

COMMITTEE ON COURT ADMINISTRATION AND CASE MANAGEMENT
OF THE
JUDICIAL CONFERENCE OF THE UNITED STATES
WASHINGTON, D.C. 20544

JOHN R. TUNHEIM
CHAIR

WILLIAM G. BASSLER
JOHN D. BATES
PAUL D. BORMAN
JAMES B. HAINES, JR.
TERRY J. HATTER, JR.

ROBERT J. JOHNSTON
BENSON EVERETT LEGG
SANDRA L. LYNCH
STEVEN D. MERRYDAY
JULIE A. ROBINSON
ILANA DIAMOND ROVNER
SONIA SOTOMAYOR
T. JOHN WARD

February 8, 2006

05-AP- 002

Honorable David F. Levi
Chief Judge
United States District Court
2504 Robert T. Matsui
United States Courthouse
501 I Street
Sacramento, CA 95814-7300

05-BK- 006

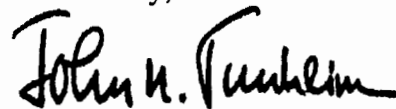
05-CV- 025

Dear Judge Levi,

05-CR- 011

Enclosed please find the comments of the Judicial Conference Committee on Court Administration and Case Management regarding the Proposed Rules to Address Privacy and Security Concerns as required by the E-Government Act of 2002. Our Committee appreciates the work you have done, as well as the opportunity to comment on this important issue. Do not hesitate to contact me with any questions or concerns.

Sincerely,



John R. Tunheim

cc: Abel Mattos
John Rabiej

Enclosure

Comments of the Committee on Court Administration and Case Management
on Proposed Rules to Address Privacy and Security Concerns
as Required by the E-Government Act of 2002

Background

In an effort to balance the competing interests of the public's right to have access to court information and the need to protect personal data in the electronic age, this Committee began studying privacy and public access to electronic case files in 1999. After two years of study, a public comment period, and a public hearing, the Committee recommended to the Judicial Conference of the United States the adoption of a policy that would allow access to civil and bankruptcy cases, with the requirement that specific personal identifiers (Social Security numbers, financial account numbers, dates of birth and names of minor children) be partially redacted from the document. The CACM Committee recommended that such access to criminal cases be studied for two years because of safety and security concerns unique to criminal cases. In September 2001, the Judicial Conference adopted this policy. (JCUS-SEP/OCT 01, pp. 48-50). Following a study that revealed no instances substantiating such concerns, this Committee, together with the Committee on Criminal Law, recommended that public access to criminal cases also be allowed. The Conference adopted this position (JCUS-SEP 03, pp. 15-16) and later adopted specific guidance recommended by this Committee for public access to criminal cases. (JCUS-MAR 04, p. 10). This guidance provides that redaction of personal information is also required for criminal documents, with the addition of the redaction of home address to city and state. The Conference-approved guidance also addresses whether certain documents and information should be included in public criminal case files.¹

Proposed Federal Rule of Appellate Procedure 25, Filing and Service

Proposed Federal Rule of Appellate Procedure 25 would apply the proposed bankruptcy privacy rule and the proposed criminal privacy rule in cases that applied those rules below. In all other cases on appeal, the proposed civil privacy rule would apply, except the criminal rule would apply when an extraordinary writ is sought in a criminal case. This approach is consistent with the Privacy Policy's statement that appellate cases are to be treated the same way the cases were treated below and the Committee supports the rule as proposed. It also specifically recognizes that, because the Case Management/Electronic Case Files system for the courts of appeals is not yet operational, there is less experience with privacy issues at the appellate level.

¹ A copy of the Judicial Conference Privacy Policy (the Privacy Policy) and the Criminal Implementation Guidance are attached for your reference and are available at www.privacy.uscourts.gov.

Further, the Committee recognizes the fact that the proposed appellate rule gives more specific guidance than does the privacy policy in making the proposed civil privacy rule generally applicable, with specific exceptions. Thus, the proposed rule addresses how to treat matters that originate in the court of appeals or that come from an administrative agency or entity other than a lower court.

Proposed Federal Rule of Bankruptcy Procedure 9037, Privacy Protection For
Filings Made with the Court

Proposed Federal Rule of Bankruptcy Procedure 9037 would require redaction of the standard personal identifiers (Social Security number, financial account number, name of minor child and date of birth) and would also provide for exemptions from the requirement. Further, it addresses sealed documents, protective orders, use of a reference list and waiver of the redaction requirements. This proposed rule, like the others, is largely based upon the Privacy Policy, as the notes make clear, and, in large part, the Committee supports it. However, the Committee does wish to point out several concerns it has regarding specific portions of the proposed rule.

Subsection (a) states that a filing “may include only” the redacted versions of the identifiers while subsection(g) states that a party waives the protections of redaction as to its own information if that information is not filed under seal and not redacted. The Privacy Policy *requires* redaction and does not contain an explicit waiver. The Notes to the proposed rules clarify that the waiver only applies to the specific information filed without redaction and not under seal and that if such is done accidentally, a party may seek relief from the court. It also points out that the waiver provision may be beneficial in cases where a party determines that costs of redaction may outweigh its privacy benefits. Based on these clarifications, the Committee supports the waiver provision and understands that in order for this provision to be possible, the wording of the redaction requirements must remain permissive.

