legal documents by email for review, approval or editing. Accordingly, lawyers who competently adapt to the accelerating rate of the email technological explosion will survive and prosper.

Those lawyers who remain unadjusted by failing to embrace the realities and risks of the new email technology, will almost assuredly experience a slow but seemingly safe demise, free from accusations of electronic malfeasance. The financial lack of profitability and operational inefficiency associated with the traditional practice of law will continue to call into question the wisdom of the pencil, paper and telephone method of practicing law in the electronic age.

Professor Catherine J. Lanctot, in a Duke Law Journal article *Attorney-Client Relationships in Cyberspace: The Peril and The Promise,* summarizes the legal

profession as a "sizeable segment that has never ventured into cyberspace and remains nostalgic for ...parchment and quill pens...yet...ignore cyberspace at their peril [because] much of the legal business of tomorrow could be conducted [on the internet]" (Lanctot, p.2).

Ethical dilemmas surrounding the use of email will continue to challenge and plague the most knowledgeable and careful legal practitioners at every juncture, where grave choices can be made that unintentionally expose client confidences to the general public or governmental monitoring during an electronic transmission by email, fax, telephone, letter or voicemail.

We shall now turn our attention to the 2001 USA Patriot Act as a dramatically broad government policy that is largely publicly uncensored, and directly impinges upon the fundamental cherished American common law and statutory rights of individuals and organizations to preserve their confidential communications between themselves and their lawyers through the use of electronic email messaging systems.

This research paper will review and seek to answer the following research questions:

1. Does the Patriot Act Policy compromise attorney client privilege when attorneys communicate with their clients using email online?
2. Do lawyers and clients waive their attorney-client privilege by using retail email providers to communicate important matters, in light of the Patriot Act interception and non-notification policy prohibitions?

3. Do existing Patriot Act policy provisions subject unsuspecting lawyers using email to potential civil and disciplinary sanctions for violation of attorney-client privilege and confidentiality rules?

Literature Review

The research seeks to address how the Patriot Act may influence the future debate concerning the legalized interception of electronic transmissions, particularly attorney client email. The review of literature examined three areas.

1. The Patriot Act as originally enacted and public reactions to its wide ranging amendments.
2. The U.S. Department of Justice agency perspective on the Patriot Act and related enforcement recommendations.
3. The American Bar Association (ABA) Formal Opinion on email use by attorneys.
4. The purpose and scope of the attorney client privilege
5. The circumstances under which the attorney-client privilege can be waived, lead to disciplinary proceedings, or civil liability.

USA Patriot Act 2001

The USA Patriot Act was enacted on October 26, 2001, as possibly the most far reaching and significant anti-terrorism legislation in recent U.S. history. (Patriot Act) Several provisions that will be discussed in this research paper appear to directly impact attorneys and their clients, as current and potential users of email electronic

communications during the course of the attorney-client relationship.

The seminal government compendium on the enforcement of the USA Patriot Act is the *U.S. Department of Justice Computer Crime Search and Seizure Manual* ("DOJ Manual") revised in 2002 by Nathan Judish, Esquire. (Judish, DOJ Manual). The DOJ Manual was originally authored by Orin S. Kerr, Esquire, a Professor at George Washington University Law School. The DOJ Manual contains important informational resources for law enforcement officers, and prosecutors, that can be analogized in our research paper for use by practicing attorneys to gain valuable insight into the methods that are likely to be used by government agents and prosecutors in gathering, searching and intercepting electronically stored messages under the Patriot Act. (Judish, p.1)

The national applicability of the DOJ Manual 's electronic search and seizure directives, make it a particularly useful starting point for our research analysis and provides key commentary on government Patriot Act enforcement policies applicable to the interception of electronic communications.

Thus, a working definition of what constitutes an "electronic communication" is crucial to an understanding of the potential impact of the Patriot Act, upon electronic communications between attorney and client, covered within the scope of this research paper.

18 U.S. C. Section 2510 (12) defines "electronic communication" in part as :

> Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or part by wire, radio, electronicmagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include

(A) any wire or oral communication…; (DOJ Manual, p.90)

Judish, in the DOJ Manual opines that "most internet communications (including e-mail) are electronic communications" (Judish 2002, p.91) I agree. We will therefore, generally adopt Judish's broadly defined categorization of "electronic communications" in summary, [as transmitted signals delivered through varying mechanisms that affect interstate or foreign commerce]. The U. S. 4th Circuit Court of Appeals in Brown v. Waddell, distinguished the expanded coverage of The Electronic Communications Protection Act, and also defined an "electronic communication" generally consistent with our adopted research definition in this research paper. (Brown, 1995)
No attempt is made here to discuss what not an electronic communication.

Section 2703 of the USA Patriot Act essentially gives government agents [carte-blanche] authority to intercept emails traveling through an Internet Service Provider's (ISP's) computer system anywhere in the country, without necessity of oversight by local authorities, prosecutors or judges. (Judish, 2002 p.72,75), (See also, Patriot Act, Section 2703).

This new approach to the foreclosure of local judicial jurisdiction over electronic message interception cases creates an unsettling and unfamiliar landscape for practicing attorneys to traverse. The question becomes - What court is empowered to hear a request for legal redress where attorney-client emails have been intercepted by the government under the Patriot Act? We may discover that there is no hard and fast answer right now.

On October 3, 2001, Jerry Berman, Executive Director of the Center for Democracy and Technology expressed grave concerns about the passage of the 2001

Patriot Act , in a cautionary tone before a Senate Judiciary Subcommitee on the Constitution & Terrorism. Berman testified that the proposed Patriot Act, [in addition to other proposed post 9/11 antiterrorist legislation would] "allow the government to intercept the content of Internet communications without any fourth amendment protections." (Berman, p.6)

These concerns are not totally unfounded. Professor Susan Herman, of the Brooklyn Law School also questioned the propriety and balance of the USA Patriot Act in her article *The USA Patriot Act and The U.S. Department of Justice: Losing Our Balances?*

Herman illuicated the fact that:

> "most of the provisions [of the USA Patriot Act] amend previous law by adding or deleting words, paragraphs, or sections, forcing people reading the legislation to embak on an elaborate treasure hunt, tracking each amendment back to try to determine its impact on the previous law. In addition, it is difficult to comprehend the new changes if one is not already conversant with the labyrinth webs of law in many different areas." (Herman, p.2)

Following Herman's logic concerning the complexity of the amendments contained in the USA Patriot Act, it becomes increasingly unlikely that busy practicing attorneys using the internet for sending confidential client emails, have stopped to read, digest and appreciate the overall intrusive impact that the USA Patriot Act may have on the clients that they serve, nor its impact on the privileged status of their confidential electronic communications in the future.

