JUDICIAL CONFERENCE PRIVACY SUBCOMMITTEE

CONFERENCE ON PRIVACY AND INTERNET ACCESS TO COURT FILES*

PANEL ONE: GENERAL DISCUSSION ON PRIVACY AND PUBLIC ACCESS TO COURT FILES

OPENING REMARKS
Hon. Reena Raggi**

MODERATOR
Daniel J. Capra***

PANELISTS
Joel Reidenberg¹
Ronald Hedges²
Peter Winn³
Lucy Dalglish⁴
Hon. Cecelia G. Morris⁵
Maeva Marcus⁶

* This Conference was held on April 13, 2010, at Fordham University School of Law. The text of the Conference transcripts has been lightly edited. The terms CACM (Committee on Court Administration and Court Management), and PACER (Public Access to Court Electronic Records), an electronic public access service for United States federal court documents, will be used throughout.

** United States Circuit Judge of the U.S. Court of Appeals for the Second Circuit; Chair, Judicial Conference Privacy Subcommittee.

*** Reed Professor of Law, Fordham University School of Law.

¹. Professor of Law & Director, Center on Law & Information Policy, Fordham University School of Law.

². Former Magistrate Judge for the District of New Jersey.

³. Department of Justice, University of Washington Law School. Mr. Winn is speaking in his personal capacity only and not on behalf of the U.S. Department of Justice.

⁴. Reporters Committee for Freedom of the Press.

⁵. United States Bankruptcy Court Judge, Southern District of New York.

⁶. Professor, George Washington University Law School.
JUDGE RAGGI: Good morning.

Everyone knows that we are here this morning for what is an important part of the work of the Privacy Subcommittee of the Judicial Conference Standing Committee on the Federal Rules.

Just to give you a little background on that work, the federal courts, obviously, are engaged in the public’s business, and so the presumption is that our work, including our files, are open to the public. There are many reasons informing that presumption. Open files are important to the litigants who are involved in the cases before us. Open files are important to the public’s oversight of the courts’ work. Public access is also important to history. There is much that can be learned about a society from the work of its courts; from the concerns that prompt individuals to seek assistance in the courts.

All of these reasons have led the judiciary to presume that our files would be open. But increasingly, there have been concerns voiced about unnecessary disclosures of private information in court files. Some of these are not new. There has always been a concern about information disclosed in court files that could actually facilitate other criminal conduct. Identification information, such as Social Security numbers, that could be used as part of identity theft or information about individuals cooperating with government investigations, who, because they are helping to target individuals involved in crimes, could find themselves targeted by criminals.

There has also been a general concern about whether a high loss of privacy for litigants in the court will prompt people not to use the courts as a means of resolving their disputes. As history teaches us, a society where people do not think they can resolve their disputes in a court is a society where they find some other means to do so, not always positive. So we face these competing concerns of public access and protection of privacy.

The Federal Rules already provide for protection of privacy in many respects. And those are relatively recent rules. Nevertheless, the last decade’s experience with greater public access on the Internet to court files has sharpened our understanding of privacy concerns. So in 2009 or thereabouts, the chairman of the Standing Committee on the Federal Rules, Lee Rosenthal, who I am so pleased is here with us today, started to receive inquiries from members of Congress that seemed to deal with both of the matters I have addressed: public access to the court. Congress is concerned about whether we are going online fast enough and whether our access is broad enough to serve the public. At the same time, Judge Rosenthal has received congressional inquiries about why we are not doing more to protect private material in these publicly available documents.

So in the best traditions of all bureaucracies, a subcommittee was formed to study this matter. This subcommittee is, of course, the one that is here today at Fordham.

We operate as a subcommittee of the Standing Committee on the Federal Rules, but I really have to say that our efforts represent a joint endeavor by both the Standing Committee and the Committee on Court Administration.
and Court Management, CACM. They, of course, have responsibility for policy, and the Standing Committee has responsibility for implementation. I want to say thank you very much to all of my colleagues from CACM for helping us, and most particularly, to the former chairman of that committee, Judge Tunheim, who I am also pleased was able to join us today.

Most of you are here to serve on panels. I want to explain to you how we view your contribution in the overall work of the subcommittee. We broke our work down into two phases. The first I will call statistical. Through the work of the Administrative Office and the Judicial Center, we have been able to crunch lots and lots of numbers to get an idea of what is publicly available, what kind of private information is showing up in court files, and, just from a statistical perspective, how large a problem we have and in what areas.

With the benefit of that information, we are now moving to phase two, which is this conference. The subcommittee decided that it would be most helpful to have the viewpoints of as many different persons in the legal and related-to-law communities about public access and private information. So we have invited you today, civil and criminal lawyers, prosecutors and defense attorneys, academics, judges, and a variety of people who serve the court—who serve the court as clerks of court and in various other support functions—to come and talk to us about your experiences in these areas. I thank you so much, on behalf of the subcommittee, for giving us your time. And I want to remind you of what would be most helpful to us. You are here to educate the committee. Please be frank about what you have seen and where you identify concerns, and do not hesitate to disagree with your fellow panelists. I cannot emphasize enough our view that we need to hear diverse views on how to calibrate the balance between public access and protection of privacy.

All of this effort today is the work of one person, and that is the subcommittee reporter, Daniel Capra, Professor of Law here at Fordham. I thank Dan many, many times for his work for this committee. He also serves, in his spare time, as a reporter for the Evidence Committee and a variety of other tasks. As everyone says, he is a dynamo, and most particularly in the service to the judiciary. So thank you, Dan.

Of course, I also want to thank Fordham University for hosting this and for really giving a lot of thought to what the conference should involve. With that by way of welcome and introduction, let me turn it over to Dan Capra.

PROF. CAPRA: Thank you, Judge. Thank you very much for that excellent introduction, which sets forth basically what we are trying to do today.

I am moderating a panel which we have called the general panel. The subcommittee is considering at least possible changes to the privacy rules. The privacy rules are located in your materials, actually in a couple of places. There were some pamphlets that were given out by the Administrative Office, and behind Joe Cecil’s report is the particular
privacy rules that were enacted in 2005, 5.2 of the Civil Rules, 49.1 of the Criminal Rules, and the like.