This proposed rule, as do the proposed civil and criminal rules, includes exemptions from the redaction requirement that the current policy does not specifically include. The Committee understands the need for these exemptions and generally supports them. However, concern has been expressed that the exemption for records of a court “whose decision is being reviewed” may not be appropriate because the language could be read to suggest appellate review, in which bankruptcy courts do not engage. However, the record in a bankruptcy case does often contain a record from another court proceeding as evidence, or otherwise. The Committee therefore suggests that thought be given to using language other than “reviewed” in the wording of this exemption. (For example, perhaps the rule could refer to a court whose “decision becomes part of the record.”) Since identical wording is used for this exemption in the proposed civil and criminal rules, as well, this suggestion would apply to those rules as well. Regardless of the specific wording, the Committee believes that the focus should remain on the fact that a record from another court does not need to be redacted.

Proposed Federal Rule of Civil Procedure 5.2, Privacy Protections for Filings
Made with the Court

Proposed Federal Rule of Civil Procedure 5.2 would also require redaction of the standard personal identifiers and also provides for exemptions from these requirements. Like the bankruptcy rule, it also addresses sealed documents, protective orders, use of a reference list and waiver of the redaction requirements. Again, the basic structure and provisions of this rule are similar to the Privacy Policy and the Committee supports it. There are, however, two specific points the Committee wishes to make regarding the proposed civil rule.

First, our comments made above in reference to the proposed bankruptcy rule regarding the waiver provision and the exemption for records of a court “whose decision is being reviewed,” also apply to the civil rule. Second, the Committee has some concerns regarding subsection (c), which provides for limitations on remote access to electronic case files.

The Privacy Policy provided for such limitations only in the context of social security cases on the grounds that such cases often contain voluminous administrative records that necessarily include the claimant’s social security number and detailed medical and financial information.² The proposed rule retains limited access to these cases, which the Committee supports, yet also provides for limited access in immigration cases. In previous communications with the Rules Committee, this Committee opposed extension of such limited access because it views social security cases as distinctive since extensive personal information is necessary in every case. We suggested that other types of cases be handled on a case by cases basis rather than by category. However, this Committee indicated that it would consider limited access for immigration cases if it could be demonstrated that their volume is substantial and that the information routinely appearing in their records should be protected. The Committee recognizes that there has been a substantial increase in the number of immigration cases in the federal courts since this restriction was first suggested. The Committee also appreciates that the data routinely contained in such cases includes personal and identifying information. Thus, the Committee would support limited electronic access to the bulk of documents in immigration cases as long as the initiating documents (e.g., opinions issued by the Bureau of Immigration Appeals and Immigration Judges) and orders and opinions remain remotely, electronically available to the public. Because these documents would likely contain personal information, the Committee further suggests that the party filing the appeal from the prior decision be required to redact the initiating document as it would any other filing under the proposed civil rule.

² Even though the Privacy Policy limits remote public electronic access to filings in social security cases, such limitation is not intended to apply to court opinions. The Committee assumes that opinions will be available in immigrations cases as well, if the same limitations are applied.

Proposed Federal Rule of Criminal Procedure 49.1: Privacy Protection for Filings
Made with the Court

Proposed Federal Rule of Criminal Procedure 49.1 would apply the same redaction provisions as the other proposed rules, with the addition of home address to city and state. Likewise, it also contains exemptions from these provisions as do the bankruptcy and civil rule. Again, the Committee generally supports this proposed rule, but has several specific areas of concern. First, our comments about the waiver and exemption for records of a court “whose decision is being reviewed” would again apply to this proposed rule.

Further, the Committee notes that the exemptions from redaction in the criminal rule are more extensive than those in bankruptcy and civil. It exempts the same documents as the other rules, but also exempts habeas filings, a filing in relation to a criminal matter or investigation that is prepared before the filing of a criminal charge or that is not filed as part of any docketed criminal case, arrest or search warrants, and charging documents or affidavits in support thereof. The Committee is concerned that this list may be overly inclusive and suggests that personal identifiers can be redacted from many of these documents, such as executed warrants and charging documents. This redaction will allow the document to be included in the public file while still protecting the privacy of the individual concerned.

It should be noted that the initial Privacy Policy did not allow for remote public electronic access to criminal files and that such access was only recommended by the CACM Committee and approved by the Judicial Conference after a two-year pilot program and study conducted by the Federal Judicial Center revealed no instances of harm and a substantial benefit to the bar and public in the 11 courts where such access was permitted.

