

# FDCC QUARTERLY

## FDCC

FEDERATION OF DEFENSE  
& CORPORATE COUNSEL

**BAD FAITH: THE ADMISSIBILITY OF EXPERT TESTIMONY AND THE CHALLENGES  
THAT FOLLOW**

**Thomas F. Segalla and Joseph M. Hanna**

**DEFENDING COMMERCIAL DAMAGES**

**Lori E. Iwan**

**UNUSUAL FORMS IN THE SURPLUS LINES INSURANCE INDUSTRY**

**Gerald A. Melchiode**

**ETHICS NOW AND FOR THE FUTURE IN OUR HIGH-TECH *EMAIL* WORLD**

**Salvatore J. DeSantis and D. David Keller**

**USE AND ADMISSIBILITY OF HIGH DEFINITION VIDEO VISIBILITY STUDIES,  
COMPUTER ANIMATIONS AND COMPUTER SIMULATIONS**

**David M. Louie, Carlos Rincon, Victor R. Anderson, III and  
Paul Kayfetz**

**NATIONAL INSURANCE ACT OF 2007 & DEMUTUALIZATION OF INSURERS:  
THE DEVIL IS IN THE DETAILS**

**Douglas P. Faucette and Timothy S. Farber**

VOL. 58, NO. 1

FALL, 2007

# Ethics Now and for the Future in Our High-Tech *Email* World<sup>†</sup>

Salvatore J. DeSantis  
D. David Keller

## I.

### INTRODUCTION

Every law office recognizes that the speed, economy and space-saving benefits of email have made it an indispensable tool. Email arguably is the most efficient means of communication yet devised. However, the adoption of email as a principal means of communication presents a variety of ethical considerations for attorneys. Is an email message a confidential communication? Is email part of a client's file that must be retained? Should an email from one client be separated from the rest? Can it be certain that no one is eavesdropping on an attorney-client communication? Does sending an email breach attorney-client privilege? Are there any rules? Are there any limits on using technology in the name of zealous advocacy? This article offers law firms and in-house counsel some guidance and recommendations on how to better use electronic mail in the workplace while safeguarding confidentiality.

## II.

### EMAIL CONFIDENTIALITY ISSUES

#### A. *Case Law*

Confidentiality is the single most difficult ethical challenge for the lawyer who communicates with clients over the Internet. Unfortunately for all, confidentiality is also among the obligations most easily compromised. There are wide varieties of potential eavesdroppers on the Internet. These eavesdroppers are referred to as Hackers, Crackers, Spoofers

---

<sup>†</sup> Submitted by the authors on behalf of the FDCC Construction Section.



*Salvatore DeSantis is a member of the firm of Molod, Spitz & DeSantis, PC. He received his B.A. from the State University of New York at Binghamton and his J.D. from St. John's University. Mr. DeSantis concentrates his practice in the areas of construction litigation, premises liability and insurance coverage. He has vast trial experience and is known for his no-nonsense approach to negotiating cases. Mr. DeSantis also serves as a lecturer on the defendant's perspective in personal injury cases, and as an author on topics such as defense ethics and professionalism. He has earned an AV rating from Martindale-Hubbell and counts his pro bono activities as an advocate for families and small businesses impacted by the September 11 attack as among his most significant*

*He is admitted to practice in the United States District Court for the Eastern and Southern Districts of New York and the District of New Jersey as well as the bar associations of those states. Mr. DeSantis is also a member of the Columbian Lawyers Association, the Defense Research Institute, the Trial Lawyers Association, the Federation of Defense and Corporate Counsel, and the New York State Bar Association.*

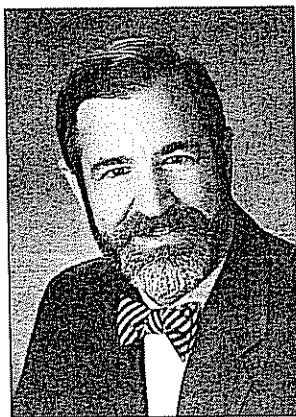
and Sniffers.<sup>1</sup> A Cracker can copy or delete an attorney's email to a client. In addition to cracking emails, a Cracker can also invade firm files that are stored electronically. Capturing information as it is passed over the network is referred to as "sniffing." A "Sniffer" need not know the attorney's password in order to steal the client's secrets. On the other hand, a "Spoofers" operates by having its computer pretend to be that belonging to someone else. This allows the Sniffer to read an email, make a reply, and send it back to the unsuspecting lawyer who remains unaware that he is communicating with an imposter.