The subcommittee, as I say, is considering whether rule amendments are necessary and also is considering a discussion of policy changes, but all within the context of this broader idea that Judge Raggi was talking about: the balance between privacy on the one hand, and open access to court records on the other, in the light of ease of Internet access. So we thought it would be appropriate to kind of set the day with a general panel. By “general,” it does not mean airy and platonic and talking about love and things like that. There will be practical discussions involved as well, but within the context of setting a broader framework.

I need to give my own thanks. First of all, I need to give my thanks to Joe Cecil for all his fine work in terms of the statistics that he has done and all the searches of the records that he has done over the past month. It has been truly amazing. He will talk about that later on today, but since I have the opportunity, I wanted to thank him for his excellent work in that respect. I want to thank Susan Del Monte, who gave me many great recommendations about who to call and who to bring here, especially for the Plea Agreements Panel. I think we have a Plea Agreements Panel that represents all the views that all the districts have been coming up with. I would like to thank Susan for giving me those suggestions.

Allyson Haynes, from the University of Charleston School of Law, I would like to thank because Charleston did a program that covered some of these issues, and she was very helpful in helping me to form ideas for this program.

With that, I am done. I would like to give you over to my colleague, who I am proud to have here on the panel, Professor Joel Reidenberg, Professor of Law at Fordham Law School and Director of the Center on Law and Information Privacy.

PROF. REIDENBERG: Thank you, Dan, thank you, judges. I think it is terrific that you are focusing so carefully on these issues.

My background is as a privacy scholar, not as a civil procedure expert. So my remarks will be focused on some of the broader privacy issues that open access raises.

To set the stage, I would like to focus on a few of the problems associated with too much transparency. We do not often think about publicly held information as giving us too much transparency in our society. But to follow up on some of the comments that Judge Raggi made just a few minutes ago, in the past, when we thought about the openness of public records and particularly about court records that were open to the public, we would find that those records still had an effective privacy protection through practical obscurity. Access to the information was not easy and physical or geographical limitations restricted how widely information in the public records could actually be disseminated or obtained. This made public record information practically obscure.

The Internet and network information flows eliminate that practical obscurity today. We now live in a context with an increasingly and
completely transparent citizen that has, I think, some very significant dimensions. I would like to focus on two points during this short presentation and make a suggestion for a way of approaching the tradeoff between openness and privacy.

The first point is that completely open access has important public safety implications. The Amy Boyer case illustrates this problem. Amy Boyer lived in New Hampshire and was murdered by an ex-boyfriend who, through access to information obtained from an information broker, found out where she lived and worked, stalked her, and shot her at her workplace.7 That same kind of data, locational data, can now easily be gleaned from publicly available court records, if they are online and searchable, and used just as Boyer’s ex-boyfriend used the same data obtained from the information broker. That is one obvious problem.

The less obvious, but very difficult, problem is the de-contextual use of information that would be contained in court filings and court decisions. If information about individuals is extracted from court filings and exploited through data mining or combined with additional information acquired from data brokers, from other public databases or from other publicly available information, the original context is lost and the data mining leads to the development of behavior profiles of individuals, to stereotyping, and to decisions based on what I will call “secretive data processing” because the data mining and profiling is hidden from the individuals. In effect, by making all this information about the citizen so transparent, the public does not really know what happens to their personal information and, ironically, the accuracy of the information describing individuals can be compromised through out-of-context compilations and profiling.

Another obvious consequence of the transparency of personal information is identity theft. The richness of data that is in court filings would be very useful for identity thieves. A criminal can very easily masquerade as someone else if data can be taken from varied sources and combined together to provide enough personal information about the victim.

The second point is that the integrity of the judicial system is challenged. This goes back to the comments that were made earlier in today’s session. Unprecedented wide access and dissemination of everyday court records and proceedings can have an impact on jurors’ willingness to serve and on witness candor. If the personal cost for engaging with the legal system is a perceived loss of privacy because the data is now publicly accessible, freely searchable, and “Google-able” on the Web, the public hesitates or opposes participation in the judicial system. Similarly, parties may be intimidated by the Internet accessibility of personal information related to their participation in a court proceeding. There is a qualitative difference from the days when an observer had to go to a musty courthouse to find the data. People will be reluctant to come to court to vindicate their rights if they perceive that it makes their lives a completely open book.

Lastly, the transparency has an impact on perceptions of judicial integrity. The data mining that might go on with respect to litigants, witnesses, or statements made in a court filing can just as easily occur with respect to the judges themselves and the judges’ personal lives. Many would be surprised at the associations about judges that might be made by data mining information in court cases just from the way judges manage their cases. So these issues suggest that public safety and the integrity of the judicial system are at risk from over-transparency.

As to my suggestion, I would like to focus on the approach to the trade-off between openness and privacy. I know that court systems have focused very carefully on redaction as one potential solution. The redaction model is also used outside the United States, in many foreign jurisdictions, as a way of balancing privacy interests with court oversight. But another model that I would like to recommend as a very worthwhile avenue for the courts to explore is limited-purposes disclosures. This approach makes personal information available publicly, but only for defined purposes. We see this approach in American legislation, specifically the Driver’s Privacy Protection Act. Under the Act, driver’s license information is a public record, but the data cannot be used for purposes other than those enumerated in the statute. The permissible purposes relate to the reasons why the data is public information such as driver authentication, car insurance, recalls, that sort of thing.

I think we need to explore this approach in the court context. The court system should be addressing key questions. Why is the information about these individuals publicly available? What is the reason for the information to be publicly available? What are we trying to accomplish? Can we construct limits on use in ways that are compatible with the public purpose for the information being out there?

I will close with that.

PROF. CAPRA: Thank you, Joel.

I turn now to Ron Hedges, former Magistrate Judge for the District of New Jersey. He worked very hard to get the Sedona Conference to come up with principles on privacy and public access to courts in a civil context. I will also put in a plug that he is an excellent Special Master in the matter of In re REFCO.  

MR. HEDGES: As are you.

PROF. CAPRA: I do not know about excellent, but I am as well. Over to Ron.

MR. HEDGES: Good morning. Thank you for allowing me to be here. I want to spend a few minutes talking with you about how The Sedona

---

Conference\textsuperscript{10} [Sedona] came up with its Best Practices on Public Access and Confidentiality in Civil Litigation.

Sedona works through “Working Groups.” The Best Practices were a product of Working Group 2 [WG2], and I was a member of the editorial team. I think I can tell you, not surprisingly—I expect you are going to hear it today—this was a very contentious process. There were a number of interests involved.