When the Judicial Conference decided in September 2003 to allow remote electronic public access to criminal case files subject to the redaction requirements, it stayed the implementation of this change until the CACM Committee could work with the Committee on Defender Services and the Committee on Criminal Law to develop guidance for implementation of access to electronic criminal case files. That guidance, which the Judicial Conference approved, explains that certain documents and information are not to appear in the public case file, in paper or electronic form, at the courthouse or via remote access. These included presentence and pretrial reports, juvenile records, statements of reasons, unexecuted warrants of any kind, sealed documents, and identifying information about jurors and potential jurors. This is designated as “III. Documents for which public access should not be provided” (Part III of the guidance) and it is not clear how the exemptions of the proposed rule relates to this guidance. In order to comply with current policy, many courts are redacting or having filers redact the stated personal identifiers from executed warrants so that they can be filed and available to the public. Likewise, courts are being instructed to redact copies of documents with juror identifying information, such as the foreperson’s name in the form of his or her signature, so that a copy of the indictment can be included in the public criminal case file, whether it be paper or electronic. The original indictment or other document with this information is most often sealed to protect

the identifying information.

If the proposed rule is intended to permit the filing of the name of the grand jury foreperson, thereby identifying that individual, it contravenes the guidance, and the Committee would oppose it. The notes mention the guidance, even the specifics of Part III, yet suggest that their substance can be accommodated by sealing the documents. The problem with sealing the indictment without providing a redacted version for the public file is that there then is no public access to that document. If a redacted document is filed in addition to the sealed document, the public can see the substance of the indictment, such as its specific counts, without impacting the privacy, in this case, the grand jury foreperson.

The Committee understands that there may be opposition to requiring redaction of these documents for several reasons. The first being, in the case of an indictment, concern about the impact of redaction upon the requirement in Rule 6 of the Federal Rules of Criminal Procedure that the indictment be signed by the foreperson. Following the guidance, the indictment would still be signed and returned in open court, where it could be stated on the record that the foreperson's signature is on the return. However, to protect the identity of the foreperson, the publicly available copy of the indictment would confirm but not display the signature of the foreperson. The indictment with the signature could be sealed or retained by the government. There may also be concern over retaining two copies of the indictment, one sealed with the signature and one public without it. This concern is understandable because it does require some duplication of records, but it is necessary in order to both protect the juror and provide the public with the information contained in the charging document. Finally, concern has been expressed over who will effect the redaction of the indictment. In keeping with the redaction requirements elsewhere in the Privacy Policy, it is recommended that the government, as the filer of the document, have this responsibility.

In summary, the CACM Committee generally supports the proposed privacy rules and recognizes and appreciates the difficult task undertaken by the Rules Committee in drafting them. The CACM Committee also appreciates the opportunity to comment on the proposed rules and to have been included during the drafting process. Please do not hesitate to contact Abel Mattos of the Court Administration Policy Staff at 202-502-1560 if you have any questions.

Attachments

Home : Electronic Access to Courts : Judiciary Privacy Policy Page : Privacy Policy : Judicial Conference Report

Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files

The Judicial Conference of the United States requested that its Committee on Court Administration and Case Management examine issues related to privacy and public access to electronic case files. The Committee on Court Administration and Case Management formed a special subcommittee for this purpose. This subcommittee, known as the Subcommittee on Privacy and Public Access to Electronic Case Files, consisted of four members of the Committee on Court Administration and Case Management: Judge John W. Lungstrum, District of Kansas, Chair; Judge Samuel Grayson Wilson, Western District of Virginia; Judge Jerry A. Davis, Magistrate Judge, Northern District of Mississippi; and Judge J. Rich Leonard, Bankruptcy Judge, Eastern District of North Carolina, and one member from each of four other Judicial Conference Committees (liaison Committees): Judge Emmet Sullivan, District of Columbia, liaison from the Committee on Criminal Law; Judge James Robertson, District of Columbia, liaison from the Committee on Automation and Technology; Judge Sarah S. Vance, Eastern District of Louisiana, liaison from the Committee on the Administration of the Bankruptcy System; and Gene W. Lafitte, Esq., Liskow and Lewis, New Orleans, Louisiana, liaison from the Committee on the Rules of Practice and Procedure. After a lengthy process described below, the Subcommittee on Privacy and Public Access to Electronic Case Files, drafted a report containing recommendations for a judiciary-wide privacy and access policy.

The four liaison Committees reviewed the report and provided comments on it to the full Committee on Court Administration and Case Management. After carefully considering these comments, as well as comments of its own members, the Committee on Court Administration and Case Management made several changes to the subcommittee report, and adopted the amended report as its own.

Brief History of the Committee's Study of Privacy Issues

The Committee on Court Administration and Case Management, through its Subcommittee on Privacy and Public Access to Electronic Case Files (the Subcommittee) began its study of privacy and security concerns regarding public electronic access to case file information in June 1999. It has held numerous meetings and conference calls and received information from experts and academics in the privacy arena, as well as from court users, including judges, court clerks, and government agencies. As a result, in May 2000, the Subcommittee developed several policy options and alternatives for the creation of a judiciary-wide electronic access privacy policy which were presented to the full Committee on Court Administration and Case Management and the liaison committees at their Summer 2000 meetings. The Subcommittee used the opinions and feedback from these committees to further refine the policy options.