Even if a Hacker, Cracker, Spoofers or Sniffer does not invade the privacy of another, whether client or lawyer, it is always possible for someone to access a lawyer's computer password. Once that security is breached, inauthentic emails can be sent in the lawyer's name.

Email can be more easily examined by an outsider while in transit from sender to receiver, as opposed to postal mail, which carries an inherent verification. Without special software (such as Verisign Digital ID(R)), there are few opportunities to know whether an

---

<sup>1</sup> Gary L. Stuart, The Ethics of Email, <http://www.ethicslaw.com/ethics-email.html> (last visited Oct 5, 2007)



*D. David Keller is a shareholder in the Fort Lauderdale firm of Bunnell Woulfe Kirschbaum Keller McIntyre Gregoire & Klein, P.A. He received his undergraduate degree from Florida Atlantic University in 1976 and his J.D. from the University of Florida in 1979. Mr. Keller's practice includes all types of commercial defense litigation, with emphasis on legal malpractice claims. He also has substantial experience with insurance coverage disputes, property insurance, arson, fraud, and bad faith cases. Mr. Keller has tried over 45 cases to jury verdict and handled numerous court trials and arbitration proceedings as well. Mr. Keller is a member of the Federation of Defense and Corporate Counsel, the American Board of Trial Advocates, the Defense Research Institute, the*

*Florida Defense Lawyers Association, and the American Bar Association House of Delegates. Mr. Keller maintains an AV rating from Martindale-Hubbell, and has been named a "Top Lawyer" by the South Florida Legal Guide in 2006 and 2007.*

email has been tampered with or modified prior to receipt by either the attorney or the client. In fact, sender authentication can be difficult through the Internet, even if the sender is known personally and has a long-standing relationship with the recipient, since any person who might acquire the user identification and password of the sender can post mail in the sender's name.

Experience with the written letter is fairly uniform given its standard format: the author's signature at the bottom of the page, a company's letterhead or logo at the top of the page, and a postmark from the post office all support the integrity of the letter as legitimately issued by the named sender. Similarly, with a phone call, the recipient can recognize the caller's voice. A standard, un-encrypted, un-signed email, however, carries none of these features.

No present consensus exists regarding the ethical impact of inadvertent disclosure of confidential data or information, but most courts hold that inadvertent disclosure does not automatically waive the attorney-client privilege.<sup>2</sup> New York Courts have held that email communication is privileged and that only deliberate disclosure waives the privilege.<sup>3</sup>

<sup>2</sup> Bank Brussels Lambert v Credit Lyonnais (Suisse) S.A., 160 F.R.D. 437 (S.D.N.Y. 1995).

<sup>3</sup> Galison v Greenberg, 799 N.Y.S.2d 160 (Sup. Ct. 2004).

Similar to these courts, the United States District Court for the District of Massachusetts, in *Amgen Inc v. Hoechst Marion Roussel, Inc.*,<sup>4</sup> denied defendant's motion to compel the return of inadvertently produced documents in hard copy because the plaintiff failed to take precautions to protect privileged documents.

Given the burgeoning use of electronic communication, however, it is conceivable that other courts may construe a failure to encrypt email as a failure to take the precautions necessary to protect privileged communication. Consequently, the courts could determine that attorney-client privilege is lost when documents are sent to the client via email in clear text. Encryption of email thus may be desirable to avoid a potential loss of privilege. Privacy Enhanced Email (PEM), developed twenty years ago, has the ability to ensure that an email in fact issued from the purported sender. It later evolved into S/MIME (Secure/Multipurpose Internet Mail Extensions).<sup>5</sup>

Some courts also have suggested that the cautionary statement commonly used on facsimile transmissions might be sufficient protection when used for email.<sup>6</sup> Extending that rationale to electronic transmissions, use of the following disclaimer might be effective in protecting confidentiality when placed at the end of an email message:

This email transmission contains confidential information that is the property of the sender. If you are not the intended recipient, you are notified that any retention, disclosure, reproduction or distribution of the contents of this email transmission, or the taking of any action in reliance thereon or pursuant thereto, is strictly prohibited. No warranty is given by sender that this email is free of viruses, interception or interference. Sender disclaims liability for any unauthorized opinion, representation, statement, offer or contract made by the sender on behalf of sender. Sender delegation of authorities, setting out who may make representations or contract on behalf of sender, is available by contacting sender at mail@sender.com. Jurisdiction for all actions arising out of dealings with sender shall lie only in a court of competent jurisdiction of the State of sender.<sup>7</sup>

#### B. *Statutes*

It should be noted that the enactment of state and federal legislation concerning the retention and confidentiality of emails, and/or criminalizing the interception of an email

---

<sup>4</sup> 190 F.R.D. 287 (D. Mass. 2000).

