IN THE SUPREME COURT OF FLORIDA

IN RE: AMENDMENTS TO THE FLORIDA RULES OF JUDICIAL ADMINISTRATION, etc.
_____/

Case No. SC10-2101

COMMENT FROM KURT E. LEE

For the reasons set forth below, I oppose the adoption of proposed Rule of Judicial Administration 2.516 and its mandate that all filed papers be served by litigant/attorney-controlled email.

This Honorable Court should, instead, ensure that all County Clerk of Court electronic filing processes comply with Policy 8.2 of the Electronic Filing Committee's E-Filing Operational Policies for Florida Statewide Electronic Filing Portal document which provides for email notice of and secure Internet access to all filed papers.

I. Email's Delivery And Security Problems Should Prevent Adoption Of Rule 2.516

A. Delivery Problems

The Out-of-Cycle Report Of The Florida Rules Of Judicial Administration Committee On Email Service And Conforming Changes In The Other Court Rules Of Procedure ("Petition") gives short shrift to the problems associated with email. The Petition dismissively notes that "some lawyers have expressed concern that email might not be received even though it is sent (just as United States mail is

sometimes not received even though it is mailed)." (Petition, p. 20) There are, however, far more transmission hurdles for email to clear than there are for regular mail.

After one clicks "send," an email begins to travel from the individual's email program to the identified recipient but, if the user is part of a private network, the email might never make it past the network's firewall. (John Garcia Affidavit)(copy attached as Exhibit "A") If the email makes it out of the office, it, or parts of the email,[1] might, among other problems, be ensnared by the internet service provider ("ISP"), caught by a "blacklist," intercepted by a spam filter, deposited as "junk," or blocked by a fire wall. (*See* Garcia Aff.)

The Petition makes the unsupported statement in the Petition that "the delivery of email is as successful, and probably significantly more successful, than the use of United States mail." (Petition, p. 20) If, however, the Court is going to rely upon anecdotal evidence for such an important rule change, then I would respectfully note that I can count on one hand how many times mail has been lost,

---

[1] After a user clicks "send," an email message is broken down into smaller pieces or "packets" of a few hundred bytes in size. Each packet is wrapped in an envelope containing the IP address and protocol to use and then sent to its destination using the best available route. This is determined by the network and is not part of the packet itself. Packets may take different routes to their destination. When the packets arrive, they are reassembled so the complete email message can be viewed. (Garcia Aff. ¶ 4)

but I would need to use both hands and take off my shoes to start counting how many times emails have been lost. My experience with lost emails is not unique.

The Economist's science and technology blogger recently noted that

> … more of my e-mail has gone astray in the last year than in the 25 years that came before. … And a poll of many friends and colleagues says [his] experience is both common and recent. *E-mail is losing its predictability*.
>
> ***
>
> … from my own experience and stories I hear from fellow hoary internet veterans, something has broken. Many dozens of emails I've sent in the last year have never reached even a recipient's filtered folder. A few weeks ago, a note about compensation failed to reach the editor of this blog. (Yes, I believe him. Why do you ask?) Likewise, many messages never arrive into my inbox or spam folder. No rejection message arrives, to be decoded; no ham waits to be discovered among the spam. *Mails are simply disappearing*.
>
> … I believe that the complexity of getting through a spam-filter maze with ever more dead ends is a key cause. When you put together many rules and different systems, some of which are not specifically designed to work with each other, unexpected properties emerge. This is much how intelligence may work, at a vastly more complicated scale. But certainly, emergent properties make it difficult to predict how a given input will be output.

Posting of G.F. to Babbage blog, "The emerging ambiguity of e-mail," http://www.economist.com/blogs/babbage/2010/12/over-eager_spam_filters (Dec.

15, 2010, 00:56 EST)(emphases added)(a copy of this blog posting is attached as Exhibit "B").

Until email is demonstrated to be at least as reliable as regular mail, email alone[2] should not be an acceptable method of service and it certainly should not be made the exclusive method of service of filed papers.

B. Security Problems

At various stages of an email's journey, the email and the PDF files attached to it, might be intercepted and examined by unauthorized third parties for "sniffing."

> Sniffing in this context means the surreptitious planting of software on a router to intercept e-mail traveling through a router on its way to the recipient. The routers on which packets travel very briefly hold the packets intended for another router further down the line on the Internet, closer to the recipient. For example, routers on the "backbone" of the Internet look at and move millions of packets of information *every second*. Capturing this information as it is going through these intermediate

[2] Since 1992, papers may be served by facsimile. Fla. R. Civ. P. 1.080(b)(5). But, "[w]hen service is made by facsimile, a copy shall also be served by any other method permitted by this rule." *Id.* Facsimile transmissions are far more predictable and reliable than email because the sender of a facsimile transmission receives an error report or his fax machine will issue an "alarm" when something goes amiss. If service by facsimile has required a "back up" method of service for almost two decades – and will still require a back up method under proposed Rule 2.516(b)(2)(E) – service of papers by email should also be accompanied by some other method of service.