Email Communications

The American Bar Association Standing Committee on Ethics and Responsibility (ABA) in a 1999 opinion No 99-413, approved of email as a "reasonable" medium of communication for lawyers, while noting that messages sent by attoneys using email Internet Service Providers (ISP's) may be compromised by:

(1) the ISP's legal, though qualified, right to monitor e-mail passing through or temporarily stored in its network, and (2) the illegal interception of e-mail by ISP's or "hackers" (ABA, p.5).

In a July 1999 article *You've Got Mail: Email Ruled Secure by ABA,* The Internet Lawyer reported that the ABA Opinion No. 99-413, in essence, utilized a "reasonable expectation of privacy" approach in discussing attorney use of email for client communications, while acknowledging that it is nevertheless important for an attorney to consult with a client for direction in circumstances where highly sensitive information is contemplated for transmission (The Internet Lawyer, p1). Furthermore, the committee's opinion was quoted as stating "Whether is it is reasonable for a lawyer to use any particular medium to communicate with or about clients depends on the objective level of security the medium affords and the existence of laws intended to protect privacy..." (The Internet Lawyer, p.1).

The enabling wisdom and advice of the ABA Opinion No. 99-413 has drawn sustained criticism over time, because few courts have had the occasion or inclination to directly rule on email as an appropriate medium for use by lawyers seeking to protect

their attoney-client privilege information online during the course of legal representation. Furthermoe, the ABA opinion, while instructive, does not have the force of law sufficient to serve as a basis for taking any professional action as a lawyer on behalf of a client.

Moreover, despite the increased use of email by attorneys since the publication of the 1999 ABA opinion, the USA Patriot Act presents a rigorously new challenge for all attorneys, with potentially more damaging consequences reaching far beyond the mere prospect of having attorney email messages "hacked' or "illegally intercepted" – they can now be "legally" intercepted by the government.

Privileged Communications

Maryland law, as an example, provides a statutory protection against compelled disclosure of confidential communications between attorneys and their clients. The privilege is codified in the Annotated Code of Maryland, Courts & Judicial Proceedings, Section 9-108 (2002) and reads as follows:

> § 9-108. **Attorney-client privilege**
>
> A person may not be compelled to testify in violation of the **attorney-client privilege** (Md. Ct. & Jud. Proc. Code Ann., 2002).

Court decisions, legal authors and attorneys, frequently cite varying state and federal authorities in acknowledging the attorney-client privilege as being "one of the oldest privileges for confidential communications known to the common law." (Hirshorn, p.1). The Maryland courts have similarly echoed this principle in a more moderate fashion in State v. Pratt , holding that "the attorney-client privilege, deeply rooted in common law, is now memorialized in...[Section 9-108]". (See State v. Pratt, p. 2). Moreover, the court further held in Pratt "that the **attorney-client privilege** is

based upon the public policy that an individual in a free society should be encouraged to consult with his **attorney,** whose function is to counsel and advise him "(Pratt, p.3).

The Pratt case goes even further in explaining that in Maryland "the attorney-client privilege is a rule of evidence that forever bars disclosure, without the consent of the **client,** of all communications that pass in confidence between the **client and his attorney** during the course of professional employment or as an indication of professional intercourse between them (Pratt, p.5). "Or, as succinctly stated in Levitsky v. Prince George's County, "for the purpose of obtaining legal advice "(Levitsky, p.6).

A final amplification under Pratt, is the recognition that:

> "the **attorney-client privilege** is not confined in scope to communications made solely between an **attorney and his client** but includes communications made to agents employed by the **attorney,** such as a stenographer, secretary, clerk, or any employee necessary for effective operation...[embracing at least in criminal cases] those agents whose services are required by the **attorney** in order that he [she] may properly prepare his [her] **client's** case" (Pratt p.4).

It is against this further refined background, that we continue to analyze the effect of USA Patriot Act on the attorney-client privilege online. The DOJ Manual, gives limited attention to the seizure of privileged documents or communications resulting from attorney-client privilege communications, and instead stresses compliance with the Attorney Generals' regulations contained in 42 U.S.C. § 2000aa-11(a) and 28 C.F.R. § 59.4(b), while conditionally acknowledging the existence of narrowly defined exceptions to the seizure of privileged documents or communications under 28 C.F.R. Section 59.4(b)(1) and (2) (DOJ Manual, p.49-50)

Thus, under the DOJ Manual's recommended approach by Judish, a warrant can be used to obtain privileged communications if:

> "using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought; access to the documentary materials appears to be of substantial importance to the investigation; and the application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General. (DOJ Manual, p. 50).

It becomes immediately apparent, that the legal threshold for obtaining a warrant for attorney-client privilege information under the Patriot Act, and in accordance with the guidelines contained in 28 C.F.R. Section 59.4(b)(1) and (2), is very minimal. Moreover, the warrant issuance criteria appears to be subject only to the wide-ranging discretion of an individual prosecutor's interpretation the meaning of [evidentiary] "jeopardy", the subjective importance of the evidence to a particular case, and the arguably vague internal agency standards for warrant issuance approval.

The lack of judicial oversight evident in the warrant issuance process under the Patriot Act should cause great concern in the legal community about the lack of objectivity in determining the requisite probable cause needed before a computer search or email warrant can be issued.

Hence, Judish, seemingly addresses this concern in the DOJ Manual by cautioning law enforcement agents who are considering the seizure of legally privileged computer files, to obtain the services of " a trustworthy third party to comb through the files to separate those files within the scope of the warrant from files that contain privileged material." The "third party would [presumably] provide only those non-privileged items

to a prosecution team after review" (DOJ Manual, p. 50).

In reality, the governmental or court practice of obtaining and searching attorney computers, or intercepting emails has not been standardized. Nor, has it been codified into a predictable practice (Judish, p.50). Consequently, the need practicing attorney must exercise a greater degree of professional responsibility and awareness to wisely choose his or her electronic email delivery systems, Internet Service Providers (ISP's), and the proper computer system configurations for law firm use in providing electronically assisted client representation.

It becomes equally paramount, from a standpoint of defensibility, for practicing attorneys to take the appropriate steps to preserve the attorney-client privilege in some manner by utilizing a segregated email messaging process to "separate " the routine everyday email messages such as lunch invitations and appointments, from the important privileged client representation email transmissions.

It is unlikely; however, that many busy lawyers have considered utilizing a segregated email process of this sort to handle the client emails, due to over- emphasis on the merits of encryption vs. unencrypted emails in the legal community, that has permeated most "instructive" attorney practice literature on the subject to date. Lawyers who fail to employ at a segregated email system for important client emails, will likely leave the determination concerning the disclosure of seized attorney emails to an unwilling judge, a willing prosecutor or an appointed third party. (Judish, p. 50) Neither choice would seem to be a particularly desirable option for an attorney whose email messages have been seized.

