2009

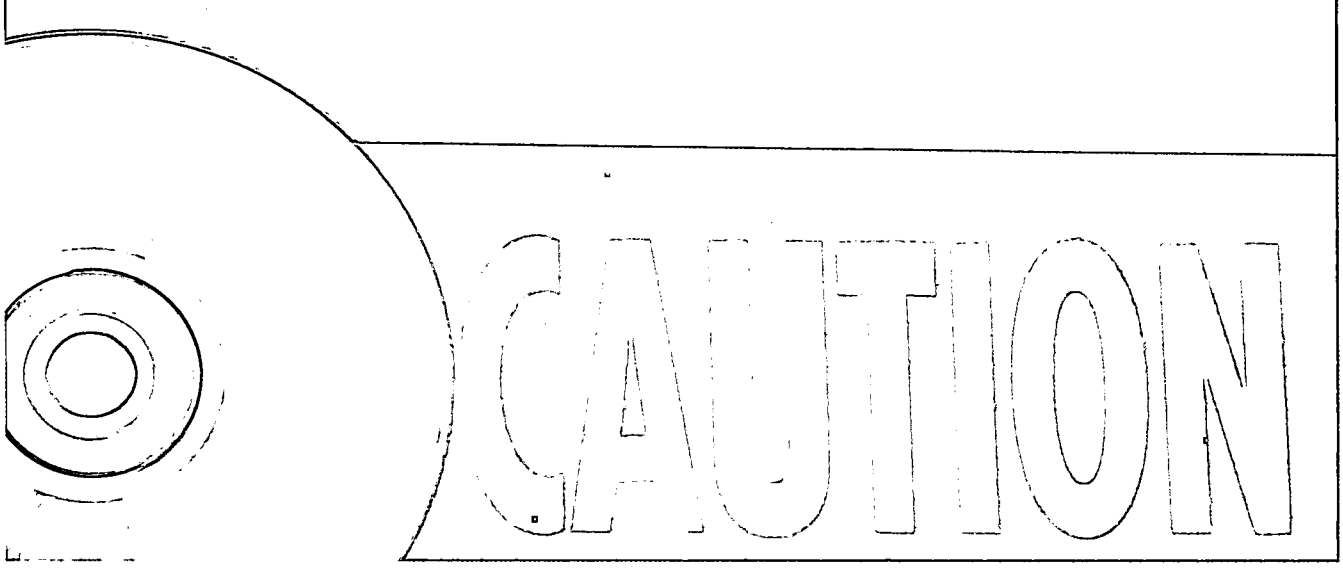
E-Filing and Privacy: What Every Lawyer Needs to Know

Rebecca Green
William & Mary Law School, rgreen@wm.edu

E-FILING and PRIVACY

What Every Lawyer Needs to Know

— BY REBECCA HULSE —



Although the e-filing revolution many predicted is not yet fully realized, lawyers should be aware of its promises and pitfalls from a privacy perspective. This article addresses what every lawyer must know about keeping a client's sensitive information safe and avoiding sanctions for the failure to do so.

It is important to acknowledge at the outset that e-filed documents raise only slightly more privacy concerns than paper records for one simple reason: many courts are retroactively "digitizing" paper records. The practical effect is that even if you still file in paper, information in documents available to the public may well wind up in electronic form and, therefore, are subject to some of the same privacy fears raised by the e-filing phenomenon. This article focuses specifically on e-filing, but lawyers should be aware that paper versus electronic filing can be a false dichotomy.

The E-Government Act's Privacy Requirements

Congress passed the E-Government Act of 2002 to facilitate the ability of citizens to access government through the Internet. The Act, which solely applies to the federal government, includes the judiciary and requires that federal courts maintain Web sites that allow public access to certain judicial documents, including docket information, all electronic filings, and court opinions.

When it passed the E-Government Act, Congress acknowledged that electronic filing, storage, and access posed privacy risks. The Act thus required the U.S. Supreme Court to establish rules to protect privacy in electronic files and records. Congress anticipated that the rules would mandate redaction of certain information to protect security and privacy, but it also required that the rules permit parties the option to file unredacted paper records under seal (either in addition to or in lieu of the redacted e-filed version).