There were a lot of people on WG2 who were very pro-access. There were others representing corporate interests that were concerned about protecting secrets, and the like, that took an opposite view. It took four years to get the Best Practices to the public version that is now available. As I said, the process was contentious throughout.

What we did was to come up with a draft, and we did a series of “town halls” around the country, five or six, inviting different constituencies to come in and comment. It is fair to say that we have a couple of themes that go through everything.

The first theme was a very basic distinction between discovery materials that generally do not see the light of day and that people can protect as much as they want under Rule 26(c)\textsuperscript{11} or the like and materials that are filed in court. We were very much opposed to the concept of confidentiality orders that included an automatic sealing provision such that, if parties exchange discovery materials, they can simply—by filing an affidavit or whatever—seal materials filed with the court. That is a First Amendment violation.

I realize that there has always been a concern that we are driving people out of the system because of transparency issues. We can debate that all day, if we need to do that. But it is fair to say that Sedona came down very much on the idea of open judicial proceedings, including jury selection, openness in settlements, and openness in anything that may be filed with the court. So we have the basic distinction between what goes on between parties and what goes into courts.

We also came out very strongly on the concept of intervention. If there are sealing orders filed, the public or the public is representative, which is often the press, should have an opportunity to come in and challenge these before a judge.

I am happy to say that we have been percolating along for three years now. We are about to go online with another version of a database that accumulates case law that has developed in the last several years, of which there is an enormous amount. I see a trend of the future that we will see a lot more issues created by electronic filings. For example, inadvertently produced materials may be on the Internet that should not have been there and how those materials are brought back.


\textsuperscript{11} FED. R. CIV. P. 26(c).
In a nutshell, that is how The Sedona Conference put together the Best Practices, what the Best Practices are intended to accomplish, and where the Best Practices and WG2 may be in the course of the next several years.

PROF. CAPRA: Thank you, Ron.

Peter Winn has been writing articles in this area for a number of years now. He provided comments on the initial redaction rules that came through. He has written an article dealing with some of the issues that the subcommittee is investigating today. Peter Winn is an attorney for the Department of Justice and Adjunct Professor of Law at the University of Washington Law School. Let me turn it over to Peter.

MR. WINN: Thank you very much.

I got into this business by accident several years ago when one of the local judges in Seattle asked me to write an article about the privacy implications of putting judicial records online.12 Over the next few years, I became less and less happy with the analysis in that article and wrote another that came out last year in the Federal Courts Law Review.13 I am already starting to reconsider some of the arguments in that article.

I keep changing my mind because two things are going on here that are very difficult to reconcile: we want court records and proceedings to be open and transparent, but we also want to make sure that sensitive information in the hands of the courts is protected. Both goals are important. Transparency is necessary for the legitimacy of the system, necessary to maintain a healthy political feedback loop, and necessary for effective public oversight. However, at the same time, courts also have a fundamental responsibility to engage in a truth-finding process. To find the truth, courts need access to sensitive information from the participants in the process—not only the litigants, but jurors and witnesses as well—people who are critical for the fact-finding process to work. Traditionally, these judicial participants have been more or less comfortable disclosing their sensitive information with the understanding it would be used only for purposes of resolving the dispute in the context of the judicial process and would not come back to bite them. When participants start getting burned or hurt after disclosing their sensitive information to the court—when the information is used for other purposes than resolving the dispute—litigants, witnesses, and jurors are going to be less and less inclined to tell the truth in the first place. Thus, to make the system work we need both transparency and privacy.

In the good old days of the paper-based system, we could have our cake and eat it too. We could have both transparency and privacy because of the practical obscurity of paper. Paper records were public, or at least ninety-nine percent of them were public—the ones that were not filed under seal. But paper records were difficult to access, very few people were

ever hurt when sensitive information was filed in the so-called “public” judicial system.

By contrast, electronic information is not practically obscure—it’s very essence is to be easy to access. In this new world of electronic information, we have become increasingly aware, sometimes shockingly aware, of just how complicated and difficult it is to have both a transparent system and a system that protects sensitive information. It was probably just as difficult when people started to use paper in the thirteenth century, but we had 800 years to get used to it.

So where are we in the federal system? I like to think of the federal system as a guinea pig, because it was out there first. That was probably because we did not know any better—the benefits seemed obvious, the costs hidden by the habits of centuries of using practically obscure paper. The state courts have been the next wave and are struggling with the same problems. I have learned much from watching the transition in the federal system, but, in many ways, the state courts have much greater challenges. Juvenile cases, divorce cases, probate cases, all present much more difficult problems than those typically faced in the federal system.

In the federal system, to some extent, we have only jumped halfway into the swimming pool. PACER is still not Google-searchable. It still has a lot of the attributes of practical obscurity, simply because of the difficulty of accessing the electronic information. I think it is almost certain that it is going to be Google-searchable in ten years or sooner. It may be Google-searchable much sooner than that. The law.gov movement, largely under the leadership of Carl Malamud, is already in the process of seeing to it that federal court records are online in a Google-searchable manner.¹⁴ It is just in the nature of electronic information that it will become much more accessible and will raise more and more difficult problems in the context of protecting sensitive information.

So how do we protect sensitive information in courts? There are three basic strategies.

One is not to put the information into the system in the first place. Categories like Social Security numbers, names of minor children, financial account numbers—a lot of times you simply do not need that information in a pleading to start with—

JUDGE MORRIS: Excuse me, let me just interrupt. The word is called bankruptcy.

MR. WINN: Right, bankruptcy.

JUDGE MORRIS: I will get there in a minute.

MR. WINN: I stand corrected. You do need to put quite a lot of sensitive information in a bankruptcy file as a matter of law. So that strategy does not work very well in bankruptcy. And more generally, that

strategy will not work when sensitive information needs to be filed with the court.

A second strategy is to try to put it in the judicial system either under seal, or offline. The 2007 privacy rules permit the use of protective orders to take documents or information offline—similar to how Social Security and immigration cases are routinely handled today. This strategy has not yet widely been adopted by lawyers. Instead, agreed sealing orders are still the norm. However, while reliable to protect sensitive information, agreed sealing orders often fail to meet the required common law and constitutional standard—a standard seldom enforced in the absence of a dispute. As electronic court records become increasingly subject to computerized audits, and as the improper use by attorneys of the agreed sealing order to protect sensitive information becomes subject to greater legal scrutiny, the agreed sealing order, itself, may become a thing of the past. If that happens, using protective orders to take sensitive information offline may become the only practical alternative.