In November 2000, the Subcommittee produced a document entitled "Request for Comment on Privacy and Public Access to Electronic Case Files." This document contains the alternatives the Subcommittee perceived as viable following the committees' feedback. The Subcommittee published this document for public comment from November 13, 2000 through January 26, 2001. A website at www.privacy.uscourts.gov was established to publicize the comment document and to collect the comments. Two hundred forty-two comments were received from a very wide range of interested persons including private citizens, privacy rights groups, journalists, private investigators, attorneys, data re-sellers and representatives of the financial services industry. Those comments, in summary and full text format, are available at that website.

On March 16, 2001, the Subcommittee held a public hearing to gain further insight into the issues surrounding privacy and access. Fifteen individuals who had submitted written comments made oral presentations to and answered the questions of Subcommittee members. Following the hearing, the Subcommittee met, considered the comments received, and reached agreement on the policy recommendations contained in this document.

Background

Federal court case files, unless sealed or otherwise subject to restricted access by statute, federal rule, or Judicial Conference policy, are presumed to be available for public inspection and copying. See *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978) (holding that there is a common law right "to inspect and copy public records and documents, including judicial records and documents"). The tradition of public access to federal court case files is also rooted in constitutional principles. See *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575-78 (1980). However, public access rights are not absolute, and courts balance access and privacy interests in making decisions about the public disclosure and dissemination of case files. The authority to protect personal privacy and other legitimate interests in nondisclosure is based, like public access rights, in common law and constitutional principles. See *Nixon*, 435 U.S. at 596 ("[E]very 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").

The term "case file" (whether electronic or paper) means the collection of documents officially filed by the litigants or the court in the context of litigation, the docket entries that catalog such filings, and transcripts of judicial proceedings. The case file generally does not include several other types of information, including non-filed discovery material, trial exhibits that have not been admitted into evidence, drafts or notes by judges or court staff, and various documents that are sometimes known as "left-side" file material. Sealed material, although part of the case file, is accessible only by court order.

Certain types of cases, categories of information, and specific documents may require special protection from unlimited public access, as further specified in the sections on civil, criminal, bankruptcy and appellate case files below. See *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) (noting that technology may affect the balance between access rights and privacy and security interests). To a great extent, these recommendations rely upon counsel and litigants to act to protect the interests of their clients and themselves. This may necessitate an effort by the courts to educate the bar and the public about the fact that documents filed in federal court cases may be available on the Internet.

It is also important to note that the federal courts are not required to provide electronic access to case files (assuming that a paper file is maintained), and these recommendations do not create any entitlement to such access. As a practical matter, during this time of transition when courts are implementing new practices, there may be disparity in access among courts because of varying technology. Nonetheless, the federal courts recognize that the public should share in the benefits of information technology, including more efficient access to court case files.

These recommendations propose privacy policy options which the Committee on Court Administration and Case Management (the Committee) believes can provide solutions to issues of privacy and access as those issues are now presented. To the extent that courts are currently experimenting with procedures which differ from those articulated in this document, those courts should reexamine those procedures in light of the policies outlined herein. The Committee recognizes that technology is ever changing and these recommendations may require frequent re-examination and revision.

Recommendations

The policy recommended for adoption by the Judicial Conference is as follows:

General Principles

1. There should be consistent, nationwide policies in federal courts in order to ensure that similar privacy protections and access presumptions apply regardless of which federal court is the custodian of a particular case file.
2. Notice of these nationwide policies should be given to all litigants in federal court so that they will be aware of the fact that materials which they submit in a federal court proceeding could become available on the Internet.
3. Members of the bar must be educated about the policies and the fact that they must protect their clients by carefully examining the documents that they file in federal court for sensitive, private information and by making the appropriate motions to protect documents from electronic access when necessary.
4. Except where otherwise noted, the policies apply to both paper and electronic files.
5. Electronic access to docket sheets through PACERNet and court opinions through court websites will not be affected by these policies.
6. The availability of case files at the courthouse will not be affected or limited by these policies.
7. Nothing in these recommendations is intended to create a private right of action or to limit the application of Rule 11 of the Federal Rules of Civil Procedure.

Case Types

Civil Case Files

Recommendation: That documents in civil case files should be made available electronically to the same extent that they are available at the courthouse with one exception (Social Security cases should be excluded from electronic access) and one change in policy (the requirement that certain "personal data identifiers" be modified or partially redacted by the litigants). These identifiers are Social Security numbers, dates of birth, financial account numbers and names of minor children.