The Supreme Court responded with, among others, Federal Rule of Civil Procedure 5.2 and Federal Rule of Criminal Procedure 49.1. These rules, effective December 1, 2007, provide attorneys with guidance on protecting the privacy of parties involved in litigation. The rules require that the following information be redacted from e-filed *and* paper-filed documents: Social Security numbers and tax payer identification numbers (to the last four digits), birth dates (to the year of birth); name of individuals known to be minors (to minor's initials); financial account numbers

(to the last four digits); and home addresses of individuals (except for the city and state). Notably, the rules stipulate that failing to redact this information constitutes a waiver of privacy rights to that information.

The Committee Notes accompanying the new rules list documents that should not be included in the public case file or be made available at the courthouse or through the Internet. These documents include executed summonses or warrants of any kind; pretrial bail or presentence investigation reports; statements of reasons in the judgment of conviction; juvenile records; documents containing identifying information about jurors or potential jurors; financial affidavits filed in seeking representation pursuant to the Criminal Justice Act; ex parte requests for authorization of investigative, expert, or other services pursuant to the Criminal Justice Act; and sealed documents.

Lawyers should know that the Rule 49.1 of the criminal code provides a mechanism for attorneys to obtain a protective order to block documents from public Internet access through PACER if they can demonstrate "good cause." (*See* Fed. R. Crim. P. 49.1(e)(3).) This is not the same as sealing a document. Documents under a protective order are still available to the public at the clerk's office; they are simply not available online through PACER. Public Access to Court Electronic Records—PACER—is the interface to the federal courts' case management system. PACER makes publicly accessible records like opinions, motions, pleadings, and other documents available over the Internet for users who register and, where appropriate, pay a fee.

Lawyers should also know that their duty to redact does not end with Rule 5.2 of the civil code and Rule 49.1 of the criminal code. Local court rules may offer additional redaction requirements and procedures that should be carefully reviewed before e-filing. For example, the U.S. District Court for the Southern District of Illinois requires that drivers' license numbers (to the last four digits) must be redacted.

Lawyers should know that neither Rule 5.2 nor Rule 49.1 provides sanctions for attorneys who fail to redact the required information. The Judicial Conference of the U.S. Courts (which the Act authorized to issue interpretive statements) recommended that attorneys who fail to redact be punished by Rule 11 sanctions, even though courts are often disinclined to enforce the rule absent egregious attorney behavior. The Judicial Conference hypothesized that clients (through malpractice or tort suits) and opposing counsel (through Rule 11 challenges) would sufficiently police redaction requirements.

So far, malpractice suits and Rule 11 sanctions against attorneys for failing to redact are not prolific, but they are not unheard of. For example, in *Luster v. City of Lebanon*, 2007 WL 61859 (S.D. Ill. 2007), plaintiff Luster moved for sanctions against the defendant for filing a document exhibiting Luster's Social Security number in violation of the E-Government Act and that court's local rules. Luster requested that the court (1) delete the offending information, (2) fine each of the three defendants $1,000, and (3) deny, as a sanction, any and all relief the defendants were requesting. Apart from deleting the offending Social Security number, the court denied Luster's request to further sanction the defendants, even though the court noted that the defendant had violated its local filing rule four times during the course of the litigation. The court's reason? Luster failed to "follow correct procedure in moving for such sanctions." The court noted that Rule 11(c)(1)(A) contains a 21-day safe harbor period allowing attorneys to correct errors. Luster failed to wait 21 days; instead, he filed his motion the day after the defendant filed the offending document with the court. Annoyed, the court still pursued civil contempt against defense counsel, ordering defense counsel to show cause why the court should not hold counsel in civil contempt for repeated failure to follow local court rules requiring redaction in e-filed documents.

In another case, *AAMCO Transmissions v. Baker*, 2008 WL 509220 (E.D. Pa. 2008), the court chose to impose sanctions on counsel for failure to redact personal identifiers in an attachment filed with the court (containing the defendant's Social Security number and date of birth) in accordance with local court rules. Despite an absence of improper intent or malice, the court noted that redaction rules would have little effect if not enforced. So, the court imposed a fine of $869 on offending counsel (based on estimated counsel fees to fix the mistake).