> routers is called "sniffing." Sniffers use software to search for unencrypted e-mail destined to or from certain hosts and copy the message as it goes through the router.

David Hricik & Amy Falkingham, *Lawyers Still Worry Too Much About Transmitting E-Mail Over The Internet*, 10 J. Tech. L. & Pol'y, 265, 277-78 (2005)(emphasis in original; internal citations omitted). A Google search for "email sniffer" provides a long list of programs which purport to intercept and sniff emails. (*E.g.*, http://www.downloadatoz.com/download/87091,intercept-email.html).

In addition to "sniffers," other potential email eavesdroppers are the network managers who own the routers through which email network packets travel. "[R]outers are owned by third parties without any contractual obligation of confidentiality to the sender or recipient of the e-mail." Hricik, *supra* at p. 277.

Even the authors of *Lawyers Still Worry Too Much About Transmitting E-Mail Over The Internet* acknowledge the security risks attendant with email. Although these authors focus upon the difficulty of intercepting a single email to support their argument, they are careful to exclude "a deliberate and sustained attempt to intercept a lawyer's messages." *Id.* at p. 290. It is the "deliberate and sustained attempt to intercept a lawyer's messages," however, about which this Court should be concerned.

Indeed, the proposed Rule 2.516, in conjunction with Rule of Judicial Administration 2.420, makes it easy for hackers to separate the wheat from the chaff. The proposed Rule 2.516 requires that all lawyer emails with court filings be readily identifiable by having "SERVICE OF COURT DOCUMENT" as their subject. Emails and their attachments transmitting court filings with confidential information will then include a "Notice of Confidential Information Within Court Filing." *See* Fla. R. J. Admin. 2.420(d)(2). Hackers who make a "deliberate" effort to search for emails with these two items should find it relatively easy to obtain confidential information which might be used for identity theft or other illicit purposes. The Petition fails to consider any of these security threats.

In addition to the threats posed by individual eavesdroppers, a lawyer's ISP can monitor emails. Even proponents of increased email usage provide that "the lawyer must ensure that his ISP abides by strict policies against monitoring e-mail, and he should consider advising his client to confirm the same with respect to the client's ISP." Hricik, *supra* at p. 277.

Given the obligations upon Bench and Bar to preserve and protect confidential information and the requirements of Rule of Judicial Administration 2.420, it is ill-advised to mandate an exponential increase in email traffic with PDF files including confidential information.

C. Email Viruses And Worms

Computer viruses and worms are most commonly delivered through email. Simply clicking on a link in an email can initiate a new virus or worm. *See e.g.*, Jeremy A. Kaplan & Jana Winter, *Beware of Link: E-Mail Virus Plays Havoc With Internet*, foxnews.com (Sept. 10, 2010) (http://www.foxnews.com/scitech/2010/09/09/beware-link-e-mail-virus-plays-havoc-internet/). It is also possible to becoming infected with a virus or worm simply by opening an email.

The proposed new rule is ill-advised because it requires attorneys to be more willing to "open" emails, including emails from unknown senders. One can readily imagine an attorney opening an email containing a virus – even though she did not recognize the sender – thinking that the email was from a staff member in an opposing counsel's office or that opposing counsel was using a different email address. The proposed new rule threatens to increase viruses and the office disruptions and costs attendant with a computer virus and worm "infections."

II. Rule 2.516 Should Not Be Adopted Because Of The Burdens It Will Impose Upon Attorneys And Their Clients

A. The "Bad Man"

In his The Path of the Law, (1897), Oliver Wendell Holmes, Jr., wrote:

> If you want to know the law and nothing else, you must look at it as a bad man, who cares only for the material

> consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience....

Given the email delivery problems described above, one may readily posit there will be a greater rate of attorneys who, intentionally or unintentionally, claim to have served material which was not received or claim to have not received served material. Indeed, the number of claims will certainly be greater with email service because more attorneys might make such claims without involving support staff. In the few instances in my career where there was a question about whether something was served or not received by mail, the issue has always generated affidavits from attorneys and their support staff regarding how mail is handled in their offices. Email simply does not involve as many "hands," making it far easier for unscrupulous attorneys to prevaricate.

