

700 Stewart Street, Suite 5220
Seattle, WA 98101
(206) 553-4985
Fax: (206) 553-4073

Peter G. McCabe
Secretary, Committee on Rules of
Practice and Procedure
Administrative Office of the U.S. Courts
1 Columbus Circle, N.E.
Suite 4170
Washington, D.C. 20544

05-AP- 003

05-BK- 008

05-CV- 027

Re: Proposed Rule 5.2 – FED.R.CIV.P.
Proposed Rule 49.1 – FED.R.CRIM.P.
Proposed Rule 25(a)(5) – FED.R.APP.P.
Proposed Rule 9037 – FED.R.BANKR.P.

05-CR- 014

Dear Mr. McCabe:

I am submitting these comments with respect to the proposed federal rules of practice and procedure referenced above, relating to the protection of privacy of court records in civil cases, criminal cases, bankruptcy cases and appellate cases. I am an Assistant U.S. Attorney, but also serve as an adjunct professor at the University of Washington School of Law where I teach Privacy Law. I have written and spoken frequently on the problem of balancing public access and privacy in the context of a system of electronic court records.¹ In preparing these comments, I have received helpful suggestions from Justice John Dooley, Judge Ronald Hedges, Robert Deyling, Professor Peter Swire, as well as many other people who have been active in the Sedona Conference and in the Courtroom 21 Project at William and Mary Law School. The views I express, however, are my own.

As set forth below, I believe that the proposed rules successfully balance the right of public access to court records against the need to protect from misuse the sensitive personal and commercial information that may be contained in them. I also believe that, consistent with current funding limitations, the proposed rules implement the Congressional directive in the E-Government Act of 2002 to make court records available on-line, while still protecting the privacy and security of sensitive information in court records, and that they do so in a manner that is consistent with the Constitutional right of access to court records. Finally, at the end of my comments, I suggest a minor change in the proposed rules which could take advantage of the

¹ See, e.g., Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 Wash. L. Rev. 307 (2004).

existing PACER technology to facilitate greater public access to court records, while, at the same time, enhancing the ability of litigants to protect sensitive information in court filings.

Any system of court records in a free society must be open to the watchful gaze of the public. The openness of judicial proceedings and records serves to check against the misuse of judicial power, and increases public respect and involvement by citizens in the legal system.² For this reason, every federal circuit protects the right of public access to judicial proceedings and court records—either under the First Amendment or as a matter of common law. At the same time, unfair publicity can be used by parties as an instrument of oppression—for instance, when parties attempt to use the public nature of judicial proceedings to generate unfair publicity and achieve an unfair advantage in the underlying litigation. Thus, there are times when the disclosure of sensitive personal or business information can create unacceptable risks of a miscarriage of justice, and cause unnecessary harm to parties and non-parties alike. As Justice Powell wisely noted:

[T]he right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes.³

Courts have long been aware of the need to balance the public's general right of access to judicial records against the need, on occasion, to protect information in judicial proceedings and court records from improper disclosure. Balancing the competing claims of transparency and privacy has never been a simple task. Both sets of interests—those in favor of the disclosure of information, and those in favor of protecting it—can be supported by forceful and cogent arguments. Over the years, however, in case after case, as courts have carefully weighed and decided between these competing interests, general common law principles have arisen which establish the proper balance between transparency and privacy.

Our society is now engaged in an electronic revolution. Information is processed faster and more cheaply than ever before in the past, and used in ways that were never before

² See Blackstone, Commentaries on the Laws of England, III, Ch. 23, p. 377 (1768) (“[T]he only effectual and legal verdict is the public verdict.”), see also Vol. IV, Ch. 3 “On Courts in General”, p. 24 (“A court of record is that where the acts and judicial proceedings are enrolled in parchment for a perpetual memorial and testimony.”) Blackstone, of course, was greatly influenced by the Italian legal scholar, Cesare Beccaria, who argued strongly for the need for transparency in judicial proceedings. See Beccaria, On Crimes and Punishments, Ch. 14, p. 36 (1764) (“All trials should be public, that opinion, which is the best, or perhaps the only cement of society, may curb the authority of the powerful, and the passions of the judge, and that the people may say, ‘We are protected by the laws; we are not slaves.’”).

³ *Nixon v. Warner Communications, Inc.* 435 U.S. 589, 598 (1978).

imaginable. Courts, as quintessential information processing systems, are not immune from the effects of these technological changes. The adoption of electronic filing systems by state and federal courts has allowed the legal system to realize substantial operational benefits, and has permitted the public to more easily access and understand the federal judicial process. At the same time, the electrification of judicial records has created new threats to the integrity of the judicial process and the administration of justice which did not exist in the past.