By contrast, it seems to follow that practicing attorneys should possess some fundamental ability to meaningfully articulate how their chosen email processes actually

work, before routinely sending off important documents and messages to represented clients.

As to the inevitability of email, Christopher Miller, in his Boston Law Review article *For Your Eyes Only? The Real Consequences of Unencrypted E-Mail In Attorney-Client Communication*, cites author Charles R. Merrill in stating " that it is merely a question of "when, not whether, e-mail will become universal among all lawyers, their clients and judges" (Miller, p.1).

Although many practicing attorneys utilize, and are reasonably familiar with email Internet Service Providers (ISP's) such as hotmail, yahoo, aol, starpower, earthlink, erols, and others, there is very little openly published literature available "in plain view" on commercial retail Internet Service Provider (ISP) websites to apprise subscribing attorneys, about how each Internet Service Provider (ISP) works in cooperation with law enforcement officials in handling client-privilege email message interception requests under the Patriot Act.

On April 19, 2003, I conducted my own empirical, but unscientific, internet field test on a hotmail.com website to ascertain the existence of "plain view" provider policies pertaining to the handling of warrants, subpoenas, and interceptions under the Patriot Act policies. My simple test consisted of signing up for a new *hotmail* email account at www.hotmail.com. While going through the sign up process, I failed to locate any readily identifiable Patriot Act, warrant, or subpoena policies in "plain view" on the retail hotmail web site, notwithstanding my scrolling through the various "terms of use" hyperlinks on the website. That does not mean, however, that no policy exists. It's just that I could not readily find the policy at the time of my new account signup.

Additionally, my empirical field research revealed that when users *log on* to send or read email messages on their hotmail account, an advisory message pops up stating:

> "You are about to leave a secure Internet connection. It will be possible for others to view information you send. Do you want to continue?

(Hotmail, April 2003)

It would seem that the express *hotmail* disclaimer type pop-up advisory message, alone, would be sufficient to dissuade a reasonably competent attorney from using a hotmail email account to communicate with clients concerning confidential attorney-client privilege matters. However, my greater sense of reality leads to the speculation that a lawyer anxious to send or receive an important client email message will invariably click the "yes" button, and send his or her message on, instead of stopping to consider alternative communication mediums.

Similarly, without signing up, I conducted a second field test on April 19, 2003, to review of the *terms of use* policies on the AOL website at www.aol.com , and determined that no information was immediately noticeable concerning the Patriot Act, warrant seizures, or civil subpoena (AOL, 2003)

However, additional research revealed the existence of an AOL *civil legal subpoena policy* on a separate AOL legal department website at http://legal.web.aol.com/aol/aolpol/civilsubpoena.html.

AOL's Civil Subpoena Policy states in part that:

> AOL's Terms of Service provide that AOL will release account information or information sufficient to identify a member "only to comply with valid legal

process such as a search warrant, subpoena or court order . . ." Thus, if you seek such identity or account information in connection with a civil legal matter, you must serve AOL with a valid subpoena.

> ...Upon receipt of a valid subpoena, it is AOL's policy to promptly notify the Member(s) whose information is sought. In non-emergency circumstances, AOL will not produce the subpoenaed Member identity information until approximately two weeks after receipt of the subpoena, so that the Member whose information is sought will have adequate opportunity to move to quash the subpoena in court. AOL invoices for costs associated with subpoena compliance.
>
> ...the Electronic Communications Privacy Act; 18 U.S.C. §2701 et seq., prohibits an electronic communications service provider from producing the contents of electronic communications, even pursuant to subpoena or court order, except in limited circumstances. Further, AOL's e-mail system retains e-mail for a period of only approximately two days after the e-mail has been read. After that time, the e-mail is automatically deleted. Unread and sent e-mail is preserved on our system for approximately 27 days. If a member deletes any e-mail, that e-mail is automatically deleted after 24 hours from the AOL systems. Finally, AOL does not retain the contents of chat room or instant message communications, nor does it store information about member Internet usage or websites visited.
>
> Finally, it is AOL's policy to release information sufficient to identify an AOL member only where the party seeking the information has filed a legal action that implicates the AOL member in some legally cognizable impropriety or wrongdoing. AOL requests a copy of the complaint and any supporting documentation to indicate how the AOL e-mail address is related to the pending litigation. (AOL Civil Subpoena Policy, 2003)

At first glance, it would appear that AOL's civil subpoena policies, if adhered to, provide some degree of protective delay for attorney email subscribers, in cases where law enforcement warrants, or subpoena's have been served upon AOL to obtain subscriber account email communications under the Patriot Act. However, some non-notification provisions of the Patriot Act cast doubt on AOL's actual ability to provide advance notice to a subscribing attorney, in a case of an impending seizure of the

attorney's targeted client email communications.

In this regard, the DOJ Manual is as equally instructive for practicing lawyers whose confidential client emails face the prospect of interception, as it is for law enforcement officials seeking guidance in the appropriate execution of email communication interception warrants, and subpoenas.

Judish, comments in the DOJ Manual that:

"...Every network provider works differently. Some keep records for awhile. Some keep none and others have difficulty meeting the simplest of requests for varying reasons of software, hardware or philosophies. (Judish, p.82).

Conversely, Judish noted that [some] difficulty occurred with the preservation of evidence under Section 2703 of the Patriot Act in obtaining AOL emails, because as of July 2002, "AOL used software that required the resetting of the account passwords when AOL attempted to comply with a Section 2703 governmental request for the preservation of stored email evidence, ..[thereby making it likely to] tip off suspected targets... (Judish, p.82).

Nevertheless, the published AOL legal department website civil subpoena disclosure policies appear to be incompatible with the evidence preservation requirements of Section 2703, and may be equally inconsistent with the actual interception practices reported to be in use by Judish in the DOJ Manual. Lawyers , should therefore cautiously use AOL as their email provider for privileged client communications, until such time that actual practices can be confirmed to be consistent with published AOL legal department website disclosure policy provisions.

Waiver of Attorney Client Privilege

A waiver of the attorney client privilege can occur in many different ways. David Hricik, in his article *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail* contends that state law may be the [linchpin] in determining the existence of, and waiver of the attorney-client privilege for Internet email communications because " under Section 2517(4) of the Electronic Communications Privacy Act, state law defines the scope of any underlying privilege. " Consequently, a fundamental choice of law issue could affect whether an intercepted message was itself "otherwise privileged." (Hricik, P.8).

