COMMISSION ON PUBLIC ACCESS TO

COURT RECORDS

PUBLIC HEARING

HELD: MAY 30, 2003

42 West 44th Street

New York, NY

RACHEL SIMONE, CSR, RMR, CRR

DONNA EVANS

OFFICIAL COURT REPORTERS

Proceedings

MR. ABRAMS: Good afternoon. I am Floyd Abrams. I have the honor to share the New York Commission on Public Access to court records.

With me today -- and those who will be with me today -- are a number of members of this Commission including Stephanie Abrutyn, Elizabeth Bryson, Hugh Campbell, William Farley, Thomas Gleason, Norman Goodman, distinguished Clerk of New York County, Richard Griffin, Pamela Jones Harbour, Maria Imperial, Victor Kovner, Joseph Lelyveld, Charles Sims, and Gary Spivey.

Chief Judge Judith Kaye empaneled this Commission last year to advise the New York State Court System on a difficult and vexing issue that arises out of the technological advances of recent years. Judicial records are, as a general proposition, public. Indeed, as a general matter of federal and state constitutional law, they must be public. What Justice William O. Douglass said 56 years ago remains true today, that a trial is a public event. What transpires in the courtroom is a public event. And the same is true of most but not all court records.

The new advances in technology, the Internet in particular, now make it easier to disseminate public information far easier than ever before. But the

glories, the benefits of the Internet, the ease of availability of information, the 24/7 availability of information, the unconstrained nature of who may receive the information also may raise potential problems. Can there be too much availability of public records? Should Internet access in particular lead us to take a second look to take care about what finds its way into public judicial records in the first place?

Announcing the formation of this Commission, Judge Kaye put our tasks this way. She said: "In keeping with society's increasing reliance on technology, the court system will begin to make case files available electronically within the next few years. But while providing greater access to this information, we must also be diligent to protect the litigants' right to privacy. We recognize that court records can contain sensitive information such as social security and home telephone numbers, tax returns, medical reports and even signatures. I have charged this Commission with the hard task of examining any potential pitfalls, weighing the demands of both open access and individual confidentiality and making recommendations as to the manner in which we should proceed."

Judge Kaye's formulation makes it clear that

the important questions that this panel has been asked to address are not easily answered. The purpose of today's hearing, of the hearing that preceded today in Albany a few weeks ago, and the hearing which will take place in Buffalo a few weeks from today will be to receive and consider the views of interested individuals and organizations from around the state; and given the prominence of New York State, from around the country. A transcript of all three hearings will be made available on the Commission's website.

The notice for these hearings set forth several questions that go to the heart of this Commission's mandate:

1) In light of the recognized public interest that is served by having court case records available for public information, are there any privacy concerns that should limit public access to those records on the Internet?

2) Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the Internet by the Unified Court System? For example, are there particular privacy concerns that outweigh open access considerations regarding the disclosure on the Internet of an individual's social security identification

number, credit card information, bank or investment account numbers, or other personal identifying information?

3) If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic Internet availability?

4) If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys, and by others?

5) Should the public be charged a fee to access court case records on the Internet?

6) What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or litigants, or should searches be available by topical inquiry or statutory reference?

We are looking forward to hearing from our speakers and witnesses today. We have asked each of you to speak to us for a time period of between five to a maximum of ten minutes; or, if you wish, no minutes at all in circumstances in which they have given us copies of their testimony already. We will then address questions directly to them.

I conclude by saying that there are examples of records that are not publicly available under New York State law without a court order making them so; and they are, therefore, not within the ken of this Commission. If material is not public already, we are not here to sit to decide that they should be made public. One may, of course, argue about those things, but it is just not what this Commission is doing.

Those records include records in matrimonial matters, child custody proceedings, pre-sentencing reports and memoranda in criminal cases, documents containing HIV-related information or the identity of victims of sexual offenses and other documents that are filed under seal under New York law. As I have said, our mandate is not to revisit the law and policies that provide for confidential treatment of those materials.

We will now turn to our witnesses. I would ask each witness whether or not the person has provided us with a copy of his or her testimony to first when they speak identify themselves and their organization, if they speak for an organization. And we ask first Elisa Velazques to speak.

MS. VELAZQUES: Thank you.

I am Elisa Velazques, and I am legislative counsel for the New York State Trial Lawyers

Association.

Good afternoon, and thank you, members of the Commission, for the invitation to come and address you on the very important issue of making information contained in court records more accessible to the public through the use of enhanced technology or the Internet. The New York State Trial Lawyers Association applauds the efforts of this Commission to listen to all the different voices and concerns regarding the challenges that you face.