The recommendation provides for liberal remote electronic access to civil case files while also adopting some means to protect individual privacy. Remote electronic access will be available only through the PACERNet system which requires registration with the PACER service center and the use of a log in and password. This creates an electronic trail which can be retraced in order to determine who accessed certain information if a problem arises. Further, this recommendation contemplates that certain personal, identifying information will not be included in its full and complete form in case documents, whether electronic or hard copy. For example, if the Social Security number of an individual must be included in a document, only the last four digits of that number will be used whether that document is to be filed electronically or at the courthouse. If the involvement of a minor child must be mentioned, only that child's initials should be used; if an individual's date of birth is necessary, only the year should be used; and, if financial account numbers are relevant, only the last four digits should be recited in the document. It is anticipated that as courts develop local rules and instructions for the use and implementation of Electronic Case Filing (ECF), such rules and instructions will include direction on the truncation by the litigants of personal identifying information. Similar rule changes would apply to courts which are imaging documents.

Providing remote electronic access equal to courthouse access will require counsel and pro se litigants to protect their interests through a careful review of whether it is essential to their case to file certain documents containing private sensitive information or by the use of motions to seal and for protective orders. It will also depend upon the discretion of judges to protect privacy and security interests as they arise in individual cases. However, it is the experience of the ECF prototype courts and courts which have been imaging documents and making them electronically available that reliance on judicial discretion has not been problematic and has not dramatically increased or altered the amount and nature of motions to seal. It is also the experience of those courts that have been making their case file information available through PACERNet that there have been virtually no reported privacy problems as a result.

This recommended "public is public" policy is simple and can be easily and consistently applied nationwide. The recommended policy will "level the geographic playing field" in civil cases in federal court by allowing attorneys not located in geographic proximity to the courthouse easy access. Having both remote electronic access and courthouse access to the same information will also utilize more fully the technology available to the courts and will allow clerks' offices to better and more easily serve the needs of the bar and the public. In addition, it might also discourage the possible development of a "cottage industry" headed by data re-sellers who, if remote electronic access were restricted, could go to the courthouse, copy the files, download the information to a private website, and charge for access to that website, thus profiting from the sale of public information and undermining restrictions intended to protect privacy.

Each of the other policy options articulated in the document for comment presented its own problems. The idea of defining what documents should be included in the public file was rejected because it would require the courts to restrict access at the courthouse to information that has traditionally been available from courthouse files. This would have the net effect of allowing less overall access in a technological age where greater access is easy to achieve. It would also require making the very difficult determination of what information should be included in the public file.

The Committee seriously considered and debated at length the idea of creating levels of access to electronic documents (i.e., access to certain documents for specific users would be based upon the user's status in the case). The Committee ultimately decided that levels of access restrictions were too complicated in relation to the privacy benefits which could be derived therefrom. It would be difficult, for example, to prohibit a user with full access to all case information, such as a party to the case, from downloading and disseminating the restricted information. Also, the levels of access would only exist in relation to the remote electronic file and not in relation to the courthouse file. This would result in unequal remote and physical access to the same information and could foster a cottage industry of courthouse data collection as described above.

Seeking an amendment to the Federal Rules of Civil Procedure was not recommended for several reasons. First, any such rules amendment would take several years to effectuate, and the Committee concluded that privacy issues need immediate attention. There was some discussion about the need for a provision in Fed. R. Civ. P. 11 providing for sanctions against counsel or litigants who, as a litigation tactic, intentionally include scurrilous or embarrassing, irrelevant information in a document so that this information will be available on the Internet. The Committee ultimately determined that, at least for now, the current language of Fed. R. Civ. P. 11 and the inherent power of the court are sufficient to deter such actions and to enforce any privacy policy.

As noted above, this recommendation treats Social Security cases differently from other civil case files. It would limit remote electronic access. It does contemplate, however, the existence of a skeletal electronic file in Social Security cases which would contain documents such as the complaint, answer

and dispositive cross motions or petitions for review as applicable but not the administrative record and would be available to the court for statistical and case management purposes. This recommendation would also allow litigants to electronically file documents, except for the administrative record, in Social Security cases and would permit electronic access to these documents by litigants only.

After much debate, the consensus of the Committee was that Social Security cases warrant such treatment because they are of an inherently different nature from other civil cases. They are the continuation of an administrative proceeding, the files of which are confidential until the jurisdiction of the district court is invoked, by an individual to enforce his or her rights under a government program. Further, all Social Security disability claims, which are the majority of Social Security cases filed in district court, contain extremely detailed medical records and other personal information which an applicant must submit in an effort to establish disability. Such medical and personal information is critical to the court and is of little or no legitimate use to anyone not a party to the case. Thus, making such information available on the Internet would be of little public benefit and would present a substantial intrusion into the privacy of the claimant. Social Security files would still be available in their entirety at the courthouse.

Criminal Case Files

Recommendation: That public remote electronic access to documents in criminal cases should not be available at this time, with the understanding that the policy will be reexamined within two years of adoption by the Judicial Conference.

The Committee determined that any benefits of public remote electronic access to criminal files were outweighed by the safety and law enforcement risks such access would create. Routine public remote electronic access to documents in criminal case files would allow defendants and others easy access to information regarding the cooperation and other activities of defendants. Specifically, an individual could access documents filed in conjunction with a motion by the government for downward departure for substantial assistance and learn details of a defendant's involvement in the government's case. Such information could then be very easily used to intimidate, harass and possibly harm victims, defendants and their families.