Hricik, attempts to explain waiver of the attorney-client privilege by further postulating in a circuitous way, that concern for law firm use of computers [in general] in the practice of law may be warranted by the ABA. Likewise, he states, that law firm allowances of access by third parties to its database "are not in any way reasonably analogous to transmitting Internet e-mail". (Hricik, p.7). Unfortunately, Hricik does not go far enough in his analysis to flesh out the protections possibly afforded by the inherent use of computers by a law firm for various aspects of legal representation. More significantly, the Patriot Act had not been enacted when Hricik's article was published in 1998.

It is entirely reasonable to conclude, along with Hricik, that state law may serve as the primary determinant of the existence of the attorney-client privilege for communications between lawyer and client. Maryland's attorney-client privilege law is contained in the Courts and Judicial Proceeding Article of the Annotated Code, and is

certainly proscriptive as to the circumstances under which the privilege exists, and the corresponding conditions under which it may be waived or lost.

The Maryland Court of Special Appeals, in Elkton Care Center Associates, et al. v. Quality Care Management, Inc. invoked an intermediate *three factor standard* in 2002, to determine whether the attorney-client privilege can be lost through inadvertent disclosure during discovery. For the purposes of this research paper, the court's analysis may later prove valuable for the evaluation of email use by attorneys, and accentuate the importance of choosing an appropriate email Internet Service Provider (ISP) for client communications (Elkton Care Center, p.7-8).

The Court in Elkton, relying upon Christopher B. Mueller & Laird C. Kirkpatrick, *Evidence*, § 5.29 at 450-52 (4th ed. 1995), agreed that the loss of the privilege varies with the circumstances of each case and therefore three factors should be taken into consideration by the court:

1. The degree of care and reasonableness apparently exercised by the claimant.
2. The number of inadvertent disclosures.
3. The extent of the disclosures.
3. The behavior of the privilege claimant in taking remedial steps after disclosing material (Elkton Care Center, p.8)

By analogy, it is arguable that the future degree of care exercised by attorneys in the in the selection and use of email to represent their clients, will play an important role in the court's determination of whether an attorney's client email communications are considered privileged from disclosure in the wake of the Patriot Act interception policies.

Lawyers, taking reasonable precautions to use the latest available protective email technological processes, actively engaging in the monitoring of their email messages to

prevent inadvertent disclosure, and implementing segregated email technologies for their messages will facilitate easier judicial review in the event of a disclosure request or interception, and should therefore experience fewer difficulties in meeting the overall due diligence requirements of the legal profession necessitating the preservation of client email confidences.

Notwithstanding the American Bar Association's (ABA's) 1999 affirmation of the attorney use of email, Christopher C. Miller, noted in his article *For Your Eyes Only? The Real Consequences of Unencrypted E-Mail In Attorney-Client Communication*, the existence of relatively questionable case law in place at the time of the ABA's formal email support, and commented that:

> "attorneys should also be aware of the possible malpractice consequences of sending unencrypted e-mail over the Internet. There is still a question "whether a lawyer could be held [civilly] liable for a third party's interception of confidential client information....", and the threat of illegal interception still exists (Miller, p.4).

At the state level, in 1978 the Maryland Court of Special Appeals in Pratt, pointed out that "there is no precise formula for determining whether the **attorney-client privilege** has been waived in a particular case. In deciding this question various factors such as the **client's** intent to waive, fairness, and consistency of conduct must be considered in view of the purpose of the **privilege** " (Pratt, p.6).

Protecting Client Confidences

Under the Maryland Rules, a lawyer must maintain the confidentiality of client information. Certainly, it would arguably be expected that an attorney's voluntary selection of a medium of communication, such as the use of email, might fairly implicate a consideration of whether the attorney acted reasonably under the professional rules in protecting the confidentiality of a client's information in utilizing an unsecure email system where both legal and illegal message interceptions of confidential client communications can occur.

Maryland Rule 1.6 generally speaks to the broad responsibility lawyers have to protect client information and provides:

Maryland Rule 1.6. Confidentiality of information.

(a) A lawyer shall not reveal **information** relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b)..

(b) A lawyer may reveal such **information** to the extent the lawyer reasonably believes necessary:

(1) to prevent the client from committing a criminal or fraudulent act that the lawyer believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interests or property of another;.

(2) to rectify the consequences of a client's criminal or fraudulent act in the furtherance of which the lawyer's services were used;.

(3) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, or to establish a defense to a criminal charge, civil claim, or disciplinary complaint against the lawyer based upon conduct in which the client was involved or to respond to allegations in any proceedings concerning the lawyer's representation of the client..

(4) to comply with these **Rules,** a court order or other law.. (Md. Rule 1.6, 2002)

There are, however, no reported cases to date indicating whether the Maryland courts would even consider an attorneys' unknowing or uninformed use of an unsecure Internet Service Provider's (ISP's) email system to transmit important client communications, to be a violation of the ethical duties required under Rule 1.6, where email is intercepted under the Patriot Act.

However, the lack of any current guiding case law on this point may not preclude the future introduction of evidence in a disciplinary or malpractice proceeding against an attorney, on the required standard of knowledge or expected competency of an attorney in the relevant legal community, where the use of email for transmitting confidential client communications is involved.

The pace of attorney electronic computer competency is still debatably, too slow, to give us any level of industry-wide professional benchmark measurement at this juncture; although the level of electronic computer knowledge for practicing attorneys can be expected to continually increase with the future adaptation of technology by the courts, and the increased use by the general public.

Surprisingly, Table 1 below, illustrates the results of a *Monster.com* online survey of attorney internet use in an article *What Motivates Lawyers?* and reports informative

findings on April 17, 2002 revealing that approximately eighty-six (86%) percent of private practitioners surveyed indicated using the internet for sending and receiving messages (Monster.com, 2002)

Table 1

Monster.com Online Technology Survey

What Motivates Lawyers?

12 Issues in technology

Do you have access to the internet at home	Private Practice	In-house	>25k	25-40k	41-75k	76-120k	121k+
Yes	59%	66%	60%	59%	70%	100%	
No	41%	34%	34%	40%	41%	30%	0%

Over half of all lawyers surveyed have internet access at home with 66% of in-house and 59% of private practice lawyers being online. Frequency of access shows 49% of private practice and 45% of in-house lawyers logging on at least once a day. The most common uses for the internet cited were for sending and receiving information (86% of private practice, 91% of in-house), social purposes (78% of private practice, 76% of in-house), researching competitors (27% of private practice, 19% of in-house), researching clients (38% of private practice, 20% of in-house) and recruitment (24% of private practice, 22% of in-house)…

How do you use the internet	Private Practice	In-house	>25k	25-40k	41-75k	76-120k	121k+
Recruitment	24%	22%	36%	23%	20%	23%	0%
Research on clients	38%	20%	25%	27%	33%	46%	60%
Research on competitors	27%	19%	14%	19%	29%	27%	60%
Social purposes	78%	76%	64%	78%	88%	80%	
Sending/receiving information	86%	91%	82%	88%	86%	8%	100%

Have you ever used the internet to search for a job	Private Practice	In-house	>25k	25-40k	41-75k	76-120k	121k+
Yes	31%	39%	47%	33%	36%	22%	20%
No	69%	61%	53%	67%	64%	78%	80%

The Monster.com online survey, while not scientific, represents a "point in time" indicator of the popularity and use of the internet by attorneys for various professional functions and purposes in the practice of law. This trend can be expected to continue.