Technology changes every day, and advances that have been made in recent years have completely transformed the dynamics between government agencies and the public they serve. The Internet has made the workings of government far more accessible to the public and has liberalized information-sharing so individuals can more fully participate in government and their community.

As mentioned by the Chair, historically, judicial proceedings have always been open and subject to public scrutiny. Judicial proceedings contained in court records are legally a matter of public record, so enhancing access to records by making them available electronically can certainly provide a convenient way for individuals to monitor the court system and ensure

the fairness in the quality of its operations. In addition, greater reliance on technological advances and on the Internet can help courts manage the increase in their case loads and streamline their process for filing motions and pleadings and papers and the like.

However, the personally identifiable and often sensitive information contained within judicial proceedings, while legally a matter of public record, has always been practically obscure and somewhat of a challenge for an individual to obtain. In order to get this information, a member of the public would have to know the name or index number or some kind of identifying information about the case, and must then physically go to the courthouse where the case is filed, find the file room, fill out a petition or fill out a form to petition the file, wait in line to turn in the form, wait for a clerk to locate the file, wait for yet another clerk, you know, to bring the file over, find a place to review the file, and then finally find a working copy machine to make copies of whatever it is that they want. As arcane and cumbersome of a process as this might seem, it does actually act as an institutional safeguard because it requires a highly-motivated individual to complete this process which actually reduces the universe of individuals who

have access to the information.

But with the advent of the Internet, this information is now -- is now available through a keystroke to anybody who has access to a computer, and it is clear that such unfettered access to personal or confidential information was not foreseen and it could have serious and unintended consequences.

Also, it is questionable as to whether unrestricted access to personal and often sensitive information contained in the court file is in the public interest or is sound public policy. Protecting the integrity of the confidentiality of this personal information or making the court system as accessible to the public as possible is the challenge that you face on this Commission.

The ability of information contained within judicial proceedings on the information highway varies from state to state and from court to court. Some states or jurisdictions utilize statewide searchable databases. Some require the user to have a case number or name in order to search an existing database. Some states provide access to criminal and civil records restricting user access to records that contain sensitive personal information. Some states offer free comprehensive access to court records while others

charge a fee for online access. Within the same state one judicial district or jurisdiction may make judicial proceedings available online while yet others might not. Some examples are:

California has adopted statewide rules that allow for widespread electronic access to civil trial records while limiting electronic access to criminal records and various cases that contain personally identifiable information.

Colorado has a website that allows you to search open and closed cases, but sealed cases as well as probate mental health and juvenile records are not available to the public on the site.

Hawaii has an online access system that allows users to search for case information by case number or case name, and sealed records are confidential information and are not available online.

There are states that don't make their court records as a whole available online; Idaho and Maine. They offer information about index numbers, administrative orders, and they offer court opinions.

In New Jersey Supreme, Appellate and Tax Court opinions are available online and there is a searchable electronic civil motions calendar. However, in New Jersey, the judiciary has decided not to expand

access to court records due to budgetary constraints and the concern that making court records available online would violate privacy rights guaranteed by the Constitution and other statutes.

The struggle to help states balance competing -- the competing right to privacy and right to access interest has resulted in several national groups including the State Justice Institute, the National Center for State Courts, and the Justice Management Institute to come together and develop guidelines for public access to state court records. These guidelines are for comprehensive framework that can be referenced and used by this Commission along with similar commissions in other states examining this issue.

In developing either a statewide policy and standards for public access to court records via the Internet, the fundamental objectives of these guidelines -- and I am not sure if the Commission is familiar with them -- is to maximize public access to court records without compromising an individual's right to privacy or creating a risk of injury to individuals or businesses. The guidelines provide for access in a manner that maximizes the availability of court records, promotes government accountability,

supports the role of the judiciary as the arbiter of disputes, and contributes to public safety, but it is in a way that also minimizes a risk of injury to a individual or business and that protects individual privacy rights and interests and protects proprietary business information.

They make recommendations for the definition of key terms. They lay out general access rules and exceptions. They discuss, question, prohibit public access information in court records or obtain access to restricted information. And they discuss the obligation of vendors providing information technology support to a Court to maintain court records --

MR. ABRAMS: Your time is about up.

MS. VELAZQUES: I will go quickly.

These are the issues that are kicked around. And as plaintiffs attorneys and advocates for individuals who have been harmed --

MR. ABRAMS: I will let you speak a little slower. I will not cut you off.

MS. VELAZQUES: Okay. Thank you.