The third idea to protect sensitive information was just raised by Professor Joel Reidenberg. That is, to prevent people from using sensitive information filed in court records for secondary uses unrelated to the administration of justice. A general rule permitting disclosure of certain information in the context of the public court proceeding but prohibiting disclosure of the same information outside the courthouse would probably be unconstitutional. In my article in the *Federal Courts Law Review*, however, I suggested that a more limited set of information management requirements, unrelated to any specific content, and imposed solely on bulk data aggregators might pass constitutional muster. Data aggregators might be required by contract to adhere to certain information management procedures in exchange for the grant of bulk access privileges. Thus, for instance, they might be required to “scrub” their data for inadvertently filed Social Security numbers (as many of them do now anyway). However, with the exception of limited computer “scrubbing” techniques, I have grave doubts that general rules to address the more difficult problem of secondary use of information from court files—for instance, “data mining” judicial information for commercial purposes—will ever be likely either to pass constitutional muster or be very effective as a practical matter at protecting sensitive information. In conclusion, I do not see any obvious, easy, one-size-fits-all solution.

I do have some hope that we will be able to muddle through and find solutions to these problems, but I do not think it will be easy, or that the solutions will be found quickly. We have three basic tools available: rules, training, and technology. I think the rules that the federal courts have developed are reasonably good. I am just not sure that there is much more you can do in the rulemaking process. You cannot have a general rule forbidding the filing of all sensitive information—much of that information must be part of the public court record, and what is sensitive in some

15. See Winn, supra note 13.
contexts is not sensitive in others. The courts have to rely on the parties and their attorneys to identify the sensitive information in their filings and take affirmative steps to protect it. That is pretty much all the rules do now, and pretty much what any rules in the future would ever be able to do.

The more significant area of deficiency—that is, the area where there is most room for improvement—is the need for better training of lawyers. Most of us have developed our intuitions in a paper-based world of practical obscurity. We have taken it for granted that documents filed with the clerk’s office will stay in the court system and will not surprise us with unexpected secondary uses. Many older lawyers still have their secretaries file their pleadings on the PACER system, and lack any real personal knowledge of the system. The younger generation is much more technologically literate, but we can all do with better training. It may not be until our children’s generation is practicing law that lawyers will become better attuned to the problems of handling judicial information properly, given the wider and more open set of possibilities for its secondary use. We, who have been trained in a particular way, will simply have to die and let somebody else take over.

The area with potentially the most promise is the improvement offered by better technology. We can do a much better job facilitating access. Court decisions, briefs ought to be Google-searchable. We can do a much better job than we are doing protecting sensitive information in the process, and technology is an important part of that solution. Professor Edward Felten has highlighted many of these potential solutions. These technological solutions are possible only if lawyers and judges begin to work proactively with computer programmers. We tend to assume that computer technology is a given when we engage in rulemaking or when we plan our CLE programs. It is not. The problems that we fashion rules to try to address, and that we train lawyers to better understand, are in part, creatures of a particular form of technology. The design of that technology can be changed to solve some of these problems. However, these technological changes often spawn new problems, making new rules and training necessary. It is an endless cycle, but that is no reason to give up.

As we struggle with these problems in the federal system, much can be learned from watching our sister courts in the state system navigate these electronic rapids. State courts have much larger dockets, and often manage much more sensitive information than do the federal courts—one need only think of the type of information handled by family courts and in juvenile criminal proceedings to see just how difficult these challenges are. One lesson that appears to have been learned by both the state and the federal courts is the importance of involving as diverse as possible group of interested parties in the development of both the rules and the technology which will be used as courts go online. At the Williamsburg conferences where state and federal court personnel meet to explore different ideas,16

---

there appears to be a consensus that it is critical to get everybody to the table when you are making decisions. The process is similar to that involved in drafting an environmental-impact-statement. When all the affected players are at the table, the conversation can be contentious. However, it makes it more likely you will identify the problems at the front end, when it is still possible to hash out some solutions. Furthermore, it makes it more likely that the proposed solutions you reach will be more likely to work, with greater buy-in by participants in the end. It is nearly impossible to identify the problems of managing sensitive information when you try to think these things through in the abstract. You have to get everybody at the table and explore the problems before you can identify solutions.

Finally, a related point I would like to make is that sensitive information is largely a matter of context. Information is not sensitive simply because it jumps out at us that it needs protection. It all depends. Information can be sensitive in some contexts and not in others. For instance, information excluded by the application of the Rules of Evidence is not sensitive if disclosed to the public; but it is very sensitive if disclosed to the jury. Thus, a motion to suppress can be filed and disclosed to the public subject to the classic judicial oversight concepts. However, if a juror uses the PACER system to learn about the cocaine seized by an illegal government search or a defendant’s prior criminal record—information which may be public and online—we may no longer be able to provide the defendant a fair trial, consistent with fundamental notions of due process.

In the eighteenth century, Jeremy Bentham argued against the exclusionary rules of evidence, arguing that jurors should be trusted to make decisions after hearing all the facts. As electronic information becomes more and more difficult to control, we may be forced to adopt Bentham’s view of the exclusionary rules. However, I believe and hope that we all can focus on this problem and get a handle on it. I think we have to get a handle on it. But I really do not have any obvious, easy solutions about how to do it, other than to try to muddle through, and continue to work together.

Thank you.

PROF. CAPRA: Thanks, Peter.

Our next speaker is Lucy Dalglish, Executive Director of the Reporters Committee for Freedom of the Press.

MS. DALGLISH: Thank you. Good morning. It is nice to be here.

The Reporters Committee, for those of you who do not know, is a legal defense and advocacy organization based in Washington, D.C. We have been around for forty years. We help journalists defend themselves when they are in trouble and gain access to all sorts of state and federal records and proceedings. I have one entire program area, run by a super-fellow, an

17. See Jeremy Bentham, Rationale of Judicial Evidence 15–16 (1827).
experienced litigator who has spent a year with us, and they are focused solely in the area of secret courts and prior restraints. This is of great interest to me. I am a former journalist and a former litigator. All of my lawyers are former reporters.

I need you to understand a little bit about the landscape that journalism is operating in right now. Whereas all of the rest of you are probably going, “Oh, my God, the Internet. Everything’s available,” reporters are going, “Oh, my God, the Internet. Everything’s available. Suddenly I might actually be able to do my job effectively.”