Accordingly, R. Scott Simon, quoting Jacob Palme in a 1998 Hawaii Law Journal article *Searching for Confidentiality in Cyberspace: Responsible Use of E-mail for Attorney Client Communications,* suggests :

> that attorneys incorporating email into [their] practice may just have to wait until legislatures and the judiciary address the evidentiary [and ethical] parameters as to when email is an appropriate vehicle for communication with clients (Simon, p.3).

Simon's suggestion for legislative intervention represents a solidly logical, and instantaneous solution, for protecting attorneys who use email to communicate with their clients during representation. Prior to the enactment of the Patriot Act, many commentators on the subject have overlooked this valuable democratic governance tool and have relied too heavily upon the encryption solution. Encryption, in and of itself, offers limited protection for the average practitioner because it is wholly based upon an attorneys' use of the appropriate level of encryption, the reliance upon which overlooks the importance of the actual "processes", procedures and judgment that should used by attorneys to protect client emails online. Simply put, using weak encryption contained in most off the shelf computer programs may correspondingly lead to weak email protection in the current fast-paced technology marketplace.

Similarly, it is the researcher's contention that attorney use of insufficiently

designed email processes is pervasive throughout the entire legal profession, and likewise leads to weak or debatable protection of attorney-client emails today.

Legislative action in codifying the common law attorney-client privilege has been used by many states in recent years to reinforce the strong public policy of promoting unfettered, although not absolute, attorney-client communications between lawyer and client.

Conversely, the enactment of a state statute identifying the use of a preferred *"client privilege email"* ™*protocol*, (Attorneyserver, 2002) on a network, such as the exclusive attorney email processes developed by the researcher author in 2002 provides the following benefits and protections:

> (1) eliminates the transmission of regular email messages by attorneys over the internet (thereby avoiding the possibility of packet sniffers & message interceptions), (2) uses strong RSR encryption or higher, which exceeds the level of protection required for financial institutions, (3) eliminates third party non-attorney Internet Service Providers (ISP's), altogether and is fully administered by the first and only known distributive law firm internet service provider (LISP) for lawyers in the U.S. to date, (4) provides standardized scheduled email purging or "e-shredding" of messages automatically, (5) is exclusively available only to qualified attorney subscribers, not the general public (6) provides digital encryption signature certificates for authentication of email messages,
>
> (7) is owned and managed exclusively by lawyers and law firms in three states (Maryland, Florida, & California), (8) provides "message read"

> receipts to both attorneys and clients (9) and employs a highly segregated email configuration process to eliminate or minimize commingling of routine non-legal email transmissions with *client privilege emails*™ for easy discernment by the courts (Attorneyserver, 2002).

If the specialized *client privilege email* ™*l* process& protocols are legislatively adopted and implemented at the state or national level, then much of the future Patriot Act debate concerning the interception of attorney emails would be abated, because lawyers would be confident in their knowledge of the necessary steps and processes to be undertaken for the protection of their clients' privileged communications online. More importantly, the courts would have greater statutory guidance, understanding, and authority on how attorney-client emails using the *client privilege email* ™*protocol* should be treated.

Use of the legislated *client privilege email* ™*protocol* approach should expand the critical discourse in the legal community concerning client email protection, and should largely end the longstanding, and often misguided, *encryption vs. unencryption* email debate in the field, that has not yielded any positive guidance for practicing attorneys in quite some time. On the contrary, the *encryption vs. unencryption* email debate, while originally necessary for the development of an initial quantum of knowledge and literature in the greater legal community years ago, has largely atrophied and paralyzed the confidence of practicing attorneys desiring to conduct legal business online today.

Moreover, the codification of a *client privilege email*™ protocol would give rise to a greater necessity for law enforcement officials and prosecutors to follow the Department of Justice cyber manual guidelines, and the Attorney General guidelines,

because they would be by necessity, dealing with a law firm knowledgeable in attorney-client privilege and technology law in the first instance, instead of a commonly anonymous third party Internet Service Provider (ISP), whose technological resources, internet technology legal knowledge, and email processes may vary from provider to provider.

Methodology

Overview of the Methodology

My research methodology focused on a review of relevant literature in the field, Maryland statutes codifying the attorney-client privilege, congressional subcommittee testimony, interest group opinions from the American Bar Association Center for Professional Responsibility, and case law explaining the nature of the communication privilege lawyers and their clients enjoy during the course of legal representation.

The greater emphasis was placed on government documents contained in the Department of Justice Cyber Crime Manual of 2002, extracts of the 2001 Patriot Act therein, and scholarly journal articles, to ascertain the overall impact of the 2001 Patriot Act policy upon the attorney-client privilege for lawyers using email to communicate with their clients.

Additionally the researcher's perspectives and experience as a practicing attorney, associate college professor of online instruction in criminal justice and business law at Howard Community College, former law enforcement officer, and developer of the exclusive AttorneyServer.com *client privilege email* ™ process/protocol for lawyers in 2002, were interspersed into the research for practical comparative analysis with the esoteric discourse of the referenced scholarly journal articles.

The researcher's thematic bias is toward progressive technological innovation in the legal field and flows from a perspective that advanced technology and legislated change evidenced by statutes such as the Patriot Act, require new vision and leadership, in an over-controlled and slowly changing legal profession, that remains technically unsophisticated while lingering far behind the times of our technically advanced constituency, and society.

Limitations of the Research

The principle purpose of the research was to explore the effect of the 2001 Patriot Act upon the privilege electronic email communications between attorneys and clients. Therefore, no effort was made to analyze the numerous other legal conflicts inherent in the Patriot Act, except as necessary for a thorough background analysis germane to the three research questions presented by this research paper.

Additionally, the research did not attempt to cover every aspect of how the attorney-client privilege can be waived by an attorney, and highlighted the general premises surrounding a waiver using Maryland statutes and case law as the primary authoritative reference.