There is a great interest in having information contained in court records readily accessible online. It can save money and time. It can help to defray research costs and online access to

records. It also enhances an attorney's ability to get valuable and difficult enough to obtain information about a particular government agency or large corporate defendant. However, as advocates for our clients, plaintiffs' attorneys also see the great danger in having personal, sensitive or confidential information available at a keystroke.

For example, a Bill of Particulars routinely contains highly personal and identifiable information regarding the plaintiff's injuries, medical history, work history, financial status. While a Bill of Particulars is filed with the Court and with the court clerk and is part of the public court record, it is a completely different issue if this highly sensitive pleading can be accessed by anybody with a computer. For obvious reasons of safety and security, neither individual nor business clients nor their attorneys would want this information readily accessible for public consumption.

In addition, the electronic availability or the extent of the electronic availability of certain information contained within court records is also dependent on other statutory requirements that affect civil practice.

For example, the Department of Health and

Human Services has just implemented the standards for privacy of individually identifiable health information. And it is called the privacy rule. And it is required by HIPPA, or the Health Insurance Privacy, Portability and Accountability Act. This privacy rule went into effect April 1 of this year, and it protects all individually identifiable health information held or transmitted by a covered entity or its business associates in any form or media, electronic, paper or oral.

As a result of the privacy rule, authorizations that attorneys have routinely used and subpoenas that they have used -- have had to use to obtain medical records and access the information contained within those medical records have had to be changed and modified in order to comply with the new requirements. Certainly the information contained in those medical records becomes part of pleadings in a civil case; and having such information readily accessible via some online searchable database seems to conflict directly with the new federal mandates under HIPPA. So, again, we raise these as issues that the Commission would have to look at when devising policy.

Quickly, in closing, we want this Commission to establish a sound policy that allows

proper access to public data without, in effect, advertising personal information.

Thank you very much.

MR. ABRAMS: We are now going to ask you some questions.

Let me start out by saying that I want to be as clear as I can about precisely what sort of information is the type that your organization believes ought not to be made available on a wider public basis that Internet dissemination would allow. You mentioned personal, sensitive, and confidential information. You cited a Bill of Particulars by way of illustration.

What is the problem with putting on the Internet as opposed to putting in a court document -- which is available to anybody that is interested -- the work history or the personal history of somebody making a personal injury claim?

MS. VELAZQUES: There could be several things wrong with that.

When a Bill of Particulars is presented, there is information in there, like you said, about a person's social security number, how many children they have, where they live. And let's just say that in the case of a medical malpractice, maybe, the plaintiff in a case like that is suing the doctor, and they have

some kind of medical condition that would be considered confidential, like you said, either HIV or maybe some kind of other condition that they wouldn't want out there. This is information that the Court needs to make determinations of fact and law, but then there is, I think, more information that is contained in pleadings that does not go directly to that function, which if made accessible would be an invasion of privacy.

MR. ABRAMS: But this is all information which the newspaper can obtain.

MS. VELAZQUES: There are various pleadings that are filed that have to be filed as a matter of course with the court and that are available in the court file, but, again, it is a different story to have to go down, physically go down to a courthouse and requisition a file and look through the file and be motivated in that sense than to have that information available in your bedroom which is just a couple of steps that you have to stumble from your bed to the computer. And that's something in terms of the interests of, I think, plaintiffs that needs to be taken into consideration.

Part of your goal is to make judicial proceedings more open to the public. You want to open

the doors to the courthouse. If people think that their business is going to be out there on the Internet, they might not be so inclined to seek redress in the courts, and you don't want to have that kind of -- you don't want to put people in that kind of situation.

MR. ABRAMS: Any questions on my left?

MR. SIMS: Yes.

With respect to your discussion about HIPPA, was it your contention that requirements of HIPPA apply even at the point at which a patient has asked the doctor to give stuff to her lawyer or the other side's lawyer in the hands of the lawyer?

In other words, does HIPPA, in your view, and then I will ask you for authority to support it, affect what a lawyer can file in court?

MS. VELAZQUES: The HIPPA regs have just -- the new privacy rule has just gone into effect April 3. I am by no means an expert on the new regs. I know working at the Trial Lawyers Association that we have been getting inundated by calls from our members who practice and who have been providing either healthcare providers or hospitals with authorizations to get medical records.

MR. SIMS: That's a different matter.

I would ask that if there is anything, either the statute or the regulations or any cases that affect filing, would you supply it to the Commission?

MS. VELAZQUES: Absolutely. I can supply -- I mean, on the Health and Human Services website there is a very good succinct summary of the rule, what the requirements are. And there is also, you know, the actual part of the federal regs that are in there, but I definitely think there is going to be some conflict in what the Commission is trying to accomplish and some other federal standards that have been implemented.