Likewise, routine public remote electronic access to criminal files may inadvertently increase the risk of unauthorized public access to preindictment information, such as unexecuted arrest and search warrants. The public availability of this information could severely hamper and compromise investigative and law enforcement efforts and pose a significant safety risk to law enforcement officials engaged in their official duties. Sealing documents containing this and other types of sensitive information in criminal cases will not adequately address the problem, since the mere fact that a document is sealed signals probable defendant cooperation and covert law enforcement initiatives.

The benefit to the public of easier access to criminal case file information was not discounted by the Committee and, it should be noted that, opinions and orders, as determined by the court, and criminal docket sheets will still be available through court websites and PACER and PACERNet. However, in view of the concerns described above, the Committee concluded that individual safety and the risk to law enforcement personnel significantly outweigh the need for unfettered public remote access to the content of criminal case files. This recommendation should be reconsidered if it becomes evident that the benefits of public remote electronic access significantly outweigh the dangers to victims, defendants and their families, and law enforcement personnel.

Bankruptcy Case Files

Recommendation: That documents in bankruptcy case files should be made generally available electronically to the same extent that they are available at the courthouse, with a similar policy change for personal identifiers as in civil cases; that § 107(b)(2) of the Bankruptcy Code should be amended to establish privacy and security concerns as a basis for the sealing of a document; and that the Bankruptcy Code and Rules should be amended as necessary to allow the court to collect a debtor's full Social Security number but display only the last four digits.

The Committee recognized the unique nature of bankruptcy case files and the particularly sensitive nature of the information, largely financial, which is contained in these files; while this recommendation does provide open remote electronic access to this information, it also accommodates the privacy concerns of individuals. This recommendation contemplates that a debtor's personal, identifying information and financial account numbers will not be included in their complete forms on any document, whether electronic or hard copy (i.e., only the last four digits of Social Security and financial account numbers will be used). As the recommendation recognizes, there may be a need to amend the Bankruptcy Code to allow only the last four digits of an individual debtor's Social Security number to be used. The bankruptcy court will collect the full Social Security number of debtors for internal use, as this number appears to provide the best way to identify multiple bankruptcy filings. The recommendation proposes a minor amendment to § 107(a) to allow the court to collect the full number, but only display the last four digits. The names of minor children will not be included in electronic or hard copies of documents.

As with civil cases, the effectiveness of this recommendation relies upon motions to seal filed by litigants and other parties in interest. To accomplish this result, an amendment of 11 U.S.C. § 107(b), which now narrowly circumscribes the ability of the bankruptcy courts to seal documents, will be needed to establish privacy and security concerns as a basis for sealing a document. Once again, the experiences of the ECF prototype and imaging courts do not indicate that this reliance will cause a large influx of motions to seal. In addition, as with all remote electronic access, the information can only be reached through the log-in and password- controlled PACERNet system.

The Committee rejected the other alternatives suggested in the comment document for various reasons. Any attempt to create levels of access in bankruptcy cases would meet with the same problems discussed with respect to the use of levels of access for civil cases. Bankruptcy cases present even more issues with respect to levels of access because there are numerous interests which would have a legitimate need to access file information and specific access levels would need to be established for them. Further, many entities could qualify as a "party in interest" in a bankruptcy filing and would need access to case file information to determine if they in fact have an interest. It would be difficult to create an electronic access system which would allow sufficient access for that determination to be made without giving full access to that entity.

The idea of collecting less information or segregating certain information and restricting access to it was rejected because the Committee determined that there is a need for and a value in allowing the public access to this information. Further, creating two separate files, one totally open to the public and one with restricted access, would place a burden on clerks' offices by requiring the management of two sets of files in each case.

Appellate Case Files

Recommendation: That appellate case files be treated at the appellate level the same way in which they are treated at the lower level.

This recommendation acknowledges the varying treatment of the different case types at the lower level and carries that treatment through to the appellate level. For cases appealed to the district court or the court of appeals from administrative agencies, the documents in the appeal will be treated, for the purposes of remote electronic access, in the same manner in which they were treated by the agency. For cases appealed from the district court, the case file will be treated in the manner in which it was treated by the district court with respect to remote electronic access.

[Home](#) : [Electronic Access to Courts](#) : [Judiciary Privacy Policy Page](#) : Guidance for Implementation

Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files

In September 2001, the Judicial Conference of the United States adopted a policy on privacy and public access to electronic case files (JCUS-SEP/OCT 01, pp. 48-50). This policy addressed civil, criminal, bankruptcy and appellate case files separately. With regard to criminal case files, the policy prohibited remote public access to criminal case files at that time, with the explicit statement that the Conference would revisit this issue within two years. In March 2002, the Judicial Conference approved the establishment of a pilot project that would allow 11 courts, ten district courts and one court of appeals, to provide remote electronic public access to criminal case files (JCUS-MAR 02, p. 10). A study of these courts conducted by the Federal Judicial Center outlined the advantages and disadvantages of such access, to court employees, the bar, and the public. The study did not reveal any instances of harm due to remote access to criminal documents. The results of the study were reported to the Committees on Court Administration and Case Management and Criminal Law.