The research did not attempt to cover every manner in which an attorney can be subject to disciplinary action for violating the attorney-client privilege or confidences of a client, except to contrast the Patriot Act interception and disclosure provisions with related Maryland Rules of Professional Conduct, the 1999 ABA Opinion of the Center for Professional Responsibility, and related scholarly journal interpretive commentary.

The research also avoided any heavy analysis of the ABA testimony or testimony of interest groups who opposed the Patriot Act, except to discern the existence of some opposition to the Patriot Act as a threat to the attorney-client privilege online, or to elucidate whether the ABA has taken sufficient steps to help guide or protect the attorney-client privilege online against the implications of the existing Patriot Act.

No heavy scientific statistical analysis of attorney email usage habits was presented because the potential market data is too vast for the issues that were covered in this research paper. However, a statistical online survey of lawyers from Monster.com

was referenced as a general barometer of lawyer internet use nationally.

The research, as indicated earlier in this paper, relied heavily upon published provisions of the government Department of Justice Cyber Crime Manual pertaining to the seizure, interception and disclosure of email messages. The focus was almost singularly on the preservation of privilege for attorney-client email transmissions out of the recognition that future challenges to seized or intercepted emails under the Patriot Act are likely to focus on the government's implementation of appropriate policies, practices and safeguards to minimize unwarranted intrusions into the attorney-client privilege territory.

Correspondingly, some attention is given to the necessity for practicing attorneys to consistently use *state of the art technology* to protect their client interests online, without digressing to discuss the unlimited array of electronic communication equipment now publicly available for social discourse such as text messaging, wireless communications (WAP), pagers, removable hard drives, digital telephones, video telephones, video conferencing, voicemail, facsimile, and interactive legal web sites, etc.

Characteristics of the Practicing Attorney Model

The practicing attorney model used for the purposes of this research paper is the solo practitioner, small law firm attorney in a practice of 1-3, or 3-10 attorneys, or medium size law firms of up to 20 lawyers, although the same principles and analysis of this paper will individually and collectively affect large regional and national law firm lawyers as well.

Local Data Collection

A ten (10) item attorney questionnaire was prepared for dissemination as part of this research paper to determine the technological proficiency and Patriot Act knowledge

of identified solo practitioners in Maryland, Florida, and California. The questionnaire presented questions on the frequency of internet use by attorneys, the purposes for which the internet was used by attorneys in their law practices, the frequency of requests from clients for communication by email during the course of representation, and an assessment of the attorney's knowledge about encryption, along with the provisions of the Patriot Act applicable to email seizures/interceptions.

However, time limitations for the completion of this research paper, rendered the use of the survey approach unworkable, and the survey follow-up must therefore take place at a future date and time.

Findings

Compromise of Attorney-Client Privilege

The review of relevant literature lends great credence to support a contention that the Attorney-client privilege email communications may be unnecessarily compromised under the 2001 Patriot Act policy electronic seizure and interception provisions, because lawyers have no established computer framework or electronic email system integrity configuration(s) or protocol standards to use for sending electronic communications (emails) to clients during the course of legal representation. Additionally, Internet Service Providers (ISP's) do not have uniform or reliable subpoena, warrant or interception disclosure policies in place, of which practicing attorneys are likely to be aware of when subscribing for email services, that can routinely be depended upon to protect their privileged email communications.

The newness of the 2001Patriot Act has caused the necessary critical public review by the greater legal community to evade recent discourse, concerning the

unknown, but foreseeable repercussions affecting attorney-client email communications today. Instead, the focus has been only on advanced encryption technologies, and speculative soliloquy by attorneys and law professors on "how the courts might rule" in the future concerning the use of emails by lawyers for important client communications. Reliable predictions in law have been historically based upon prior known legal precedent (decisional law). Minimal persuasive legal precedent exists today in the area of email technology as applied to the attorney-client privilege.

Furthermore, courts historically, do not give advisory opinions. Presumably, this is what keeps the law fluid and dynamic. The answers to the attorney-client email question will ultimately be found in the details of a test case at that reaches the highest levels of the state or federal court, that is both technologically informed, and demonstrates a willingness to critically examine and demystify the common technologies in use by lawyers in society today, such as email, or the new *client privilege email*™ protocol processes developed exclusively for lawyers by AttoneyServer.com, in Maryland.

Email Waiver of the Attorney-Client Privilege under the Patriot Act

The relevant literature suggests that there is no clear consensus for the proposition that the use of email to transmit privileged client communications results in a waiver of the attorney-client privilege. The research shows that while the 2001 Patriot Act policy gives law enforcement officials the expansive authority to intercept attorney email messages, each Internet Service Provider (ISP) as a practical matter, responds differently to the government intercept efforts, or not at all, making email seizure and interception outcomes less predicable than originally perceived at the outset of this research.

Therefore, as to the issue of waiver of the attorney-client privilege, " it just depends on the circumstances." For example, using an Internet Service Provider (ISP), such as America Online (AOL), which at least publicizes a strong subscriber disclosure policy on its legal department website, may not necessarily result in an automatic or eventual waiver of the attorney-client privilege. AOL's strong disclosure "notice to subscriber policy", however, may in practice, be unusable because of the Patriot Act's "non-disclosure to the investigative target" provisions.

The research also reveals that it is hard, on the one hand, for attorneys to argue for the preservation of the client privilege online, while knowingly using anonymous third party Internet Service Providers (ISP's), whose employee "access" to important privileged emails, the subscribing attorney can't control.

At least the Maryland court, may, as a result of a recent 2002 ruling in Elkton Care Center Associates, look at the nature of any email message disclosures, the extent and frequency of the disclosures [or access to the privileged messages by third parties], and the attorney's attempts to remediate, resolve or correct access and disclosure issues.

Such a review may eventually turn on the nature of the email technology being used, in addition to the basis of the judgment used by the attorney in addressing the problem. The AttorneyServer.com *client privilege email* ™ process/protocol uniquely addresses the problematic attorney technology email questions of today, well in advance of any meaningful court inquiry and ruling on the subject. Moreover, the *client privilege email process*™*/protocol* quells the often repeated mantra in the legal community and the information technology (IT) community that "all email is unsecure".

The question to be answered, still remains ; Why should an attorney knowingly put himself or herself in a position of risk to have to defend a decision on the use of a

commercially available, garden variety email process, the security of which he or she does not fundamentally understand or agree with? We can look to technology lawyers seeking new sources of revenue from lawyer misuse of email technology, and future malpractice litigants ensnarled in the vast net of Patriot Act email interception enforcement efforts to help shape this inevitable future debate.

