



**U.S. Department of Justice**

*Executive Office for United States Attorneys  
Office of the Director*

*RFK Main Justice Building, Room 2261  
950 Pennsylvania Avenue, NW  
Washington, DC 20530*

*(202) 514-2121*

October 26, 2007

Mr. Abel J. Matos, Chief  
Court Administration Policy Staff  
Administrative Office of the United States Courts  
*Attn:* Privacy Comments  
1 Columbus Circle, N.E. (Suite 4-560)  
Washington, DC 20544  
[privacycomments@ao.uscourts.gov](mailto:privacycomments@ao.uscourts.gov)

Re: Response to Request for Comments on the Privacy and Security Implications of  
Public Internet Access to Federal Plea Agreements

Dear Mr. Matos:

I am pleased to transmit the views of the Department of Justice in response to the request for comments by the Court Administration and Case Management Committee (CACM) of the Judicial Conference of the United States. The request seeks public comments on (1) a proposal to remove all criminal plea agreements from the court's Internet access system, the Public Access to Court Electronic Records (PACER) system, and (2) possible policy alternatives to that proposal. *See* 72 Fed. Reg. 51659 (Sept. 10, 2007).

The proposal upon which comments are being sought is the proposal that the Department of Justice made to the CACM back in December 2006. The Department continues to support its proposal, as discussed below. Additionally, we discuss the risks and benefits of some other policy alternatives, including a tiered access approach whereby the clerk's office could limit public Internet access to plea agreements on a case by case basis, and the possibility that the sensitive, cooperation portion of a plea agreement be provided to the court in a non-public document, custody of which might be maintained by the United States Attorney's Office.

The Department recognizes the inherent difficulty in balancing the competing interests of security and public access. We note that the integrity of the judicial process is implicated on both sides of the ledger because threats to witnesses, cooperating defendants, and law enforcement affect not just the particular individuals involved, but the overall reliability of the criminal adjudication process as well. We appreciate the serious consideration that the CACM has given to this issue thus far, as well as the opportunity here to further elucidate our views.

### Background

When the Judicial Conference first proposed allowing electronic access to criminal cases in 2000, the Department warned of security risks and proposed a tiered approach whereby the public could be afforded full Internet access to “basic or ‘core’ information for purposes of monitoring the criminal justice system,” while other more sensitive documents would be provided only to litigants and law enforcement. *See* Comment No. 240 (2/9/01), Department of Justice, [www.privacy.uscourts.gov/matrix.htm](http://www.privacy.uscourts.gov/matrix.htm).

Thereafter, the Judicial Conference instituted a two-year pilot program in ten district courts under which criminal case documents were filed electronically with the court and were made available on the Internet. All non-sealed criminal case documents were made available on the Internet in the ten pilot districts. Pilot program policy required that certain personal identifiers – such as Social Security Numbers (SSNs) and financial account numbers, dates of birth, minor children’s names, and home addresses – be redacted from criminal filings prior to submission.<sup>1</sup> In 2003, following completion of the two year pilot program, the Judicial Conference found “no significant reports of misuse of criminal case documents . . . [or] harm stemming from the availability of these documents via public Internet access.” 72 Fed. Reg. at 51660.

Since that time, the reach of the Internet has continued to expand, however, and there are a variety of Internet-related threats to personal security today that did not exist in 2003. Electronic forms of identity theft and Internet scams such as “phishing” have greatly increased in number and sophistication since 2003. Of particular concern for these purposes is the website [www.whosarat.com](http://www.whosarat.com), which came online well after the close of the two-year pilot study. This website appears to be dedicated to identifying those individuals who cooperate with the government in criminal prosecutions. The posting on this website of personal and sensitive information about cooperating witnesses, defendants, and informants has created a potentially serious risk of harm, and the site has already created substantial difficulties in several federal prosecutions. The site provides an “informant profile” for each listed individual, and contains pictures and personal data, including age and the city where the individual is believed to live. In addition, for some cooperating defendants, the site posts a copy of the actual cooperation plea agreement, downloaded from the courts’ PACER system.

### The Department’s December 2006 Recommendation

In December 2006 the Department proposed to CACM that it adopt a uniform policy removing all plea agreements in criminal cases (including docket notations thereof) from Internet access via PACER. Our recommendation was patterned after the Judicial Conference’s policy excluding Social Security cases from remote electronic access, in order to mitigate witness safety

---

<sup>1</sup>That policy is similar to the currently pending Criminal Rule 49.1, which will take effect in December 1, 2007 absent Congressional action. [www.uscourts.gov/rules](http://www.uscourts.gov/rules).

issues and protect the privacy of sensitive personal information.<sup>2</sup> The Department's proposal was in direct response to Internet security dangers, such as the Whosarat website, that did not exist during the pilot study just a few years earlier.

In making our proposal we noted the increase in violent, victim-related crimes in federal court. *See, e.g.*, Federal Judicial Caseload Statistics 2005, Table D-2 (reporting that, from 2001 to 2005, there has been an 18% increase in assault charges, a 23% increase in kidnapping, a 24% increase in violent racketeering, and a 36% increase in firearm offenses). Cases such as these, as well as gang-related prosecutions which the Department has made a priority in recent years, typically require testimony from either victims or cooperating defendants. The level of retaliation and witness intimidation in such cases is high and getting higher.