In the days of a paper based system of court records, much of the sensitive information contained in court files was protected merely by the cost of retrieving the records. Only those with a relatively strong and individualized interest in the information would take time out of their day to travel to the clerk's office, wait in line, fill out the necessary forms to request the retrieval of the records, wait for the clerk to find the files, read through them to find the relevant records, copy them, and then pay the necessary copy charges. As a result, while records in a paper based system were technically "public" in the sense that any member of the public had the ability to access almost any court record, the vast bulk of the sensitive information in judicial records was protected by a the sheer difficulty of accessing the particular record in question. This fact greatly reduced the dangers of the misuse of sensitive information—something which was recognized by the Supreme Court when it recognized and granted legal protection to the "practical obscurity" of court records.⁴

The practical obscurity of paper records allowed our legal system to treat court records as public, although we still could enjoy substantial practical protections for any sensitive personal information in those records. Now that judicial records are fully electronic, however, computers can search, compile, aggregate and combine vast quantities of information in court records in a matter of minutes, and at minimal cost. Technological change brings its rewards and its punishments indifferently. As we enjoy the great convenience of a system of on-line electronic court records, we also must mourn the death of practical obscurity. As our new technology renders all court records fully transparent, the risk of misuse of sensitive personal information in court files dramatically expands. Thus, the death of practical obscurity has not eliminated the need for the courts to continue to engage in the careful process of balancing transparency and privacy—it has merely made this balancing process infinitely more difficult.

Whether one views these changes as a blessing or a curse, there is no turning back. The inevitability of the technological revolution in court records was acknowledged by Congress in section 205 of the E-Government Act of 2002 (the "E-Government Act" or the "Act").⁵ In the Act, Congress directed the federal courts to provide for electronic public access to court records. With its usual desire to eat its public cake and have its privacy too, Congress also directed that the federal courts establish rules governing such electronic access which would protect the

⁴ *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989).

⁵ Pub. L. No. 107-347, § 205, 116 Stat. 2899, 2913-2915.

privacy and security of personal information. For this Herculean task, Congress saw fit to provide no additional funding to the courts. Congress did provide the courts with the following suggestion--that the rules adopted by the courts to address privacy and security concerns take into account the "best practices of federal and state courts." Unfortunately, since federal and state courts have only recently implemented their systems of electronic access, there is relatively little experience measuring the costs and benefits of different competing systems of electronic access.

The subject itself is relatively obscure. There is only a small number of people at the state and federal levels who are even interested in the problem--consisting mostly of certain federal and state judges, staff attorneys at the Administrative Office of U.S. Courts, attorneys like myself at the Department of Justice, as well as information brokers, the media, privacy advocates, and law professors. There has been an excellent dialogue among this group, and the process does not appear to have been politicized. However, the various technologies are changing too quickly for there to be any clear consensus about "best practices." We are all scrambling, and we will be lucky if we can just muddle through. One thing is clear with respect to the federal process. With no new funds, the federal courts have only the computer systems that were in place before the passage of the E-Government Act. For better or for worse, for the foreseeable future, the PACER system will be the technological backbone of the federal courts.

The federal PACER system uses a system of computer privileges to manage remote access to court records. There are roughly *three* different levels of privileges.

- 1) The first level of privileges allows court records to be filed "under seal." Access to this information is not permitted to members of the general public.
- 2) The second level of privileges allows on-line access to court records on an individualized basis--to specially named persons only. While this level of privileges is usually used when a record is filed under seal, the technology actually permits any other specifically designed person to have on-line access on an individualized basis.
- 3) The third level of privileges--the default--allows access to the general public--or more accurately, to any person who possesses a userid and a password, and pays a small fee to download the pleading.

In addition to the system of remote electronic access, it is still possible to file paper records with the clerk's office. Such paper based filings are still permitted for the bulky records on review from federal administrative proceedings, social security cases, immigration cases or on collateral attack from other state and federal tribunals in *habeas corpus* litigation. In these cases, the pleadings themselves are filed electronically, but the administrative records are allowed to remain in paper form. At some point, it may be assumed that this system will change when the records of the various tribunals themselves become electronic.