Lawyer Discipline & Civil Liability – Confidentiality Rules

The relevant literature and research does not actually support a current expectation that lawyers using unsecure email to communicate with their clients online may unsuspectingly run afoul of their ethical duty to preserve client confidences, although it was originally suspected that uninformed lawyers may face disciplinary action for selecting and using an unsecure Internet Service Provider (ISP) to send confidential emails to their clients, where unauthorized disclosure or interception under the Patriot Act occurs.

The courts will take some time to catch up with this issue, and must balance the purposes of the professional rules (protecting client confidences) with the realities of the present lack of technological sophistication inherent in basic Internet Service Provider (ISP) emails. However, the research suggests that an untested area which may, nevertheless, be ripe for litigation is the potential for individual civil liability on the part of an attorney for negligently, or without sufficient understanding, utilizing third party unsecure email, in the face of known risks of interception and disclosure under the broad authority granted to the government under the provisions of the 2001 Patriot Act.

In a general sense, ignorance of the law will be no excuse for a lawyer to avoid civil liability for a failure of reasonable performance in protecting client confidences online, particularly given the widespread publicized public outrage expressed by

congressional leaders, public interest groups, bar associations, city governments, librarians, and others based upon the perceived extreme invasion of privacy under the provisions of the Patriot Act, as originally enacted in 2001.

In Maryland, expert testimony is usually required in attorney malpractice cases, to help establish the relevant standard of care in the legal community, where an allegedly negligent lawyer practices law. We must therefore, stay tuned for continuing developments as the 2001 Patriot Act undergoes further revision, as various amendments sunset in December 2004 and beyond.

Areas for Further Research

Informed attorneys should routinely warn their clients, in writing, about the potential damaging consequences (criminal or civil exposure) of communicating with legal counsel by email, and should receive written consent before sending any client communications online.

Additional research is needed in the area of lawyer responsibility for negligently selecting and using e-mail communications that result in the unauthorized or harmful disclosure of attorney client privilege information online. No cases are available on point, and future litigation will reveal that this is a new area ripe for review by knowledgeable and experienced information technology lawyers and judges. Emerging technology courts in many states should evolve to address the standards of practice for lawyers using email to facilitate client representation. However, the focus of the local courts is likely to be on the administration and management of the court judicial processes, and they may therefore limit their attorney guidance to the filing of, and responding to court pleadings.

Although Maryland has announced Elkton Care Center Associates Limited Partnership, as a case of first impression concerning the inadvertent disclosure of confidential or privileged client information, additional research is required for comparison of other jurisdictional approaches to the "inadvertent disclosure" standard, when attorney-client privilege information becomes disclosed, or is likely to be disclosed under the Patriot Act policies.

More empirical information is needed on the on national application and use of the AttorneyServer.com *"client privilege email"*™ process/ protocol developed by the researcher of this research paper, and the value of the Attorneyserver.com email process as an antidote in addressing attorney email communications, and protecting against the unwarranted interceptions and disclosures under the 2001 Patriot Act provisions.

Conclusion and Policy Recommendations

It is imperative for policy recommendations to be made and implemented at the national level to embrace all aspects of the attorney-client privilege; thereby improving national legislation and strengthening attorney-client privilege email protection(s) as codified exceptions to the current electronic seizure, interception and disclosure provisions of the 2001 Patriot Act.

It is similarly imperative that policy recommendations be made and implemented at the state level and local level for improved legislation strengthening, clarifying and providing direct "qualified" privileged communication protection of attorney-client privilege emails, from any seizure, electronic disclosure, wiretap, warrant, interception, or discovery request, if an attorney can demonstrate strict compliance with the established AttorneyServer *"client privilege email"*™ process/protocol, in the local jurisdiction where the electronic communications are sought to be intercepted. This

forward-thinking legislation may establish independent state grounds for the protection of the attorney client privilege emails, notwithstanding the provisions of the Patriot Act.

The qualified privilege from disclosure, would consist of a rebuttable presumption against disclosure, requiring only proof of compliance with the "*client privilege email protocol*" ™. Thereafter, the burden would shift to the party seeking disclosure to present "clear and convincing evidence" to overcome the presumption of privilege.

This legislation will eliminate the inevitable headache for judges who will increasingly have to consider wading through a cache of attorney-client emails, to discern what is relevant from what is not relevant, to any proceeding before the court. It will also place a greater responsibility on practicing lawyers to be careful in their use of the client privilege email system, with a corresponding existing ethical duty to be cautious in their representations to the court, which is governed by the Maryland Rules of Professional Conduct requiring "candor toward the tribunal."

The state or local legislation adoption of the "*client privilege email*"™ *process/protocol* will revolutionize the practice of law, facilitate the technological advancement of the practice of law, positively enhance the administration of justice, advance the technological education of attorneys and judges, while instilling greater confidence in clients that their online confidences with legal counsel are duly protected from unwarranted disclosure.

REFERENCES

American Bar Association Standing Committee on Ethics and Responsibility Formal Opinion No. 99-413. *Protecting the confidentiality of unencrypted e-mail.* (March,1999).

America Online (2003). *website legal department notices*.

AttorneyServer.com (2002). *Client privilege email* by Patrick J. O'Guinn, Sr., Esq, Columbia, Maryland.: Web Author

Berman, J. (2001). Testimony of Jerry Berman, Executive Director of the Center for Democracy and Technology, before the Senate Judiciary Committee on Constitution, October 3, 2001. Washington, D.C.: Author.

Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995).

Electronic Communications Privacy Act, 18 U.S.C. § 2701-12 ("ECPA") (1986), as amended.

Elkton Care Center Associates Limited Partnership t/a Medpointe (Medpointe) v. Quality Care Management, Inc. (QCM), (2002). 145 Md.App. 532.

Harris, B. R. (2001, August). *Counseling clients over the internet*. The Computer & Internet Lawyer.

Hricik, D. (1998, Spring). *Lawyers Worry Too Much about Transmitting Client Confidences by Internet Email* 11. 459 Georgetown Journal of Legal Ethics.

Herman, S. (2001) *The USA Patriot Act and the US Department of Justice: losing our balances?*

Hirshorn, R. A., (2001, Novemer). *ABA statement on monitoring Attorney-Client Communications*,.

Hotmail.com (2003). *terms of use policy.*

Judish, N. & Kerr, O.S. (2002, July). *Searching and seizing computers and obtaining electronic evidence in criminal investigations.* Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, Washington DC: Author

Lanctot , C.J. (1999, October). *Attorney-client relationships in cyberspace:The peril and the promise,* 49, 147. Duke Law Journal.

Md. Courts and Judicial Proceedings Code Ann. § 9-108(a) (2002). *Attorney client privilege*.

Maryland Rules of Professional Conduct, Rule 1.6. (2002). *confidentiality of information*.