We are in a situation where there are a lot fewer journalists in mainstream news organizations. By having easy access to this information, they are able to do a better job of reporting the news to the public. There are some jurisdictions—probably not Manhattan, but certainly in places like Utah—where you have many local newspapers and really only one federal court that covers an enormous geographic area. Now they are able to accurately and completely report news stories as well. We view the PACER system as miraculous. It by and large works very, very well. I work on cases all across the country, and I love it, because I no longer have to rely on a local lawyer to go and dig out some information about a case I have heard about.

There are, as I said, fewer reporters. Many of them who were able to support a family on a journalism income in the past are no longer able to do that, so you have a lot more independent journalists. Money is an obstacle to PACER. A lot of them just cannot even afford to use it anymore.

I want to break my comments, very briefly, down into several categories. One, I would like to talk about the identifiers issue. I would like to talk briefly about plea agreements. I would like to talk very briefly about settlement agreements, the trend toward anonymous juries, and then the most important problem of all, which really was not even on the agenda, the issue of disappearing cases in the federal docket system.

First of all, identifier issues. I was one of the folks who testified back in 2002 or when you came up with the first rules. By and large, I think the redaction system that you have implemented that allows the last four digits of bank account numbers and Social Security numbers works fairly well. It does not cause a lot of phone calls from reporters. They are not all that concerned about it.

One thing that is a problem, however, is the birth date issue. Reporters’ issues have to do almost exclusively with making sure they have the right person. I come from the land of Johnsons, Anderssons, Sorensons, and Carlsons. And there are not just hundreds of them; there are thousands of them. You need to make sure that you have the right John Anderson. Reporters do not want to identify the wrong John Anderson as a criminal. They want to be accurate. Often the best way to ensure you have the right John Anderson is to know the birth date of the person who has been charged with a crime. Perhaps even worse than having personal identifying information released about someone actually involved in a court case is when information is released and everybody thinks it is about the wrong
guy. That is a real problem, and the more information you can provide, particularly a birth date, helps reporters identify the right person.

If you do not need all the rest of this stuff—I understand bankruptcy is an exception—if you do not need it, why are you collecting it? I think you really need to think very carefully about the identifying information that you do collect in the federal court files.

Plea agreements are something that reporters traditionally have relied upon—not every day, but sometimes there is very useful information that appears in those cases. It is helpful to flesh out a story, to identify trends. Lately, with the reporters who are calling me and asking me, “Why can’t I get this plea agreement information?” it has to do with business cases, where they are trying to figure out who in Enron or who in whatever other criminal economic case they have is talking to whom. That information is very useful.

One of the problems that I hear is from reporters who work for the national publications and national broadcast stations. You guys have rules that are different all over the country. I have one summer intern coming in this summer who is going to work on just keeping track of what the feds are doing with plea agreements, because we need to be able to tell reporters what they can get and what they cannot get in each district.

There is, in my mind, an appalling trend toward completely anonymous juries in the federal system and the state system as well. I understand that we are asking people to give up a lot when they become a juror. But you know what? That is something that, when you are an American citizen, you just sign up for. We have a responsibility to serve on juries. I think the notion that you cannot find out who jurors are in the federal system, unless you are really, really lucky or you file requests for it months and months after a case is resolved or you are lucky enough to sit through a trial, to find out who is sitting on that jury panel—I think it is appalling. I think a criminal defendant is entitled to a fair trial, and part of that is having the ability for the public to know whether or not the people who were empanelled on that jury should have been empanelled on that jury.

The best case I can think of about this—and it was not a federal case, but I think it illustrates my point—there was a murder case being tried in New Jersey. It resulted in a mistrial. *The Philadelphia Inquirer* did a story about what was going on in this entire case. They were the ones that figured out that the jury foreman did not even live in New Jersey. She was from Pennsylvania. She had apparently had a car licensed in New Jersey. She got elected to be the jury foreman in this murder trial. That is just appalling. And it was a reporter who figured that out.

When you came up with the electronic court access rules, this completely slipped right by us. It was not until probably six months afterwards that reporters were calling saying, “What is going on? All of a sudden we

---

cannot find out who is sitting on a federal jury unless we are actually sitting there and we might overhear a name.”

It turned out that this was part of the electronic access rules that completely slipped by us. You would have heard from us if I had been paying better attention way back when.

Settlement agreements—I think Ron is going to talk more about all of this. There is some very important information that can be accessed. It is of great public benefit. Probably the best example—and perhaps Dave McCraw can talk about this a little bit more from The New York Times Company standpoint—The Boston Globe—again, I think these were mostly state court cases—found out a great deal of information from their Pulitzer Prize-winning stories on priest abuse in the Archdiocese of Boston. Most of that information came after they were able to go back twenty, thirty, forty years and get a lot of those settlement agreements unsealed. I think when the safety of children is involved, there is no reason whatsoever why all of these things need to be sealed. It is a public safety issue.

Finally, the secret docket cases. I never in a million years would have thought this would be possible. We have a system of open courts in this country. I understand that in certain circumstances when you are conducting a criminal investigation and you have not completed all of the indictments in your case that you are trying to present and you are trying to get all your ducks in a row and get people charged in the right order, maybe it has to be temporarily sealed. But right now, as far as I can tell, there is not a single district in this country who has figured out how to reopen those completely secret cases once they have been closed.

What usually happens is a U.S. Attorney will come in and say, “We just caught this really bad guy,” and you will go in and try to find the case—this is not in every district, but in a fair number of them—and it does not exist. You go to the clerk of court and they say, “We cannot open it unless we have a court order.” You go to the judge and he says, “I cannot unseal it unless the U.S. Attorney tells me I can.” And you go to the U.S. Attorney and they say, “Well, that is a problem that the judge is supposed to come up with.”

Meanwhile, at one point several years ago, we found thousands of cases in the federal system where docket numbers were just missing. Now, I know the Judicial Conference has attempted to address this issue, but it has not been fixed yet.

My very last point is on the civil side. There was a case we got involved in about a year ago, involving a federal civil case that was conducted entirely in secret in Pennsylvania for seven years. It was a situation where a woman brought a claim under the federal anti-pregnancy discrimination law. She sued her former employer, who, she contended, fired her

---

because she had an abortion. This thing was litigated for seven years. The only way we found out about it was when it was appealed to the Third Circuit and the Third Circuit decision was released and the local legal newspaper said, “What is this?” They went back to get the documents, and the entire case was sealed.