Proponents of the new Rule will respond that the onus is upon the sending attorney to confirm delivery. This requirement does nothing for the "bad man," but it makes service by email far more onerous on the scrupulous attorney than current methods of service. If a recipient fails to confirm delivery by issuing a receipt to the sending "good man," then there is little reason to expect the recipient to acknowledge a subsequent email seeking to confirm the prior email's receipt. Thus, the conscientious lawyer will need to call or send an additional copy of the

emailed paper via fax, mail, or personal delivery to confirm email service. Careful attorneys will also need to regularly monitor their court dockets to ensure that they have received everything opposing attorneys have filed. The confirmation process which will be required for email service will have the unintended consequence of making the practice of law more difficult.

The new Rule's reliance upon the parties to serve items by email needlessly invites dishonesty and needlessly complicates and increases the costs of practice for conscientious counsel.

B. User Error

Given the ease by which an email might be sent to an unintended recipient, it is ill-advised to force people to send emails. An attorney typing a few letters into the "to" space may be quickly "aided" by Microsoft Outlook because it can automatically complete the name of the potential email recipient. However, Outlook may select a similarly named recipient as opposed to the actual name of opposing counsel. An attorney might also incorrectly enter the name of the intended recipient and inadvertently disclose a client's confidential information. *See e.g.*, Posting of "bkl" to http://www.google.com/support/forum/p/gmail/thread?tid=0e4aafab4d59d5aa&hl=en (Jan. 6, 2010)(client describing his attorney's disclosure of confidential information by incorrectly addressing email).

While all attorneys have an ethical obligation to be careful with confidential information, it is too easy to inadvertently do the wrong thing with email.

C. User Burden

The proposed Rule provides no relief or safe harbor for those attorneys who opt not to use email[3] or do not have a document scanner. The costs associated with maintaining an email account with the software necessary to filter spam and identify viruses is not insubstantial. In addition, users, to better avoid being "blacklisted," may need to obtain a more expensive static (as opposed to dynamic) IP address. *See e.g.*, Posting of Chuck Redman, "Troubleshoot - Understanding Causes Of Lost Emails," to http://www.zen-cart.com/wiki/index.php/Troubleshoot_-_Understanding_Causes_Of_Lost_Emails (Feb. 27, 2010, 23:19). Likewise, it is undeniable that there are costs associated with purchasing and maintaining a document scanner. The attorneys who do not have an email account or who do not have a scanner certainly should not be required to incur – particularly in this difficult economy – the costs associated with obtaining and maintaining these items.

---

[3] The proposed Rule only permits attorneys to avoid email service if they serve a motion and demonstrate that they have no email account *and* lack access to the Internet. This exception is illusory because everyone in Florida has "access" to the Internet through telephone lines, TV cable, fiber optics, cell phones, or satellite dishes.

Another burden results from the interaction between the proposed Rule and The Florida Bar's ethical guidelines. In Florida Ethics Opinion 00-4, the Bar determined that attorneys were required to follow their clients' instructions before transmitting "highly sensitive" emails. More specifically, the opinion stated that an attorney "should consult with the client and follow the client's instructions before transmitting highly sensitive information by e-mail." Florida Eth. Op. 00-4 (July 15, 2000). Proposed Rule 2.516(b)(B) only excuses email service with a court's permission. Thus, the proposed Rule imposes the costs of motion practice upon clients who do not want their "highly sensitive" information sent via email.

The proposed Rule is unnecessarily expensive for attorneys and their clients.

III. Electronic Delivery Of Filed Documents Through A Clerk Controlled System Avoids The Pitfalls Of Litigant Controlled Email

In 2006, this Court established the Electronic Filing Committee ("EFC"). Admin. Order SC06-3. The EFC produced the E-Filing Operational Policies for Florida Statewide Electronic Filing Portal document (a copy of which is attached as Exhibit "C"). E-Filing Operational Policy 8.2 provides that parties who are approved for electronic filing "shall" be served with filed papers by electronic means. As papers are e-filed, the Electronic Court Filing or "ECF" system emails notice of the electronic filing to the pertinent ECF participants. This procedure is the same procedure that has long been employed by Florida's federal courts.

Policy 8.2 should be the manner by which Florida's state courts adopt electronic service of papers because this Policy avoids the problems described above.

Delivery Problems – With each Clerk's website being the known and identifiable sender of all court-related emails, the recipients may make the way clear for such emails by ensuring that such sender is not blocked by a firewall or relegated to spam or junk mail status. The Clerk's sending email address, as a government address, is not likely to be blacklisted nor is the Clerk's ISP likely to block its emails.