<sup>5</sup> See Nicholas C. Zales, *Lawyer Meets Encryption Software*, *The Internet Lawyer*, Nov. 1999, Vol. 5.11

<sup>6</sup> *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 884 (1997).

<sup>7</sup> Drafted by author DeSantis.

communication, does not resolve the lawyer's higher ethical duty to safeguard a client's confidences. The Electronic Communications Privacy Act (ECPA)<sup>8</sup> criminalizes the interception of email transmissions and also appears to mitigate the risk of losing the evidentiary privilege. In that regard, 18 U.S.C. § 2517(4) provides that, "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [the ECPA] shall lose its privileged character."

In the State of New York, email communications are treated in identical fashion as other attorney client communications. New York law states: "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication."<sup>9</sup> California adopted a similar provision in its Evidence Code:

A communication between persons in a relationship listed in subdivision (a) does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.<sup>10</sup>

### C. *Bar Association Determinations*

State bar associations, ethics committees, and commentators have adopted a variety of positions. These range from a determination that email is not so insecure a medium as to constitute failure to protect client confidentiality obligations, to the determination that email, at least unencrypted email traveling across the Internet, is insecure. Therefore, use of unencrypted email traveling across the Internet may, in some cases, risk both a waiver of the attorney-client privilege and a breach of the lawyer's ethical obligations to protect a client's confidential information.

Some state bar ethics committees have opined that email communications are only entitled to the attorney-client privilege if the client signs an express waiver.<sup>11</sup> And the Bar Associations of Illinois, North Dakota, South Carolina and Vermont have concluded that

<sup>8</sup> 18 U.S.C. 2510-2522 (1994)

<sup>9</sup> N.Y. C.P.L.R. § 4548 (McKinney 2007)

<sup>10</sup> Cal. Evid. Code § 917(b) (West 2007)

<sup>11</sup> The ethics opinions of a particular bar association are available at <http://www.bestcase.com/statebar.htm>.

the use of unencrypted email does not violate obligations to treat client communications as confidential.<sup>12</sup>

ABA Model Rule 1.6 precludes a lawyer from disclosing information relating to representation of a client unless the client consents after consultation (DR 4-101). In discussing the various factors affecting the confidentiality of un-encrypted email communications, the ABA Committee on Ethics and Professional Responsibility notes:

When the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult the client as to whether another mode of transmission, such as special messenger delivery, is warranted. The lawyer then must follow the client's instructions as to the mode of transmission.<sup>13</sup>

As noted by the Massachusetts Bar Association Committee on Profession Ethics, the employment of a third-party software vendor further complicates this responsibility:

A law firm may provide a third-party software vendor with access to confidential client information stored on the firm's computer system for the purpose of allowing the vendor to support and maintain a computer software application utilized by the law firm. The law firm's clients are deemed to have "impliedly authorized" the firm to make their confidential information accessible to the vendor pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients. However, the law firm must "make reasonable efforts to ensure" that the conduct of the software vendor (or any other independent service provider that the firm utilizes) "is compatible with the professional obligations of the lawyer[s]," including the obligation to protect confidential client information reflected in Rule 1.6(a).

---

<sup>12</sup> See North Dakota State Bar Ass'n, Ethics Comm., Op. 97-09 (1997); South Carolina Bar, Ethics Advisory Comm., Op. 97-08 (1997); Vermont Bar Ass'n, Comm. on Professional Responsibility, Op. 97-5 (1998); Illinois State Bar Ass'n, Comm. on Professional Responsibility, Advisory Op. 96-10 (1997). Other ethics committees which have considered this or analogous issues have reached inconsistent conclusions. Compare Az. Op. 97-04 (1997) (email may pose a risk to confidentiality); Iowa Op. 96-1 (1996) (attorneys must obtain waiver from clients as to email security risk); N.Y. City 94-11 (1994) (advising that an attorney should use caution and consider security measures when speaking to a client via cordless or cellular telephone because of the risk that client confidences or secrets may be overheard); *with* D.C. Op. 281 (1998) (no per se rule barring use of unencrypted internet email to transmit client confidences); South Carolina Op. 97-08 (1997) (examining the privacy of internet communications in view of current technology and laws prohibiting interception or monitoring of email communications, and concluding that internet users may have a reasonable expectation of confidentiality); Vt. Op. 97-5 (1997) (email may pose no risk to confidentiality).