That is just plain not right.

PROF. CAPRA: Thanks, Lucy.

I will say there are people in this room who are on the case of some of the issues that Lucy was dealing with, particularly disappearing docket numbers, entirely sealed cases. That report, to my understanding, is forthcoming.

So there has been significant work done on that. The Privacy Subcommittee and the Sealing Subcommittee have been kind of working in tandem on these issues, because the issues do tend to overlap in some respects.

But thanks for bringing that up. That is an issue that the Judicial Conference is working on.

You have already heard the fact that some of these issues are much more difficult in bankruptcy than anywhere else. We will see when Joe Cecil presents his data that many of the unredacted Social Security numbers that have been found in the two-month search that Joe did were in bankruptcy proceedings. So we thought it appropriate in terms of setting the table for the rest of the day to bring in an expert on these matters. That is Judge Cecelia Morris, who is from the Southern District of New York Bankruptcy Court and also served as the clerk of that court for many years.

I turn the floor over to Judge Morris.

JUDGE MORRIS: Okay, everybody, get a pen and paper out right now and number from one to five. I am serious. Do it. I was given this idea by Karen Gross, the president of Southern Vermont College since 2006.

I want you to write down five entities that you owe money to. Do it. This is a serious test. Besides writing down who you owe money to, write down how much you owe them. And do not tell me you do not have any debt. If you have a phone in your pocket, you have debt, because they give it to you on credit. They give you electricity on credit. So you have debt.

While you are doing this, I want your full name, every name you have been known under, and your Social Security number. Your monthly mortgage payments, your cable bill, your insurance premiums. Keep writing. I see people not writing.

I want the ages of your minor children. Are you getting there?

Now, beginning right here, I want you to come up to this podium and read everything you have just written to this room.

That is how it feels to file bankruptcy.

Privacy is important. Last year the consumer cases skyrocketed, and 1.3 million entities filed bankruptcy, most of those filings were individuals that had to do exactly what you did. And, by the way, we are putting it on the Internet.
MS. DALGLISH: Full Social Security numbers are going on the Internet?

JUDGE MORRIS: No, full Social Security numbers are no longer going on the Internet. But that is what you are doing, and we are sending your full Social Security numbers to your creditors. They are not going on the Internet.

By the way, we are also putting this information on PACER at an incredibly low price. The idea that you cannot afford to go on PACER at how much a page? That is sort of beyond me.

There is a difference here also between the number of cases filed in federal district court of about 300,000 and the 1.3 million cases filed in bankruptcy courts. Bankruptcy, as we have already heard, more than any other area of law, has a pronounced dichotomy between the debtor’s privacy rights and the rights of creditors and the public to this information.

Section 107 of the Bankruptcy Code states that information filed in the bankruptcy court is “public records and open to examination by an entity at reasonable times without charge.” That is what it says.

The press may want the birth date. My financial world wants my Social Security number. In 1995, when CM/ECF went live, I did not even know my Social Security number. Why did I not know it? I did not have to have it for every credit card, for every financial transaction. Today it is memorized. Why? Because it is part of every financial transaction.

So I am filing bankruptcy. What do I need? I need my name, address, birth date, familial situation. Am I married? How many kids do I have? What are their ages? Employer, current income, assets, including real property, jewelry, household goods, liabilities, current rent, mortgage payment, taxes, club fees, medical expenses, tuition payments, charitable donations, creditors, judgment, liens, leases, security deposits, IRAs, and all other retirement accounts. Each of those entities that I owe money to needs correct information in order to prosecute their claim. Your credit life is now tracked through your Social Security number.

The bankruptcy electronic filing system is vital to the practitioners, the creditors, the judges that participate in the bankruptcy system. It also greatly expands the number of individuals who can easily access the information. The debtor and the creditors and the public all benefit from the thorough disclosure of information. My name is Cecelia Morris. I do not want to be confused with the Cecelia Morris that filed bankruptcy in Brooklyn. It is similar in this way to the no-fly list that unless you have another identifier to distinguish Cecelia Morris in Poughkeepsie and Cecelia Morris in Brooklyn, it would mess up my credit report.

In response to privacy concerns, we have all heard about the December 2003 rules that allow only the disclosure of the last four digits of a Social Security number on the publicly available bankruptcy petition. You still

23. CM/ECF (Case Management/Electronic Case Files) is the case management and electronic case files system for most United States federal courts.
have to file the Social Security number, because your creditors are entitled to the full Social Security number. It is only the public information and the public docket that redacts everything except the last four digits. Again, you want to make sure the right parties and interests have the right notice, the proper notice, and are necessarily at the meeting of creditors.

When I described to you about coming up here and talking, that is the meeting of creditors. The meeting of creditors is run by a trustee. “Raise your right hand. Do you solemnly swear that everything you have told me on this petition is true and correct? Does anyone have a question?”

Under this new system, most of the account numbers are redacted, including bank accounts, credit cards, loans. When a case is filed pro se, the court makes every effort to protect private information since pro se debtors will often fail to redact confidential information. There is good quality control in the bankruptcy court clerk’s office. There is really very good quality control on the petition filed by attorneys. The lawyers know how to do it. It gets done. The pro ses hand it in physically—remember, the electronic case filing system in the bankruptcy court is made for lawyers. It is not made for pro ses. Pro ses still have to come to the court.

The last thing that happened to me in the courtroom that was just blatant was when a lawyer had filed a petition with the wrong Social Security number and, in filing with the wrong Social Security number, she then filed a motion that said that was the wrong Social Security number and this is the correct one. The motion had the full Social Security number. Needless to say, she was chastised in court. She also fired a staffer. I am sure that was not the only thing the staffer had done, but that incident underscores the importance of maintaining a high level of discipline when it comes to redacting information.

Now let’s talk about creditors.

Everybody is familiar with the Bernie Madoff case. Does anyone in the room not know about Bernie Madoff and the Ponzi scheme? Guess what happened? All of the proofs of claims have attachments. What did they do with the attachments, these creditors? They scanned those—Social Security numbers, home addresses, investment account numbers. Some of these people are worth a lot of money. With their Social Security numbers, you can go down to the bankruptcy court or sit at home on your computer, and you can find out a lot of information.