Combined with this trend is the increasingly sophisticated use of computers by the violent criminal element. It has been reported that some gang members have opened PACER accounts. It is understood that defendants utilize public websites to check on the incarcerated status of their associates. In our December proposal we noted "the rise of a new 'cottage industry' engaged in republishing court filings and related information about cooperators on public websites for the clear purpose of witness intimidation, retaliation, and harassment." Thus, we believe that any policy addressing security and public access issues should anticipate the continued and increasing use of the Internet by those who would seek to intimidate witnesses and threaten the integrity of the judicial process.

Our proposal addressed these converging trends by recommending the removal from PACER of all plea criminal agreements, which are a primary, albeit not the only, source of sensitive, personal information used to intimidate cooperating defendants and other participants in the criminal process. Under our proposal all non-sealed plea agreements and related docket entries would still be available for public viewing at the courthouse, either electronically or in paper form. Examples of related docket entries include those for the plea hearing and any continuances, as well as the filing of the plea agreement itself.

It has been noted that the Department's proposal is overinclusive, in that all plea agreements would be removed from PACER, not just those that are sealed or contain cooperation agreements, and at the same time incomplete, in that other criminal documents that might potentially reveal cooperation or sensitive information would remain on PACER, and non-sealed cooperation plea agreements would still be publicly available at the courthouse, either in paper or electronic form. By definition, no balancing of the competing concerns here can fully satisfy both interests. We believe the uniform removal of all plea agreements and related docket entries is appropriate for the following reasons.

---

<sup>2</sup>The Department also recommended that PACER computer screens contain user warnings against misuse of the downloaded documents, and that a uniform policy be adopted prohibiting camera cell phones and similar devices in the courtroom. Those two recommendations are not the subject of these comments, and we do not elaborate on them here.

First, we proposed the removal from PACER of all non-sealed plea agreements, including those without cooperation agreements, in order to foil the interested PACER reviewer who would otherwise be able to discern without too much difficulty that the only items being removed from PACER were cooperation plea agreements. When all pleas agreements are routinely removed from PACER, an interested PACER reviewer does not know which pleas will contain cooperation agreements. Additional effort to discern this fact would have to be expended by physically going to the courthouse to see the document. The Department's proposal seeks to induce precisely that additional effort. Thus, our proposal bars access to plea agreements only to those who do not have sufficient interest in the case to physically travel to see the documents. In other words, solely with regards to plea agreements, public access would be the same as prior to the implementation of electronic filing.

Second, with regard to the removal from PACER of docket entries for pleas, including pleas under seal, the proposal seeks to alleviate the "red flag" that results when notation of a sealed docket entry appears on PACER. We believe that for "anyone with Internet access, a PACER account, and a basic familiarity with the criminal docketing system, the notation of a sealed plea agreement or docket entry in connection with a particular defendant is often a red flag that the defendant is cooperating with the government."<sup>3</sup>

Finally, our proposed policy was intended to provide a bright line, *i.e.*, all plea agreements that were easy to follow in order to eliminate inadvertent mistakes. Were such a bright line policy to be adopted, prosecutors would expect to rely on the certain exclusion from PACER of all plea agreements and related docket entries. Such reliance would factor into the prosecutor's decision whether or not to seek to seal a particular plea agreement.

Prosecutors always have the option to seek an order to file plea agreements under seal. But we do not believe that a wholesale increase in the number of documents filed under seal is the appropriate response to Internet-based security threats, such as the Whosarat website.<sup>4</sup> Rather, our proposal was based on the belief that a fair balancing of the interests at stake militates in favor of public access to plea agreements at the clerk's office, but not the instantaneous, permanent, and literally worldwide access created by the Internet.

It has also been suggested that a blanket policy of removing all plea agreements from PACER may be inconsistent with currently pending Criminal Rule 49.1, which, as noted above, will take effect absent Congressional action on December 1, 2007. Rule 49.1 deals with the

---

<sup>3</sup>For the same reason that a mere docket entry is a red flag, no policy based on simply redacting sensitive information from plea agreements while still having them available on PACER can be seriously considered. The redaction of such information would announce the defendant's cooperation as loudly as if it were printed on the page.

<sup>4</sup>Certainly the Department maintains a strong presumption against closed proceedings. The Deputy Attorney General must expressly approve any motion seeking to seal a courtroom proceeding, and such motions are rare. *See* USAM 9-5.150.

redaction of personal identifiers and sensitive information, such as social security numbers, dates of birth, precise home addresses, a minor's initials, and financial account numbers. The removal of plea agreements from PACER would not affect the need to redact such personally identifying information. Rule 49.1(e) allows a court "by order in a case" to "limit or prohibit a nonparty's remote electronic access to a document filed with the court." Thus, the text of the rule allows for case by case action in limiting remote electronic access. Yet we see no reason why the CACM or the Judicial Conference would be prevented by the text of the rule from adopting as a policy matter that a particular class of documents are inappropriate for remote electronic access.