State Level Redaction Requirements

E-filing has a growing presence in state court filings. As of April 2009, 32 states have e-filing procedures. Some states, such as Arizona and California, are working towards implementing statewide e-filing programs. Some state courts allow e-filing for all matters while others make e-filing available for only certain case types. For example, the State of Connecticut Judicial Branch offers e-filing for tort, contract, and most property cases. In some state courts, e-filing in certain case types is mandatory. For example, in the District of Columbia all represented parties

REBECCA HULSE *is a senior lecturer at William & Mary Law School where she is assistant director of privacy and technology at the Center for Legal & Court Technology (CLCT).* *Special thanks to Tom Clarke, vice president for research and technology at the National Center for State Courts, and Susan M. Del Monte, senior attorney on the court administration policy staff at the Administrative Office of the U.S. Courts, for sharing their insights. Thanks also to Calisa Smith for her expert research assistance.*

in civil cases must e-file (pro se litigants are exempt).

States follow different models for redacting or otherwise protecting sensitive information in e-filed documents. As a rule, responsibility for redacting sensitive information is placed firmly on the shoulders of the filer. There are three broad methods used by state courts to protect privacy. First, mirroring federal practice, some states require that filers redact certain information (such as Social Security numbers and names of minors) prior to e-filing the document. A second approach, employed in Arizona, for example, requires use of a "confidential cover sheet" on which all sensitive information for a specific case file is placed. Other documents in the public file are redacted. The confidential cover sheet, as its name implies, is never accessible to the public. Finally, some states still manually redact documents after they are filed. (Typically, the clerk's office will do so only after a public request to view the file.)

Aside from redaction, there are other methods lawyers can use to protect their clients' privacy when e-filing in state courts. Virtually all jurisdictions allow litigants to seal e-filed and paper records as appropriate (determined by statute, local court rule, or most typically by the judge on a case-by-case basis). Some jurisdictions are experimenting with protective orders analogous to the federal criminal Rule 49.1(e)(3) to prevent otherwise publicly accessible documents becoming available online. Additionally, some courts have instituted "waiting periods" making e-filed documents unavailable to the public until a number of days have passed. The lag time is useful to the extent it provides parties an opportunity to prevent public access to sensitive information, yet it relies on the diligence of attorneys. When thousands of pages are being e-filed in a case, it can be a heavy burden for the lawyer.

E-filing and electronic court records have been around long enough that several high-profile screwups have surfaced in which sensitive information contained in electronic court records has made its way into the mainstream. Oklahoma recently experimented with remote online access to its retroactively scanned electronic database only to face media scrutiny over Social Security numbers and other sensitive information revealed in those records. Oklahoma immediately pulled the records off the Internet, but the toothpaste, as they say, was out of the tube.

Privacy Risks of Aggregated Court Record Data

Even after litigants redact the sensitive information required by the courts, court filings very often contain information that litigants might consider private (medical or work histories, credit records, alleged sordid details of a crime, etc.) Lawyers should understand that such information becomes vulnerable when posted online to entities that gather and sell the data for commercial purposes and to individuals with invidious intent, such as identity thieves and stalkers.

At the federal level, well before passage of the E-Government Act in 2002, the Judicial Conference of U.S. Courts recognized the privacy risks associated with online court records. In 1999 the Judicial Conference formed a Privacy Subcommittee under the Committee on Court Administration and Case Management (CACM) to develop a federal policy on access to electronic records. After carefully studying the issue, the federal judiciary opted to provide full access to public federal court records over the Internet through PACER with limited exceptions (for example, Social Security cases). A few years after this initial decision in 2001, following pilot studies that indicated no instances of harm deriving from public access to criminal records, the Judicial Conference placed non-sealed criminal records online through PACER as well. The federal judiciary concluded that if a document is public, the public deserves an efficient form of access to that record.

PACER provides a slightly heightened degree of protection for sensitive information because not just anyone can access it. Access requires (1) a PACER account (access to documents retrieved on PACER can therefore be traced to specific users) and (2) a fee (currently eight cents per page, although some documents, such as opinions, are free and some users, such as academics, indigent, and pro bono attorneys, have free access). Though these hurdles are not formidable barriers, they do, for example, keep PACER records off of Google. That said, lawyers should know that PACER's built-in access protections may not be the last word for (at least) two reasons.