If I had to identify the greatest source of unredacted information, I would point to proofs of claims filed by pro se creditors. Not all creditors are large banks with legal counsel; many creditors are small businesses or individuals who will attempt to fill out a proof of claim themselves. As in the Madoff case, they will attach all sorts of identifying information about both the debtor and themselves. Compounding this problem is that these proofs of claim, unlike the bankruptcy petition itself, is not quality controlled by the bankruptcy clerk’s office.

With respect to pro se debtors and pro se creditors, it is clear that they do not know why it is so important to redact identifying information. The court and the official forms may be able to do a better job at clarifying why
things need to be redacted, to prevent identity theft, and how to redact information, block it out. Clear, unequivocal instructions such as, “Do not give us your full Social Security Number in this proof of claim.”

PROF. CAPRA: Thank you, Judge.

As Judge Raggi pointed out in her introduction, a historical kind of framework for this is going to be very valuable for the committee. We could not get anybody better on that particular task than Professor Maeva Marcus. I would like to turn it over to her. She is a Research Professor of Law and Director of the Institute for Constitutional History at George Washington University Law School.

PROF. MARCUS: Thank you.

After reading the summaries of what will be discussed today, and after hearing my fellow panelists, I realize that historians’ concerns are somewhat different from the problems on the conference agenda. We take the long view: we want court papers to be saved exactly as they were filed and to be accessible in the future, because they are a fruitful source for all kinds of historical research. Since the beginning of the national government in 1789, the operations of the federal judiciary have played a significant role in the development of the nation, and no one today can anticipate what particular topic will be of interest to scholars in the coming decades. It is impossible to determine what will be relevant and important to the questions that will be studied fifty or a hundred years from now. Historians, therefore, do not want records to be changed in any way or destroyed.

They also do not want records to be sealed. I do not have firsthand experience with case papers that have been sealed. I do know, however, that papers are sealed too frequently, and litigation has ensued. If these papers are not eventually opened, who knows what will have been lost to history. Historians would urge the privacy subcommittee to devote the time and energy to finding technological solutions to practical problems like the redacting of information that would identify individuals or making voir dire transcripts public, so that scholars can have access to as many court papers as possible in the future. I understand that there are instances in which sealing the record, or part of it, is the only feasible solution at the moment. I would encourage the subcommittee to consider time limits for sealed papers.

Time limits have been used in a variety of situations where privacy is a concern. Judges who leave their papers to public repositories, for example, often provide in the deeds of gift that the collections cannot be used for a specified length of time. We assume, especially when the time limit is stated as “after all judges who served with the subject have left the bench,” that the concern is to spare embarrassment for the judge’s colleagues. But often a judge’s papers contain items such as information about litigants that raise privacy concerns. Historians sometimes find copies of court filings in these collections, and these papers do not necessarily have the redactions that you find in the official copies of the documents. And this is a good thing for us. The very items of information that are redacted are often
useful to scholarly studies. While the judge and parties might not want this information disseminated at the time the case is being considered by the court, we would like it to be preserved. Historians believe that primary sources should be kept just as they originated. No changes should be made by another hand. If a time limit is imposed on sealed court records or redactions, I think that privacy concerns would dissipate.

As illustration of historians’ need for unadulterated court papers, I can point to a number of very important books whose authors have used federal court records as their primary sources. Most of these concern courts in the eighteenth and nineteenth centuries. Mary K. Bonsteel Tachau produced the only monograph dealing with a federal district court in the 1790s, an in-depth study of the court in Kentucky that served by law as both district and circuit court.24 My own work on The Documentary History of the Supreme Court of the United States25 required many visits to regional archives to find the lower federal court records that would reveal how and why the case was brought to the Supreme Court.

For the nineteenth century, Christian Fritz’s book, Federal Justice in California: The Court of Ogden Hoffman, 1851–1891, is a perfect example.26 This monograph illustrates a new trend in judicial history. Formerly, and still today to a large extent, our conclusions about the role of courts and judges in our society were based on appellate opinions. But a thorough study of a particular district court provides a view of the operation of law that had not been available to us previously. We learn about all kinds of judicial business that did not eventuate in appellate court decisions. The great variety of litigation, the people involved in it—and the trial court involves the largest number of people in the federal system—all inform the legal, economic, and social history of the period being studied. For an accurate picture to be drawn, records cannot be tampered with. Nothing has been removed from the eighteenth and nineteenth century records used in these works. If information is removed from twenty-first century court records, historians will not be able to produce equally valid studies.

Some authors who have tackled twentieth century topics that required research in federal court records have found the court records useful but had to supply information that had been redacted from them. Often, this information was found in copies of these court documents in private collections. Examples include Allen Weinstein’s book, Perjury: The Hiss-Chambers Case27 and Stanley Kutler’s work, The American Inquisition: Justice and Injustice in the Cold War.28

Writing history has changed a little bit in the twenty-first century. For example, a book on *Bush v. Gore* came out sooner than it would have in the twentieth century, because all the Florida court records were on the Internet, and the author was able to do research in those records quickly.

I have addressed myself to the privacy concerns with which this conference is concerned. Let me just say in conclusion that there is a larger question in the minds of historians, and that is the condition of the permanent records and where they will be found in the future. Everyone seems to be talking about instant access online. Will the courts continue to administer the electronic database or will electronic records be turned over to the National Archives, as the law requires?

The records of federal executive agencies—and lower federal courts are treated as agencies by the statute—are to be turned over to the National Archives, and it is the National Archives’ responsibility to decide which records should be kept permanently. When space for paper records was an issue, there were fights over the destruction of records by the National Archives, and court records often were involved.

About thirty years ago, for example, the National Archives decided to keep all bankruptcy records from the nineteenth century but to destroy a large portion of the twentieth century records because there were too many of them. In the early 1980s, Chief Judge of the Northern District of California Robert Peckham and a group of historians began a campaign to encourage the National Archives to rescind its decision. They were partially successful. The Archives agreed with the historians on a sampling plan that would preserve a sufficient number of twentieth century bankruptcy records to enable economic, social, and historical analyses to proceed. But I gather that this sampling may not yet be in place.

A similar problem has befallen the records of other federal courts. The National Archives put on hold its most recent records schedule, because of opposition to the plan to destroy a large number of court records. The Archives agreed to do an assessment, but that has not been completed.