We note that several district courts, including the Southern District of Florida, the Eastern District of Pennsylvania and the Western District of Texas have adopted policies similar to, or as restrictive as, our recommendation.

#### Alternative Policy Approaches

Although the Department believes the uniform removal of all plea agreements and corresponding docket entries presents the best balancing of public access with security protection, we acknowledge that other alternatives may accommodate the Departments' interests to varying degrees.

First, a closely related approach would be to file all plea agreements electronically, but to electronically limit access to the court, counsel for the defendant, and counsel for the government. This has the attraction of maintaining the agreement in electronic form and making the agreement available for the litigants or the court as may be necessary. It differs from our original proposal in that it assumes that all pleas would be filed electronically, and an electronic version would be made available in the Clerk's office for public review.

A second alternative approach would be for the court clerk to remove remote Internet access for particular plea agreements or other criminal documents that contain sensitive information on a case by case basis upon the filing of a motion for protective order.<sup>5</sup> The potential benefit to this approach is that it would by default retain full remote electronic access to those plea agreements and other documents that carry little risk of retaliation for the defendant or witness involved. A potential risk to any case by case approach is that it affords more opportunities for human error than a uniform, bright line approach. Also, this approach would allow an interested, sophisticated, and ill-intentioned reviewer of PACER entries, upon checking at the courthouse, to deduce that the only documents being removed from PACER are those that contain sensitive information. Once such a deduction is made and broadcast to those who would seek to intimidate witnesses and cooperating defendants, then removing such documents from PACER is no longer of any value whatsoever.

Indeed, it is precisely the uniformity of the Department's proposal to remove all pleas that

---

<sup>5</sup>Presumably, such a motion would be filed under currently pending Rule 49.1(e), assuming that the rule becomes effective on December 1, 2007.

prevent that logical deduction from being made. Under the Department's proposal, an interested PACER reviewer who went to the courthouse to see what had been removed would find all types of plea agreements, most of which do not contain cooperation agreements.

The case by case approach also points up the importance of docket entries on PACER. As noted above, removal of the document itself without removing the corresponding docket entry is of little value. Thus, in the event that the case by case approach was adopted, and individual motions for protective order were required, such motions should be removed from PACER, as well as docket entries regarding them, or the very purpose for their being filed would be undermined. In many ways, the case by case approach is little different from the current procedural status, whereby a prosecutor can by motion seek to restrict the public's access to criminal documents in a variety of ways.

A third related approach for electronically filed plea agreements would be to arrange a uniform system of tiered electronic access with the Clerk's office. Certain documents would be restricted to just the defendant's counsel and the government, other documents might go to a broader group of counsel for all parties, and a third category would go to the general public. This approach would allow individual documents to be designated for a given level of access according to a set, pre-determined schedule, obviating the need for individual motions for each document. The drawback is that it would place a greater burden on the Clerk's office to track the access level for individual documents, increasing the risk of inadvertent error.

A fourth, alternative approach that has been alluded to is the possibility that prosecutors file a generic plea agreement in all cases that contains standard and hypothetical references to cooperation. In those cases where actual cooperation occurs the prosecutor could notify the court of a defendant's cooperation through a non-public document, *i.e.*, a "cooperation codicil." The benefits of such an approach are that it would permit public access to the basic fact of a defendant's plea while limiting sensitive information and any cooperation language from public inspection. Such a policy would address in some ways the Department's primary security concerns outlined above.

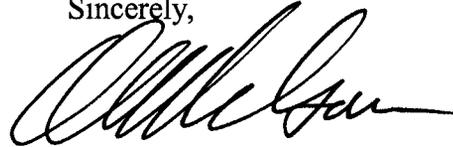
Risks to such a policy include the requirement that prosecutors maintain custody of the cooperation portion of a plea agreement, which is essentially a court exhibit. This could easily create custodial concerns as to exactly how the document was maintained by the prosecutor, whether it was the same document exhibited in court, etc. In most United States Attorneys' offices, and we believe in most district courts, such a practice is not used. We understand that some United States Attorneys' offices do have a practice of maintaining custody of plea agreements, and in those districts the culture of that process is well established, and by most accounts such a procedure works well in the districts where it occurs.

However, creating both the necessary procedures and the "legal culture" within both the USAO and the district courts whereby this process could work effectively would be a significant challenge. Moreover, current plea practices are not uniform across the county, nor does the Department expect that they should be. Although this approach does address in many respects

the security concerns prompting this discussion, we expect that implementation of such a policy across all the United States Attorneys' Offices would be difficult.

We very much appreciate CACM's desire to seek public comments on this important issue. We would be pleased to address the Committee, if you wish, in order to provide further details. Should you have any questions, please contact Anthony J. Ciccone (202-307-0003) in the Executive Office for United States Attorneys, which is the Department's program management office for electronic case filing issues.

Sincerely,

A handwritten signature in black ink, appearing to read "K. Melson", written in a cursive style.

Kenneth E. Melson  
Director