First, PACER's biggest users are data resellers (firms that purchase information, repackage it in commercial databases, and resell it), meaning that information in filings may be widely dispersed. Second, thanks to the efforts of access advocates such as Carl Malamud at Public.Resource.org, a PACER account and a fee are no longer necessary for access to some federal electronic records. Acting on the belief that public records should be free, Malamud's organization works to put federal court records online, free of the access barriers PACER and for-profit records database companies impose. Making the most of a recent experiment to allow free PACER at 17 libraries across the country, Public.Resource.org encouraged access activists to head to those libraries and snag as much free data as possible. Public.Resource.org then posted with free access an estimated 20 percent of the database (19,856,160 pages of text). PACER soon suspended its free library access experiment (which, it should be noted, few had taken advantage of). What is the lesson? One never knows how accessible (or searchable) documents filed in court will be unless they are filed under seal

or unless a protective order keeps them off the Internet. As a side note, after conducting an extensive audit of the PACER records it receives, publicresource.org uncovered a huge number of unredacted documents in violation of the federal rules and has since worked with the federal judiciary to tighten enforcement of redaction requirements.

In addition to addressing privacy concerns in online court records generally, the federal judiciary has also responded to privacy concerns for certain types of documents. For example, the federal judiciary recently considered a proposal to restrict public Internet access to plea agreements in criminal cases. This proposal responded in large part to uproar over the Web site whosarat.com, a site posting information on "snitches" gleaned in part from information contained in Internet-accessible court records. Because of the obvious threat this site posed to informants' safety and willingness to come forward, the federal courts wondered whether removing plea information from public Internet access on PACER would stem whosarat.com's impact. After considering the option of barring online access, amid strenuous objections from access advocates, the Privacy Subcommittee under CACM decided to recommend against changing the national policy. Instead, the committee suggested that district courts consider adopting local policies to protect the interests of plea bargainers as they see fit. Some federal courts now bar nonparty remote access to plea documents, including, for example, the Eastern District of Pennsylvania, the Eastern District of Texas, the Southern District of Florida, and the Southern District of California. In these jurisdictions, online access is barred but the documents are publicly accessible at the courthouse. In other courts, plea agreements are excluded from the public record entirely (for example, in the Southern District of New York).

State courts, as one might expect, have taken divergent approaches to the question of putting public records online. Some, as in the erstwhile Oklahoma example, have gone with PACER's "public is public" approach and made all public files available over the Internet. Other courts provide only nonremote access to electronic records, for example, with "courthouse only" access policies requiring those seeking access to use computer kiosks at the courthouse to access public electronic records. Some courts make only certain case-type files available online and not others, while yet other courts stick with paper records access only.

Another potential glitch associated with e-filing in state courts is that as each state—and courts within each state—develops redaction policies, there is no guarantee that the same approach will be taken as to which parts of personal identifiers must be redacted. The practical effect is that one state may redact, for example, the first five digits of a Social Security number while another state might redact the last four. If the same person winds up in court databases in both states, data aggregators can "re-marry" the data to form the complete identifier. This issue has been raised periodically at William & Mary Law School's Conference on Privacy and Public Access to Court Records (the conference is presented jointly by the Center for Legal and Court Technology and the National Center for State Courts and is held at 18-month intervals in Williamsburg, Virginia; the next conference is slated for spring 2010. (*See* http://www.privacy.legaltechcenter.net/privacy.) While the problem has been recognized by forward-looking courts, others have not thought through this problem.

The reaching power of electronic records should give any lawyer cause to reflect on the ramifications to clients.

Regardless of the policies of the courts at which lawyers file, including those courts that do not (yet) have e-filing systems in place, lawyers should understand that unless paper or electronic documents are (1) filed under seal, (2) filed under protective orders prohibiting Internet dissemination, or (3) redacted, any sensitive information contained in those documents may—and likely will—end up online. "Practical obscurity" (the term coined for the de facto privacy litigants enjoyed because of practical difficulties associated with accessing dusty paper court files) is effectively dead.