Security Problems – With e-filing, confidential documents are filed through the e-portal and not via email. As a result, there is nothing to be intercepted and the risk of inadvertently sending confidential information is extinguished. While third parties might yet eavesdrop on the email notification sent by the Clerk's offices, the eavesdropper receives nothing useful for a nefarious purpose. Policy 8.2 makes confidential information only available to parties of record "[t]hrough use of a unique and encrypted URL."

Email Viruses And Worms – Because the Clerks of Court will be responsible for the email notifications of filing, there is a high degree of confidence that such emails will be virus- and worm-free. Instead of attorneys receiving multiple emails from lawyers with no or inadequate virus and worm protection, attorneys will receive email from reliable sources – Florida's Clerks of Court.

"Bad Man" – The "bad man" is thwarted by the Clerk's e-filing and electronic service system. When something is filed, the filer receives confirmation from the Clerk of Court. When something is filed, the Clerk of Court, not an interested party, concomitantly sends out the notice of filing material to the parties of record. All filings and electronic service activities are confirmed by a disinterested third party – the Clerk.

User Error – User error is eliminated by relying upon service through the ECF system. There is no ambiguity about e-filing – you are either in a Clerk's website and uploading a document or you are not. If you choose the wrong Clerk's website, then your case will not be there to receive the e-filed document. The Clerk, not the individual users, then handles electronic notification of the pertinent ECF participants.

User Burden – By relying upon the e-filing system, the burden associated with electronic filing and service will no longer be imposed upon attorneys. Because Policy 8.2 is an opt-in procedure, only those attorneys who are approved for e-filing are obliged to use it. This does not mean, however, that only those attorneys who are technophiles will use it. Most attorneys will e-file because they are already doing so in Florida's federal courts and because it is the cheapest way to file and serve court papers.

There is also no problem with the Bar's ethical requirements because confidential information is not being transmitted by email.

IV. Conclusion

E-filing in the Florida state system is coming – and coming soon. *See Phasing in e-filing*, Fla. Bar News, Jan. 1, 2011, at 1. Indeed, Florida's Clerks of Court are under a legal mandate to establish electronic filing processes. *See generally* Fla. Stat., §28.22205. Because e-filing and Policy 8.2 provide the safest and most efficient way to implement the electronic delivery of filed papers, this Court should deny the Petition, not adopt Rule 2.516 and its multitude of attendant and ancillary rule changes, and, instead, ensure that Policy 8.2 is a part of every Court of Clerk's electronic filing process.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing has been furnished by U.S. Mail to:

Robert M. Eschenfelder, Chair,
Code and Rules of Evidence Committee
1112 Manatee Avenue W., Suite 969
Bradenton, FL 34205-7804

John Granville Crabtree, Chair,
Appellate Court Rules Committee
240 Crandon Boulevard, Suite 234
Key Biscayne, FL 33149-1624

Robert T. Strain, Chair,
Criminal Procedure Rules Committee
3801 Corporex Park Drive, Suite 210
Tampa, FL 33619-1136

Donald E. Christopher, Chair,
Civil Procedure Rules Committee
P.O. Box 1549
Orlando, FL 32802-1549

Steven P. Combs, Chair,
Family Law Rules Committee
3217 Atlantic Boulevard
Jacksonville, FL 32207-8901

William W. Booth, Chair,
Juvenile Court Rules Committee
425 Fern Street, Suite 200
West Palm Beach, FL 33401-5839

Michele A. Cavallaro, Chair,
Small Claims Rules Committee
6600 N. Andrews Avenue, Suite 300
Ft. Lauderdale, FL 33309-2189

Jeffrey S. Goethe, Chair,
Probate Rules Committee
3119 Manatee Avenue W.
Bradenton, FL 34205-3350

John J. Anastasio, Chair,
Traffic Court Rules Committee
3601 S.E. Ocean Boulevard, Suite 203
Stuart, FL 34996-6737

Katherine E. Giddings, Chair,
Rules of Judicial Administration Committee
106 E. College Avenue, Suite 1200
Tallahassee, FL 32301-7741

John F. Harkness, Jr., Executive Director
Jodi Jennings, Liaison,
Rules of Judicial Administration Committee
The Florida Bar
651 E. Jefferson St.
Tallahassee, FL 32399

this 3rd day of January, 2011.

CERTIFICATE OF COMPLIANCE

I certify that this document was prepared in accordance with the font requirements of Florida Rules of Appellate Procedure 9.100(l) and 9.210(a)(2).

Respectfully submitted,

_____

Kurt E. Lee
Florida Bar No. 983276
Kirk ▪ Pinkerton, PA
50 Central Avenue, Suite 700
Post Office Box 3798
Sarasota, Florida 34230
(941) 364-2400
klee@kirkpinkerton.com

g:\document\kel\florida supreme court\comment.docx