It is important to note that given the PACER's system's computer architecture, there is no option to make all judicial records available to any person at no cost on the Internet. Userids and passwords are necessary to insure the financial integrity of a self-financing system in the absence of a specific Congressional appropriation to pay for a new one. Interestingly, this aspect of the PACER technology indirectly, and probably unintentionally, allows greater protection for the privacy and security of sensitive information in court records. When all users are required to maintain a minimum level of financial accountability to obtain their userids and passwords, the courts are in a better position to police what users do with the information. Users who engage in systematic misuse of personal information in judicial records are at risk of losing their privileges. While hardly a perfect system, PACER does provide some protection against the most obvious potential harms which would take place if all information in court records were freely and anonymously searchable through powerful Internet search engines like Google. However, there are also aspects of PACER's technology which are probably best described as a technological purgatory. The PACER system's technology was not designed with the competing goals of facilitating access and protecting privacy in mind. As a result it contains very few privacy enhancing technologies—e.g., software programs which can automatically identify and flag sensitive information such as social security numbers, or programs which permit the easy and effective redaction of sensitive information in pleadings. Thus, in fashioning the proposed rules, the Judicial Conference is necessarily constrained by the limits of the PACER technology.

To make up for the lack of privacy enhancing technologies, the proposed rules make attorneys the front line in the protection of sensitive information in judicial filings. The rules provide that if sensitive information is in a document that needs to be protected, the decision to do so must be made before it is filed, not afterwards. And the rules also caution attorneys to file sensitive personal information under seal or in a redacted form, after obtaining permission from the court. Unfortunately, while attorneys may be in a good position to decide what information of their clients is in need of protection, they may not be quite as attuned to the need to protect the sensitive personal information of others—the opposing party, witnesses to the case, jurors, and the many other voluntary and involuntary participants in the judicial system. This is an obvious weakness in the rules, but, given the PACER technology, there appears to be little choice in the matter. The courts have done the best they can with the technological cards they have been dealt by Congress, and attorneys will have to bear that burden until Congress steps in with financial assistance.

In an attempt to lessen the burden on attorneys, the proposed rules create a presumption that certain identifiers not be placed in the court record, and they permit the redaction without court approval of certain sensitive information--social security and tax identification numbers, names of minor children, birth dates, and financial account numbers. As the comment makes clear, similar forms of information would also probably qualify--such as driver's license and alien registration numbers. One could add to this list individual health identification numbers and physician identification numbers, as well as other similar types of numerical identification systems.

The presumption in the proposed rules that certain types of personal identifiers be excluded from the public record, may appear to change the traditional presumption about the openness of court records. However, as the comments to the rules emphasize, the rules are not intended to affect the limitations on sealing that are otherwise applicable under the law. In the past, of course, courts would have excluded such obviously sensitive information from the court record after a case by case balancing. But courts have never held that the right of public access requires that individuals be exposed to a needless risk of identity theft, merely because personal identifiers happen to be contained in otherwise public court records. Accordingly, the proposed rules eliminate the time-consuming balancing process. Instead, the rules implement the mandate of Congress in the E-Government Act, which codifies a result that earlier common law and Constitutional decisions would have reached in any event.

Finally, the rules permit the entry of protective orders. As we have seen, protective orders may be used to seal sensitive information by redaction or by the removal of the record itself from the public record. However, the proposed rules also permit a second option which was not previously available in the days of paper records. The rule allows for protective orders to be entered to provide that remote electronic access to certain records be limited to the parties and their attorneys alone, with the general public access limited to access "at the courthouse." This is an extremely interesting and important step. It appears to be an attempt to permit parties, upon court order, to create within the electronic filing system a "proxy" for the practical obscurity of the days of paper records.

There are good pragmatic reasons to try to create an "intermediate" form of access to court records--that is, to attempt to re-create something like the old system of "practical obscurity." For instance, many court records contain large amounts of confidential medical records. While the courts certainly could require the redaction of medical information in a social security case, the cost of doing so would be prohibitive. It would also be unfair, since social security claimants are often in distressed financial circumstances. Likewise, the files in immigration and naturalization appeals also contain similar sensitive personal information for which it would be burdensome and unfair to require redaction. Accordingly, for these types of files, it makes eminent practical sense to have an intermediate system of access. Under the proposed rules, then, on-line access is available for the parties and their attorneys, with public access otherwise available "at the courthouse." For social security and immigration cases, the rules create a presumption that the intermediate system of access will be the default. In other cases, the parties can seek protective orders to obtain similar treatment if they believe similar treatment is needed. Such treatment would appear to be most appropriate in almost any case in which there is a large amount of sensitive information--administrative appeals of Medicare claims and personal injury suits with large amounts of health records come immediately to mind.