The "reaching power" of electronic records should give any lawyer pause to reflect upon the ramifications to clients of filing documents—electronic or paper—with a court.

Privacy Risks of Metadata

Choosing what bits of information in e-file documents to include or exclude may be only half the battle. Some data may be a part of the e-filed documents without lawyers realizing it. These data are called "metadata" or hidden data embedded in documents and not immediately visible. Metadata is generated by software programs, includ-

ing Microsoft Word, and contains information about the document such as previous document versions, revisions, author(s) names, the name of the server or hard drive where the file is stored, template information, file properties, and more. Metadata threatens not only current clients' privacy, but potentially other clients' as well when lawyers use templates for multiple clients. Metadata from each version might lurk within the template and inadvertently accompany documents down the line.

Unless the filer has taken steps to remove it, metadata can remain hidden within the e-filed document. The fear is that anyone with access to that electronic data will, with a little technological know-how, access metadata and use this information in ways the filing attorney (and the client) may find troubling. Lawyers in a Washington, D.C., firm representing GE recently found this out the hard way. To redact sensitive information, they blacked out thousands of pages in numerous briefs by "drawing" a black box in Word to cover sensitive information. What they did not realize is that when those same documents were downloaded from PACER, copying and pasting those black bars into another Word document enabled viewers to read the original text. That's metadata—information that appears to be gone from a document that in fact sticks around.

Once aware of the metadata issue, there are two steps that lawyers can take to secure documents. First, they can "clean" documents prior to e-filing by, for example:

- turning off "track changes" when creating a document;
- turning off "automatically save version on close" in Microsoft Word;
- consulting the software provider for instructions on how to limit the amount of metadata the document software creates;
- hiring a consultant or purchase software specializing in metadata removal;
- converting the file to PDF. (Note: If this is done electronically, some metadata may linger in the document; printing and then scanning a document to PDF removes more, but not necessarily all, metadata.)

Second, redaction should be done carefully. Adobe—and the National Security Agency—suggest fully deleting all text to be redacted and replacing it with the same number of characters (for example, with *x*'s) so the document is formatted identically to the unredacted version. In a perfect world, for extra precaution, the content would then be cut and pasted into a new document. And then, as a further precaution, the document would be printed, scanned, and converted to PDF before e-filing. Practically speaking, these extreme measures threaten to undo the efficiencies e-filing enables. Lawyers e-filing large volumes of documents should determine best alternatives to ensure that documents are as free of metadata as possible.

Some concerns about metadata are at least partially alleviated by court e-filing systems that incorporate "extensible markup language" (XML), which is a means of parsing and labeling data objects. XML provides a mechanism to impose constraints on the storage and layout of data. In the e-filing context, XML offers the potential for courts and filers to "mark" and encrypt data to allow only certain uses for each piece of datum. XML-marked e-filed data are not vulnerable to the same metadata and other privacy concerns since virtual documents using XML (assuming proper encryption) do not store metadata in the same way word-processing programs do. Many courts are experimenting with XML in various parts of their e-filing regime (in forms-based filings and even in unstructured documents like pleadings). Assuming the many challenges to developing a consistent and interoperable XML model are met, XML could become a viable solution to at least some of the privacy problems inherent in e-filing.

Communicating with Clients About E-Filing Privacy

A final and important piece of protecting clients' privacy when e-filing documents is client communication. Both to protect themselves from liability and to protect their clients' interests, lawyers should:

- Fully educate clients about privacy risks associated with e-filing documents with a court such as unintended downstream uses, data aggregation, and so forth.
- Seek clients' assistance in identifying sensitive information—especially information the lawyer might not otherwise recognize as sensitive.
- Help clients understand available options to restrict or limit disclosure of sensitive information when e-filing.
- Be vigilant about what opposing counsel files and take appropriate measures to prevent clients' sensitive information from being included in the public record.

When it comes to e-filing and privacy, knowledge goes a long way. Whether it is sufficiently redacting required information, taking a sophisticated look at client privacy interests before e-filing documents, or making efforts to sweep documents clean of metadata, an informed lawyer can protect clients' privacy interests when e-filing, even in a technological age when those interests are increasingly under threat. ■

also about what is good for criminal justice. By taking our own personal interests out of the equation, we remain confident that we are promoting policies and practices that are premised on doing the right thing, for the right reasons.