<sup>13</sup> ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413 (1999).

The fact that the vendor will provide technical support and updates for its product remotely via the Internet does not alter the Committee's opinion<sup>14</sup>

As Internet communications become more ensconced in daily life, the legal profession runs the risk of seriously underestimating the breadth of its responsibility to safeguard the confidentiality of attorney-client communications.

D. *Erroneous Receipt of an Adversary's Confidential Email Communications*

Depressing the "send" button too quickly—or failing to realize that "reply to all" has been engaged—is not an uncommon experience. That situation is equally troublesome when the attorney receives an adversary's email transmission in error.

Citing the Committee on Professional and Judicial Ethics of the Bar Association of New York City and an opinion of the New York County Bar Association, a New York trial court observed that the same result obtains whether the issue involves an email message or any other communication that a lawyer knows or should know contains privileged material. The email is to be returned to the sender without first duplicating the message, and the attorney must inform any other of his or her recipients to do the same.<sup>15</sup>

### III.

#### RETAINING AND ORGANIZING EMAIL

There appears to be no published authority that addresses the retention of law office emails. The American Bar Association Model Rules of Professional Conduct require that attorneys retain client files for five years after termination of the representation. Presumably, this rule requires the retention of email messages for the same period of time. But how does one retain an email message?

Electronic messages are received in an "inbox" folder. Email messages which are transmitted through email programs such as "Outlook" or web-based email providers such

---

<sup>14</sup> Massachusetts Bar Ass'n Comm. on Profession Ethics Op. 05-04 (2005).

<sup>15</sup> *Galison v. Greenberg*, No. 602478/04, 2004 N.Y. Misc. LEXIS 2550 (N.Y. Sup. Ct., N.Y. County Slip Op. 51538U, Nov. 8, 2004) (citing Committee on Professional and Judicial Ethics of the Ass'n of Bar of the City of N.Y., Op. 2003-04, 2004 WL 837937 (2004), and N.Y. County Lawyers Ass'n Comm. on Prof. Ethics Op. No. 730, 2002 WL 31962702 (2002)). See also ABA Comm. On Ethics and Professional Responsibility, Formal Op. 05-437 (2005), *Inadvertent Disclosure of Confidential Materials*: "A lawyer who receives a document from opposing parties or their lawyers and knows or reasonably should know that the document was inadvertently sent should promptly notify the sender in order to permit the sender to take protective measures."

as “Yahoo” or “Hotmail” are also lodged in one’s “sent” folder. Unlike a letter sent through ordinary postal mail, there is no copy that is “filed” with a particular case. Since telephone conversations are not routinely recorded and memorialized as part of a client’s file, it may be that email messages need not be filed either since email is nothing more than a convenient way of placing a telephone call. However, the similarity may lose force because, unlike telephone calls that are not retrievable unless recorded, email messages are recoverable from backup systems such as tapes and optical discs, even when discarded as “trash.” Any distinction between email and regular mail may be entirely illusory. As noted in the Restatement of the Law Governing Lawyers, attorneys may have some obligation to retain and file these messages into respective client files:

The American Bar Association Model Rules of Professional Conduct, Rule 1.15(a), requires lawyers to hold client property separate from the lawyer’s own property. Rule 1.15 (a) states: “A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property.” If personal emails are being received in an “inbox folder” simultaneously with a multitude of client emails, then they are being commingled arguably in violation of DR 1.15. Consequently, an office procedure should be put into place for separating (filing) emails into individual client files and personal emails into personal files. No law office receives snail mail and piles it into one massive depository. Rather, snail mail gets logged in, given to the handling attorney and then filed into the appropriate client file. The same should be done with email. The American Law Institute provides some guidance, although email is not specifically referenced: “A lawyer must take reasonable steps to safeguard documents in the lawyer’s possession relating to the representation of a client or former client.”<sup>16</sup>