The Committee on Court Administration and Case Management reviewed and discussed the study in depth, ultimately concluding that the benefits of remote public electronic access to criminal case file documents outweighed the risks of harm such access potentially posed. This decision was based not only on the results of the FJC study, but also on the extensive information the Committee, through its Privacy Subcommittee, gathered and evaluated during the period of deliberation that led to the Judicial Conference's adoption of the initial privacy policy in September 2001. That process included the receipt of 242 comments from a wide variety of interested persons including private citizens, privacy advocacy groups, journalists, attorneys, government agencies, private investigators, data re-sellers and members of the financial services industry. It also included a public hearing at which 15 individuals representing a wide spectrum of public, private, and government interest made oral presentations and answered questions from Privacy Subcommittee members.

From the comments received and presentations made, it was clear that remote electronic access to public case file information provides numerous benefits. Specifically, several speakers noted that such access provides citizens the opportunity to see and understand the workings of the court system, thereby fostering greater confidence in government. The benefit that electronic access "levels the geographic playing field" by allowing individuals not located in proximity to the courthouse easy access to what is already public information was also frequently mentioned. Others noted that providing remote electronic access to this same public information available at the courthouse would discourage the creation of a "cottage industry" by individuals who could go to the courthouse, copy and scan information, download it to a private website and charge for access, thus profiting from the sale of public information and undermining restrictions intended to protect privacy.

After thoroughly analyzing and weighing all of the information before it, in June 2003, the Committee on Court Administration and Case Management recommended that the Judicial Conference amend its prohibition on remote public access to electronic criminal case files, the amendment to become effective only after specific guidance for the

courts was developed. The Committee on Criminal Law concurred in this recommendation.

At its September 2003 session, the Conference discussed the issue and adopted the recommendation, thereby amending its policy regarding remote public access to electronic criminal case file documents to permit such access to be the same as public access to criminal case file documents at the courthouse with the effective date of this new policy delayed until such time as the Conference approves specific guidance on the implementation and operation of the policy developed by the Committees on Court Administration and Case Management, Criminal Law and Defender Services (JCUS-SEP 03, pp. 15-16).

This guidance, which was prepared by a specially-created subcommittee consisting of members from the Committees on Court Administration and Case Management, Criminal Law and Defender Services and approved by the Judicial Conference, sets forth the implementation guidelines required by the Judicial Conference. This document has three parts. The first provides a short explanation of the policy on remote public access to electronic criminal case files and explains how it relates to similar policies for other case types. The second part provides information about the redaction requirements which are an integral part of the policy and require the court to educate the bar and other court users. The third part is a discussion of specific documents that courts are not to make available to the public.

I. Explanation of the policy permitting remote public access to electronic criminal case file documents

Not all documents associated with a criminal case are properly included in the criminal case file. The policy regarding remote public electronic access to criminal case file documents is intended to make all case file documents that are available to the public at the courthouse available to the public via remote, electronic access if a court is making documents remotely, electronically available through the Case Management/Electronic Case Files system or by the scanning of paper filings to create an electronic image. Simply stated, if a document can be accessed from a criminal case file by a member of the public at the courthouse, it should be available to that same member of the public through the court's electronic access system. This is true if the document was filed electronically or converted to electronic form.

This policy treats criminal case file documents in much the same way civil and bankruptcy case file documents are treated. Filers of documents have the obligation to partially redact specific personal identifying information from documents before they are filed. (See Section II, below for a discussion of redaction requirements.) However, because of the security and law enforcement issues unique to criminal case file information, some specific criminal case file documents will not be available to the public remotely or at the courthouse. (See Section III, below for a discussion of these documents.) It is not the intent of this policy to expand the documents that are to be included in the public criminal case file and, thereby, available both at the courthouse and electronically to those with PACER access.

It should also be noted that at its September 2003 session, the Judicial Conference adopted a policy that provides for the electronic availability of transcripts of court proceedings. The effective date of this policy is delayed pending a report of the Judicial

Resources Committee regarding the impact the policy may have on court reporter compensation. However, once that policy becomes effective, there are separately articulated requirements and procedures regarding redaction which will apply to transcripts in criminal cases.

II. Redaction and Sealing Requirements

The policy adopted by the Conference in September 2003 states in part:

Upon the effective date of any change in policy regarding remote public access to electronic criminal case file documents, require that personal data identifiers be redacted by the filer of the document, whether the document is filed electronically or in paper, as follows:

1. Social Security numbers to the last four digits;
2. financial account numbers to the last four digits;
3. names of minor children to the initials;
4. dates of birth to the year; and
5. home addresses to city and state[.]