Historians face many obstacles to using court records in their research. Even before the advent of electronic records, courts were derelict in sending their papers to the Archives. We expect to find court records in regional archives, but often they just are not there. Working in the 1980s, David Frederick, who wrote a history of the Ninth Circuit from 1891 to 1941, found no records in the Archives but, after searching the courthouse, found some relevant material in the clerk’s office. When I was working on my *Steel Seizure* book in the 1970s, I, too, looked for records at the Archives but ended up finding them at the D.C. courthouse where the steel companies filed suit. When you are lucky enough to find that a court

---

actually has sent its records to the regional archives, you are faced with a warehouse of records and no good way to search for exactly what you would like to see. Electronic records represent an advance, because they, at least, are searchable. Are they permanent, however? And historians have found that the National Archives’ own database is difficult to use and behind the times, so sending records there may not be the best thing for historians, though the law has not changed.

PROF. CAPRA: Thank you.

First, I want to ask Ron Hedges about the sealing issues. Just being involved anecdotally in cases, I see that it is kind of automatic that lawyers file things under seal. Is there something that needs to be done about this?

MR. HEDGES: I do not think it is automatic that lawyers file things under seal. I think it is automatic that lawyers sign protective orders that have provisions in them that really govern discovery, and some place in that protective order there is a sealing provision.

PROF. CAPRA: But in 

REFCO,32 we had filings just filed under seal automatically, when they did not have any confidential information in them that we could see. Does that happen routinely, in people’s experience?

MR. HEDGES: I think, depending on the nature of the litigation, yes. I supervised a lot of IP litigation, and it is common in patent litigation and the like to want to protect information because someone thinks there is a commercial secret somewhere that cannot see the light of day. The fact of the matter is, there are not many things in civil litigation that need to be filed under seal.

PROF. CAPRA: On the issue of anonymous juries, I do not know, Lucy, what the reference was to the electronic access stuff that you let go by, but there is nothing in the rules that I know about that deals with anonymous juries—in the privacy rules.

MS. DALGLISH: My understanding is, it says, while the case is pending, you cannot get it, and afterwards you can go back and make an application. Then, when the entire case is concluded somewhere down the line, you might be able to go back and do it.

PROF. CAPRA: That is not one of the Judicial Conference’s rules, in my understanding. Is it?

MS. DALGLISH: I was told that it happened at the same time as the electronic court access rules.

PROF. CAPRA: I just think that it is a case-by-case approach. Am I wrong, Judge?

MS. DALGLISH: No, it is not case-by-case.

PROF. CAPRA: In terms of what CACM has on this, is there anything on anonymous juries?

MS. DALGLISH: In other words, if I am a reporter, I can go to any federal court in the country while the jury is being selected and they have

---

just been empanelled, and I can go to the clerk of court’s office and say, “Can you tell me the names of the individuals on this jury?” I am not aware of a single U.S. district court in this country that would let you have it while the case is going on.

PROF. CAPRA: I am just inquiring as to where this doctrine comes from. Judge Huff wants to speak.

JUDGE HUFF: Isn’t there a ninety-day hold on filing transcripts to permit the redaction process to occur?

JUDGE TUNHEIM: There is, and transcripts of juror voir dire are generally set aside separately.

PROF. CAPRA: This is not an anonymous jury rule per se. We are talking, really, about the transcripts, which leads us to the panel.

MS. DALGLISH: If you go and listen in court and attempt to catch their name, you can hear their name. If you have missed jury selection and you want to go in to the clerk’s office and say, “Can I have a list of the folks who were empanelled?” they will tell you no. I am telling you, this is going on all over the country. I get about three phone calls a month.

JUDGE TUNHEIM: I am not aware of any rule or policy that affects that. You are probably right. In most instances, it depends on what the clerk’s office will turn over to you. I think technically that should be available. But it is not the subject of any rule or policy that I am aware of.

PROF. CAPRA: Mr. Hedges?

MR. HEDGES: The big debate going on these days now is in large trials, where there are extensive juror voir dires being done and there are pre-questionnaires being sent out. A question that courts are facing is whether or not those questionnaires are things that should be available, especially now that a number are being offered electronically.

The anonymous juries that I have seen are really ad hoc events because of concerns, generally, about organized crime. The last time the Second Circuit really had a fight about that was the Martha Stewart trial four or five years ago.

PROF. CAPRA: In which the Second Circuit said that the judge had acted too broadly.

MR. HEDGES: That is right.

JUDGE RAGGI: I am sure we are going to discuss this more. I think what you are talking about is what judges would not consider to be an anonymous jury.

MS. DALGLISH: You are right. I misspoke.

JUDGE RAGGI: Just so we are all talking about the same thing. Because, as you yourself pointed out, the profession of journalism has changed so much. A person who comes to the clerk’s office and says, “Could I have the names and addresses of the jury?” could be looking to do investigative reporting or could be up to mischief. No clerk is probably just going to turn it over without making sure the judge wants it. So in the end, that query is going to probably go to a judge, and then you are going to talk
to a judge about why you want it and whether he is going to give it to you or not.

PROF. CAPRA: Thank you.

I want to give Professor Reidenberg a chance to kind of sum up on this issue of limited usage. Then we will close and get to the next panel.

PROF. REIDENBERG: Thanks, Dan.

I think it is really a question of thinking about the disclosure and the uses that we associate with public access to the courts as really being part of our political checks and balances. What are some of the uses? Oversight of court fairness, oversight of court administration, uses connected with the litigation—that is the bankruptcy case.

But now, when we talk about secrecy of the identity of jurors during a trial and the points you just raised, we get into other areas where we must be far more careful. Is it okay, for example, that someone wants the names and addresses of jurors who are sitting on the jury because they want to sell them a particular cell phone service? Suppose the cell company’s marketers discover that jurors, while they are sitting on juries, tend to be more susceptible to advertisements for text plans. Is that the kind of world that we want to see? I am very unsympathetic toward those types of releases.

What about someone who wants to gain access to information from probate records to create lists for a dating service of widows and widowers who happen to be wealthy?

If we start seeing too much secondary use or out of context use, if we start putting voir dire questionnaires in real time, online, in ways that are searchable from Bing, what will be the effect on the willingness of our citizens to participate in our legal system?

PROF. CAPRA: Is the technology available to limit that kind of motivational use?

PROF. REIDENBERG: Yes. We can build the architectures. But, we also need to build a legal structure that has some kind of sanction for the non-permissible uses.