Miller, C. C. (2000, April). *For your eyes only? The real consequences of unencrypted e-mail in attorney-client communication,* 80. 613, Boston University Law Review.

Monster.Com (2002, April). *What motivates lawyers?*

Pikowsky, R. A. (1999, Summer). *Privilege and confidentiality of attorney-client communication via e-mail.* Baylor University Law Review, 51, 483.

Pratt v. State, 39 Md App., 442,447 (1978), aff'd 284 MD 516 (1979).

The Internet Lawyer, *You've got mail: Email ruled secure by* ABA, (1999, July). Vol. 5.7.

See 18 U.S.C. § 2510(8) cited in *Lawyers worry too much about transmitting client confidences by internet email* 11. 459 Georgetown Journal of Legal Ethics.

See 18 U.S.C. § 2510(12) (2001) cited in *Searching and seizing computers and obtaining electronic evidence in criminal investigations.*

See 18, U.S.C. § 2517(4) of the Electronic Communications Privacy Act. cited in *Lawyers worry too much about transmitting client confidences by internet email* 11. 459 Georgetown Journal of Legal Ethics.

See 42 U.S.C. § 2000aa-11(a); and 28 C.F.R. § 59.4(b), *Attorney general guidelines,* cited in *Searching and seizing computers and obtaining electronic evidence in criminal investigations.*

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 27 (2001).

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), Section 2703, Part 1 *Crimes, chapter 121stored wire & electronic communications electronic communications & transactional records.pdf.*

Appendix A

Source Information for References Cited

American Bar Association Standing Committee on Ethics and Responsibility Formal Opinion No. 99-413. *Protecting the confidentiality of unencrypted e-mail*, March 10, 1999
American Bar Association World Wide Web page:
http://www.abanet.org/cpr/fo99-413.html

America Online (2003). *website legal department notices*.
AOL World Wide Web page:
http://www.aol.com

AttorneyServer.com (2002). *Client privilege email,* developed by Patrick J. O'Guinn, Sr., Esq.
AttorneyServer.com World Wide Web page:
http://www.attorneyserver.com

Berman, J. (2001). Testimony of Jerry Berman, Executive Director of the Center for Democracy and Technology, before the Senate Judiciary Committee on Constitution, October 3, 2001.
Center for Democracy and Technology World Wide Web page:
http://www.cdt.org/security/usapatriot/testimony.shtm/.

Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995).
Golden Gate University Library (via Lexis Nexis)

Electronic Communications Privacy Act (1986). 18 U.S.C. § 2701-12, amended. ("ECPA").
U.S. Department of Justice World Wide Web page:
http://www.cybercrime.gov/_IIB7

Elkton Care Center Associates Limited Partnership t/a Medpointe (Medpointe) v. Quality Care Management, Inc. (QCM), (2002). 145 Md.App. 532. **Golden Gate University Library (via Lexis Nexis)**

Harris, B. R. (2001, August). *Counseling clients over the internet*. The Computer & Internet Lawyer. **Golden Gate University Library (via Lexis Nexis)**

Hricik, D. (1998, Spring). *Lawyers Worry Too Much about Transmitting Client Confidences by Internet Email* 11. 459 Georgetown Journal of Legal Ethics. **Golden Gate University Library (via Lexis Nexis)**

Herman, S. (2001) *The USA Patriot Act and the US Department of Justice: losing our balances?*
Jurist World Wide Web page:
http://jurist.law.pitt.edu/forum/forumnew40.htm

Hirshorn, R. A., (2001, Novemer). *ABA statement on monitoring Attorney-Client Communications,* **Center for Democracy and Technology World Wide Web page:**
http://www.cdt.org/security/011109aba.shtmlat.

Hotmail.com (2003). *terms of use policy.*
Hotmail World Wide Web page:
www.hotmail.com

Judish, N. & Kerr, O.S. (2002, July). *Searching and seizing computers and obtaining electronic evidence in criminal investigations.* Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, Washington DC: Author
U.S. Department of Justice World Wide Web page:
http://www.cybercrime.gov/_IIB7.

Lanctot, C.J. (1999, October). *Attorney-client relationships in cyberspace:The peril and the promise,* 49, 147. Duke Law Journal.
Golden Gate University Library (via Lexis Nexis).

Md. Courts and Judicial Proceedings Code Ann. § 9-108(a) (2002). *Attorney client privilege*. **Golden Gate University Library (via Lexis Nexis)**

Maryland Rules of Professional Conduct, Rule 1.6. (2002). *confidentiality of information* . **Golden Gate University Library (via Lexis Nexis)**

Miller, C. C. (2000, April). *For your eyes only? The real consequences of unencrypted e-mail in attorney-client communication,* 80. 613, Boston University Law Review.
Golden Gate University Library (via Lexis Nexis)

Monster.Com (2002, April). *What motivates lawyers?*
Monster.com World Wide Web page:
http://www.monster.com

Pikowsky, R. A. (1999, Summer). *Privilege and confidentiality of attorney-client communication via e-mail.* Baylor University Law Review, 51, 483. **Golden Gate University Library (via Lexis Nexis)**

Pratt v. State, 39 Md App., 442,447 (1978), aff'd 284 MD 516 (1979). **Golden Gate University Library (via Lexis Nexis)**

The Internet Lawyer, *You've got mail: Email ruled secure by* ABA, (1999, July). Vol. 5.7. **Golden Gate University Library (via Lexis Nexis)**

See 18 U.S.C. § 2510(8) cited in *Lawyers worry too much about transmitting client confidences by internet email* 11. 459 Georgetown Journal of Legal Ethics. **Golden Gate University Library (via Lexis Nexis)**

See 18 U.S.C. § 2510(12) (2001) cited in *Searching and seizing computers and obtaining electronic evidence in criminal investigations.* **U.S. Department of Justice World Wide Web page:** http://www.cybercrime.gov/_IIB7

See 18, U.S.C. § 2517(4) of the Electronic Communications Privacy Act. cited in *Lawyers worry too much about transmitting client confidences by internet email* 11. 459 Georgetown Journal of Legal Ethics. **Golden Gate University Library (via Lexis Nexis)**

See 42 U.S.C. § 2000aa-11(a); and 28 C.F.R. § 59.4(b), *Attorney general guidelines,* cited in *Searching and seizing computers and obtaining electronic evidence in criminal investigations.* **U.S. Department of Justice World Wide Web page:** http://www.cybercrime.gov/_IIB7.

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). **Center for Democracy and Technology World Wide Web page:** http://www.cdt.org/security/011109aba.shtmlat.

USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), Section 2703, Part 1 *Crimes, chapter 121stored wire & electronic communications electronic communications & transactional records.* **Center for Democracy and Technology World Wide Web page:** http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Final Version