An intermediate system of access certainly complies with the Constitutional and common law right to public access. The cases establishing a strong right of access to court records only apply where the public has been denied access to a judicial record *in toto*--that is, where the underlying information is filed *under seal*. So long as the public has some means of access to the

underlying information (for instance, the same “at the courthouse access” the public has always had), the courts are free to impose different levels of computerized privileges for different types of court records within the on-line system.

While I praise the proposed rules’ attempt to establish an intermediate system of access, the “at the courthouse” rule appears to be misguided. In an electronic age, such a rule cannot actually re-create the old system of practical obscurity; it merely imposes a system of “contrived inconvenience.” The proposed rule does not protect sensitive information in court records from a “cottage” industry of copyists, who travel from courthouse to courthouse, selling the information from court files to third parties without restriction—a cottage industry that already appears to thriving. The “at the courthouse ” rule also discriminates against people who may reside farther away from the courthouse, in favor of people who reside nearer to the courthouse. The “at the courthouse” rule still requires clerks’ offices to expend valuable staff time addressing their requests for access, and forces the needless conversion of electronic into paper records at public expense. Finally, since staff at clerks’ offices may not legally screen access requests, the “at the courthouse only” rule is unlikely to secure any meaningful privacy. For instance, a stalker seeking information about his victim will still be able anonymously and secretly to obtain the personal information he seeks. The artificiality and burdensomeness of the “at the courthouse” solution may even discourage some judges from entering protective orders which use this option, in spite of the obvious need at times for a system which avoids the cost of redacting large amounts of sensitive personal and commercial information.

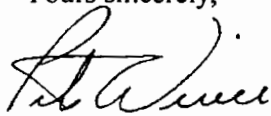
While I strongly support the attempt in the proposed rules to create an intermediate level of access, I would respectfully suggest that there may be a much simpler way to achieve it—one which takes advantage of the existing PACER technology. Instead of providing for “at the courthouse” access, the proposed rules could provide simply for remote electronic access for any interested member of the public, upon request, after notice to the parties (a notice which is automatically emailed to the parties without cost by the operation of the PACER system). In the absence of any objection, access would then be automatically granted, and the requesting person would receive the same level of access to the court file as the parties themselves enjoy. Local rules could be established to provide for a briefing schedule if any of the parties objected to access. The objecting party would, of course, then have the burden to meet the Constitutional and common law requirement for limiting such access. They would also have the expense of redacting any particularly sensitive information they wished to protect if their objection were overruled. Of course, in the vast majority of cases—as in the days of paper records—such access would raise little if any concern of harm. Furthermore, unlike an “at the courthouse” system of access, the parties with a direct interest in protecting their personal information would be in a position to know who, for instance, wanted to review their medical records. If a university researcher or a newspaper reporter wished to review social security records in a study of the Social Security Administration’s treatment of claimants, it is unlikely that many claimants would object, particularly if the requester had no interest in the individual persons in the file but was only interested in general trends. On the other hand, if the requesting party were believed to be a stalker and a party feared the potential misuse of any of the sensitive information in the court

record, that party would then be in a position to object to the access to the information, or to pursue other legal remedies they might have under applicable law.

As a matter of drafting, I would respectfully suggest that the proposed rule be changed to replace the words "at the courthouse" with "as otherwise ordered by the court, or as provided for by local rule." The court could then, on a case by case basis, or by local rule, establish a procedure for allowing the parties to seek permission to use a system of intermediate access, could implement a schedule for filing any objections, and could establish any other procedures to account, as necessary, for the specific concerns of the parties.

Please do not take my comment as suggesting anything less than full respect for what has already been accomplished in the draft rules. As presently drafted, the proposed rules successfully navigate between the Scylla of a electronic court system of complete publicity, and the Charybdis of a system of complete privacy. This achievement is even more remarkable given the technological limits of the PACER system, and the lack of funding by Congress. I would only suggest that the PACER system may have a greater capacity to solve certain problems than the drafters of the rules may have been aware. Thus, instead of attempting to "retrofit" the PACER system to reverse engineer an equivalent of "practical obscurity," it may be more appropriate to exploit the existing PACER technology to provide a different, and potentially more convenient form of "intermediate" access. This intermediate access would be individualized, instead of anonymous; and it would offer a system of accountability, if not a system of full privacy. I hope the Committee seriously considers amending the proposed rules to incorporate what I respectfully submit may be a practical and workable solution.

Yours sincerely,

A handwritten signature in cursive script, appearing to read "Peter A. Winn".

Peter A. Winn