Our Work Reflects This Spirit

One need not look any further than the organizational structure of our Section's committees, task forces, functional committees, and boards to gain an appreciation that we cover the gambit of issues and many areas related to criminal justice. From juvenile justice to problems of the elderly, to victims, to reentry and collateral consequences, to sentencing, to cybercrime, to immigration, to ethics, plus a number of others—all designed to ensure that the Section is prepared to step in with insight and solutions to the criminal justice issue under consideration.

Our development of Criminal Justice Standards is another shining example of our contribution to the greater good. The Section has been responsible for the development of more than 24 individual sets of standards since the inception of the Standards in 1968. The "black letter" standards can be found at www.abanet.org/crimjust/standards/home.html.

From start to finish, it normally takes three years or more to get through the drafting, reviewing, and final drafting stages before it is presented to the ABA House of Delegates for association-wide approval. The Section is proud of this work not only because of the quality of the scholarship, but also because it is universally accepted by trial and appellate courts, legislators, media, academics, and the public as a reliable guide of criminal justice standards that have been appropriately vetted by all the major players in the field.

The policy recommendations adopted by the House of Delegates during the 2009 Midyear Meeting also show the diversity of the Section's interest in criminal justice. Specifically, those recommendations included:

(1) Reexamination of the Adam Walsh Act www.abanet.org/crimjust/policy/my09101a.pdf;
(2) Mediation in Criminal Matters http://www.abanet.org/crimjust/policy/my09101b.pdf;
(3) Immigration Raids in Criminal Justice http://www.abanet.org/crimjust/policy/my09101c.pdf; and
(4) Child Victims in the Criminal Justice System http://www.abanet.org/crimjust/policy/my09101d.pdf.

Section Awards Reflect Selfless Service

Each year the Section presents four special awards to individuals who, through their professional works, demonstrate character, integrity, and professional achievement in the area of criminal justice. The awards are named in honor of legends in the field whose good works still serve as a reminder of what is good and noble about the profession.

The **Charles R. English Award**, for judges, prosecutors, the defense bar, academics, and other attorneys who have distinguished themselves in the field of criminal justice.

The **Norm Maleng Minister of Justice Award**, bestowed upon a prosecutor who embodies the principles annunciated in the ABA Standards for Criminal Justice, Prosecution Function, particularly that "the duty of the prosecutor is to seek justice, not merely to convict."

The **Livingston Hall Justice Award**, for an active member of the bar who devotes a significant portion of his or her legal practice to youth and children, and is making positive contributions to the field, both in and outside the courtroom.

The **Frank Carrington Crime Victim Attorney Award** to attorneys or other legal service providers who have either directly represented specific victims in criminal, juvenile, or appellate courts, or who have worked to promote or implement policies to improve the treatment of crime victims in the criminal justice system.

Each award reflects the legacy of a giant in the field of criminal justice. Importantly, the recipients of these awards all reflect the highest ideals of our profession and a strong spirit in the area of criminal justice. They get it!

Thank You for Enriching My Life

This will be my last column as chair of the Criminal Justice Section. While I will continue to be a part of the Section, hopefully for many years to come, writing this last column has given me the opportunity to reflect, and to draw the unmistakable conclusion that I have been personally blessed and professionally enriched by my service to and association with the Section.

I thank Jack Hanna, our Section's executive director, and all our outstanding staff for their hard work and for making my year so enjoyable. I thank Steve Saltzburg, our immediate-past chair, for being such a strong role model, for his friendship, and his continuing service to our Section. I thank all the volunteers who serve and will continue to serve the committees, task forces, and boards of our Section, and I want to thank the Council members (past and present) who share their time, expertise, and commitment that drives the mission of our Section. I also pledge my support to Charles Joseph Hynes, our chair-elect, who is prepared to hit the ground running.

For me, this has been an experience of a lifetime. It reflects an appreciation for a group of special individuals who understand that it is not about you, me or us—but our country and the communities that we serve.

Yes, we get it. . . . □