The Restatement also provides useful parallel commentary regarding a lawyer’s duty to safeguard documents: “A lawyer must maintain an orderly filing system, with each client’s documents separated and with reasonable measures to limit access to authorized firm personnel.”<sup>17</sup>

There is no way of predicting whether a particular Grievance Committee will adjudge the commingling of email messages to be an ethical violation. However, since the courts have imposed discovery obligations on firm clients to furnish email communications, as noted in the discussions below, it would seem a logical extension to impose on the lawyer an ethical obligation requiring the creation of an office procedure that maintains email mes-

---

<sup>16</sup> RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 46(1) (2000)

<sup>17</sup> *Id.* §46(b).

sages in accessible format. Because of new technology, courts are confronting these issues as matters of first impression, meanwhile seeking guidance from each other:

Neither the Fifth Circuit Court of Appeal nor any district court within the Fifth Circuit has had the opportunity to directly address the standards for preservation of electronic evidence and applicable sanctions where such evidence has been spoliated. The Court must therefore look to persuasive authority from other jurisdictions in deciding the present motion. The cases which have been recognized as setting the benchmark standards for modern discovery and evidence-preservation issues are the series of *Zubulake* decisions out of the Southern District of New York.<sup>18</sup>

In *Zubulake v. UBS Warburg LLC*,<sup>19</sup> a case that determined matters of discrimination and illegal retaliation, United States District Judge Shira A. Scheindlin wrote:

[t]he world was a far different place in 1849, when Henry David Thoreau opined (in an admittedly broader context) that ‘the process of discovery is very simple.’ That hopeful maxim has given way to rapid technological advances, requiring new solutions to old problems. The issue presented here is one such problem, recast in light of current technology: To what extent is inaccessible electronic data discoverable, and who should pay for its production?<sup>20</sup>

Though it concerned discovery issues, the *Zubulake* case focused those issues in the context of law firms and in-house counsel. When confronting disputes about the scope and cost of electronic data discovery, it was potentially necessary to thoroughly understand the responding party’s computer system with respect to active and stored data. For data that was maintained in accessible format, the usual rules of discovery applied.

Although not yet specifically addressed by the courts, it would appear to be prudent that emails which arrive or are sent in regard to the file of a particular client should be managed by a system that stores and retains such email communications separately from personal email and separately from other cases handled by the attorney. There are software programs available which actually make it easy to organize client-related emails by client. For example, one specific case management program (*TimeMatters*) can easily “connect” emails sent or received regarding a specific case to the correct individual digital file for that client by means of a simple process which also identifies the office file number for each specific

---

<sup>18</sup> *Consol. Aluminum Corp. v Alcoa, Inc.*, 244 F.R.D. 335 (M.D. La. 2006)

<sup>19</sup> 217 F.R.D. 3091 (S.D.N.Y. 2003).

<sup>20</sup> *Id.* at 311

email. Thereafter, any authorized attorney on the network can easily retrieve all the emails sent or received on that case, along with all the word processing documents created for that client.

#### IV. ZEALOUS REPRESENTATION AND EMAIL “METADATA”

Modern computer technology enables sophisticated users who receive documents by electronic transmission to “get behind” what is visible on the computer screen and determine, among other things, at what stage revisions were made. Sometimes even the authors of those revisions can be identified. This information is referred to as “metadata,” i.e., data about data. Use of this technology would enable a lawyer who receives email and electronic documents from opposing counsel to obtain various kinds of information that the sender did not intentionally make available to the lawyer. For example, a lawyer who has received the final draft of a contract from counsel for a party with whom the lawyer is negotiating would be able to see prior drafts of the contract and, perhaps, even learn the identity of those who made the revisions without the knowledge or consent of the sending lawyer. An effective process for “blocking” recipients from access to deletions and prior versions of the “visible” document remains unclear and a matter of debate among sophisticated computer users and users of software programs that purport to wipe documents clean of metadata.<sup>21</sup>

Incredibly, it is also possible for an email sender to determine the subsequent route of an email (including comments inserted by the ultimate recipients) through software applications or “bugs” inserted surreptitiously into an email sent to opposing counsel. The email sender actually can ascertain the identity of those with whom the first recipient shares the message and also learn their comments. Even if a user avoids applications that make it possible to receive such “bugged” messages, the recipient’s forwarded messages can still be traced if the recipient forwards the message to someone who has not taken such protective measures. Accordingly, it is nearly impossible to render one’s email system “bug-proof.”<sup>22</sup>

Of course, a zealous lawyer’s use of available technology to surreptitiously examine and trace email and other electronic documents in the manner described may not be ethical. In fact, the practice is proscribed by the New York State Bar Association’s Committee on Professional Ethics:

---

<sup>21</sup> See, e.g., M. David Stone, *Deleting Your Deletions*, P.C. MAGAZINE, Nov. 20, 2000; N.Y. State Bar Assoc. Comm. on Professional Ethics, Op. 749 (2001).