In order to inform all court users of these requirements, courts should post a Notice of Electronic Availability of Criminal Case File Documents on their websites and in their clerks' offices. An example of such a notice appears below. As part of the pilot project and study conducted by the Federal Judicial Center (FJC), participating courts were asked to implement similar redaction requirements and to inform all court users of these requirements. To assist in these requests, the participating courts were provided with a sample Notice of Electronic Availability of Criminal Case File Documents that was reviewed by a Subcommittee of the Committee on Court Administration and Case Management, with a representative from the Criminal Law Committee, that was working with the FJC on the study's design. It was suggested that the courts post this notice on their websites and in their clerks' offices in order to inform all filers and other court users that documents filed in criminal cases will be available to the general public on the Internet and that the filer has the obligation to redact the specified identifying information from the document prior to filing. A version of this notice, updated to reference the E-Government Act of 2002, is provided.

Please be informed that documents filed in criminal cases in this court are now available to the public electronically.

You shall not include sensitive information in any document filed with the court. You must remember that any personal information not otherwise protected will be made available over the Internet via WebPACER. The following personal data identifiers must be partially redacted from the document whether it is filed traditionally or electronically: Social Security numbers to the last four digits; financial account numbers to the last four digits; names of minor children to the initials; dates of birth to the year; and home addresses to the city and state.

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers specified above may file an

unredacted document under seal. This document shall be retained by the court as part of the record. The court may, however, also require the party to file a redacted copy for the public file.

Because filings will be remotely, electronically available and may contain information implicating not only privacy but also personal security concerns, exercise caution when filing a document that contains any of the following information and consider accompanying any such filing with a motion to seal. Until the court has ruled on any motion to seal, no document that is the subject of a motion to seal, nor the motion itself or any response thereto, will be available electronically or in paper form.

- 1) any personal identifying number, such as driver's license number;
- 2) medical records, treatment and diagnosis;
- 3) employment history;
- 4) individual financial information;
- 5) proprietary or trade secret information;
- 6) information regarding an individual's cooperation with the government;
- 7) information regarding the victim of any criminal activity;
- 8) national security information; and
- 9) sensitive security information as described in 49 U.S.C. § 114 (s).

Counsel is strongly urged to share this notice with all clients so that an informed decision about the inclusion of certain materials may be made. If a redacted document is filed, it is the sole responsibility of counsel and the parties to be sure that all documents and pleadings comply with the rules of this court requiring redaction of personal data identifiers. The clerk will not review filings for redaction.

The court should also be aware that it will need to partially redact the personal identifiers listed above from documents it prepares that routinely contain such information (e.g., order setting conditions of release).

III. Documents for which public access should not be provided

The following documents shall not be included in the public case file and should not be made available to the public at the courthouse or via remote electronic access:

- unexecuted summonses or warrants of any kind (e.g., search warrants, arrest warrants);
- 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 (e.g., motions for downward departure for substantial assistance, plea agreements indicating cooperation)

Courts maintain the discretion to seal any document or case file sua sponte. If the court seals a document after it has already been included in the public file, the clerk shall remove the document from both the electronic and paper public files as soon as the order sealing the document is entered. Counsel and the courts should appreciate that the filing of an unsealed document in the criminal case file will make it available both at the courthouse and by remote electronic access. Courts should assess whether privacy or law enforcement concerns, or other good cause, justify filing the document under seal.

There are certain categories of criminal case documents that are available to the public in the clerk's office but will not be made available electronically because they are not to be included in the public case file for individual criminal cases. These include but are not limited to vouchers for claims for payment, including payment for transcripts, (absent attached or supporting documentation) submitted pursuant to the Criminal Justice Act. (For detailed guidance about the public availability of Criminal Justice Act information, please see paragraph 5.01 of Volume VII of *Guide to Judiciary Policies and Procedures*.)

Model Local Rule Regarding Privacy and Public Access to Electronic Criminal Case Files

In compliance with the policy of the Judicial Conference of the United States, and the E-Government Act of 2002, and in order to promote electronic access to documents in the criminal case files while also protecting personal privacy and other legitimate interests, parties shall refrain from including, or shall partially redact where inclusion is necessary, the following personal data identifiers from all documents filed with the court, including exhibits thereto, whether filed electronically or in paper, unless otherwise ordered by the court.

- a. **Social Security numbers.** If an individual's Social Security number must be included, only the last four digits of that number should be used.
- b. **Names of minor children.** If the involvement of a minor child must be mentioned, only the initials of the child should be used.
- c. **Dates of birth.** If an individual's date of birth must be included, only the year should be used.
- d. **Financial account numbers.** If financial account numbers are relevant, only the last four digits of the number should be used.
- e. **Home addresses.** If a home address must be included, only the city and state should be listed.

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers listed above may file an unredacted document under seal. This document shall be retained by the court as part of the record. The court, may, however, still require the party to file a redacted copy for the public file.

The responsibility for redacting these personal identifiers rests solely with counsel and the parties. The clerk will not review filings for compliance with this rule.

COMMENTARY

Parties should consult the "Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files." This Guidance explains the policy permitting remote public access to electronic criminal case file documents and sets forth redaction and sealing requirements for documents that are filed. The Guidance also lists documents for which public access should not be provided. A copy of the Guidance is available at the court's website.