<sup>22</sup> See [www.privacyfoundation.org/privacywatch](http://www.privacyfoundation.org/privacywatch), *Email Wiretapping*, posted Feb. 5, 2001.

We believe that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a "secret" of another lawyer's client would violate the letter and spirit of these Disciplinary Rules. *Accord MMR/Wallace Power & Indus. Inc. v. Thames Assocs.*, 764 F. Supp. 712, 718-19 (D. Conn. 1991) . . . In the present inquiry, although counsel for the other party intends the lawyer to receive the "visible" document, absent an explicit direction to the contrary, counsel plainly does not intend the lawyer to receive the "hidden" material or information about the authors of revisions to the document. To some extent, therefore, the "inadvertent" and "unauthorized" disclosure cases provide guidance in the present inquiry. . .

First, to the extent that the other lawyer has "disclosed," it is an unknowing and unwilling, rather than inadvertent or careless, disclosure. In the "inadvertent" and "unauthorized" disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.

Nor need we balance the protection of confidentiality against the principles of zealous representation expressed in Canon 7. Our Code carefully circumscribes factual and legal representations a lawyer can make, people a lawyer may contact, and actions a lawyer can take on behalf of a client. Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy.<sup>23</sup>

It should be noted as well that the use of email "bugs" may violate federal or state laws prohibiting unauthorized interception of email content.<sup>24</sup>

---

<sup>23</sup> N.Y. State Bar Assn. Comm., on Professional Ethics, Op. 749 (2001)

<sup>24</sup> See, e.g., Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522

V.  
CONCLUSION

Email allows for high-speed attorney client communication that was unimaginable twenty years ago. All attorneys now have the ability to communicate instantly with clients through the lick of a mouse. As the speed by which information travels increases, the lines of confidentiality can become blurred. Therefore, with each technological advance, attorneys must carefully reflect on the rules of ethics to insure that client confidences are properly maintained. The risk otherwise is a call to respond when the client seeks redress through a state bar grievance committee.

*The Federation of Insurance Counsel was organized in 1936 for the purpose of bringing together insurance attorneys and company representatives in order to assist in establishing a standard efficiency and competency in rendering legal service to insurance companies, and to disseminate information on insurance legal topics to its membership. In 1985, the name was changed to Federation of Insurance and Corporate Counsel, thereby reflecting the changing character of the law practice of its members and the increased role of corporate counsel in the defense of claims. In 2001, the name was again changed to Federation of Defense & Corporate Counsel to further reflect changes in the character of the law practice of its members.*

The FEDERATION OF DEFENSE & CORPORATE COUNSEL QUARTERLY, published quarterly through the office of publication by the Federation of Defense & Corporate Counsel, Inc. 11812 North 56th Street, Tampa, FL 33617.

All inquiries as to subscriptions or back issues should be addressed to the Executive Director - FDCC, 11812 North 56th Street, Tampa, FL 33617.

**Subscription Rates:** Non members \$60 00 per year or \$15 00 per copy (International - \$70 00) College/University/Law School Libraries \$50 00 per year or \$12 50 per single issue (International - \$60 00)

Entered as Periodicals matter at Tampa, Florida and additional mailing offices.

Manuscripts and correspondence relating to the submission of articles for possible publication should be sent to the Editor, Professor John J. Kircher, Marquette University Law School, 1103 West Wisconsin Avenue, P.O. Box 1881, Milwaukee, WI 53201-1881. All other correspondence should be directed to the Executive Director.

Views expressed by authors are solely their own and do not necessarily reflect the position of the Federation, its Officers, or the Editor.

The FDCC is pleased to provide electronic access to Quarterly articles from 1997 to present at its Internet website. [www.thefederation.org](http://www.thefederation.org)