MR. SIMS: But HIPPA affects what the hospital can give out voluntarily. I am not sure it says what a lawyer can do once he subpoenaed that information. And do you think it affects the lawyer's obligations or his abilities after he gets something pursuant to subpoena? And if there is something, please supply it to the Commission.

MS. VELAZQUES: Okay.

MR. FARLEY: I want to follow up a little more with what you think the harm is. We considered certain types of information like bank account numbers, PIN numbers, things like that. That might facilitate a fraud or something of that sort. The kinds of things you were talking about, certain medical conditions or

something of that sort, don't seem to lend themselves to those kinds of harms. You were suggesting, perhaps, that these are things that might be embarrassing to the individual or uncomfortable for the individual. And I just want to press that point a little bit because we have had a submission from some other people who will be talking to us today who say that fear of shame or embarrassment should not be enough to prevent the release of information even over the Internet.

I would like you to address that, if you would.

MS. VELAZQUES: I think we would agree that fear of embarrassment should not trump the need to make information, public information more accessible to the public; however, the information very often that is contained within these pleadings could work harm in other ways, I think.

You know, if you have -- let's say you have, for example, a case where there is a no-fault case or there is a no-fault insurance carrier, it has a lot of resources and they can maybe go online and start searching information about people that they might have claims against them. They want to find that information and use that information in some way, shape or form to either benefit them, hurt the client or do

something with the case.

I think, again, that in the area where you where you are in active litigation, and, you know, you are trying to resolve an issue, you have to also take into consideration that there are entities out there and there are people out there who would go on to the sites and use this information in ways that might not be intended by what this Commission wants the information out there for. And my position is not to say that it shouldn't be done, but my position is that the Commission understand that there are these different types of scenarios that can play themselves out and I'm sure you would want to address those types of issues because it would impact a lot of people that bring cases in court.

MS. BRYSON: Ms. Velazques, representing the trial lawyers, obviously your interest is, in part, on the practicalities, I assume, of what the implications are depending on what our recommendation is and what the courts decide to do.

There have been proposals to the Commission that what should happen is that lawyers themselves should be obligated, that there should be a set of rules that should be issued to lawyers saying, Thou shalt not file the following types of information in

your routine pleadings unless you take certain steps, etcetera.

For example, lawyers might be required not to include social security numbers in their primary pleading but, perhaps, to put it in an envelope and seal it if it was a necessary piece of information.

You know, if you have a dispute with a credit card company about whether this was your bill, you might also have the lawyer obligated not to provide the credit card numbers and so on.

Does the trial lawyers organization have a position with respect to whether this is a feasible and an acceptable course for protecting the very clients that you are talking about?

MS. VELAZQUES: I am sure it is feasible. And, I guess, you know, we would have to see what the final -- you know, what the final rules or the final breakdown of rules would be. But if there is a way to do it and there is a way to protect that information, and if there is accountability built into that and if there is an education process so that lawyers are very clear about what they are supposed to be doing, also information providers that will be managing the information; if they are all very clear about what should be out there and not out there and that there is

some accountability built into that rule system if there is a breakdown, you know, I think that would be something that would be okay with us.

MS. BRYSON: Do you have any experts within your organization with respect to the technological aspects of this?

One of the challenges that we have seen in some of the other testimony and in some of the other materials that we have examined is, for example, an attachment to a pleading might be photocopies of a record that are really -- that really you have to sit there with page by page and look and see whether there was something confidential on it and redact it; perhaps it is a photograph of a rape victim or something.

Do you have any expertise with respect to that or does your organization have access to that?

MS. VELAZQUES: I am sure we do. I mean, there are members that are more up on this and involved in this more than I am personally; but I am sure that whatever expertise we have and wherever we think we can give references to the Commission, we would be more than happy to do so.

MS. BRYSON: Thank you.

MR. GOODMAN: Carrying on the practical aspects of this, and as was just mentioned, something

about redaction; do you feel that if you have information, if you do file, if we do go to Internet access and you have information that is carried in the pleadings or the Bill of Particulars or in any of the papers that are filed, who would be there if the attorneys -- if the attorneys didn't do it, who would be there to redact it, and could this be done within the court? Do you have any feelings about that?

MS. VELAZQUES: Well, I don't think that there is anybody now -- I don't think there is a system in place now that the courts have to do that kind of work. I mean, I think it would take a commitment on the part of OCA, you know, to put those resources there to do that. Is it possible to do? I am sure it is. But I think it would be -- there is cost to consider, you know, and there is restructuring to consider. And if it is deemed that it can be done and this Commission feels it can be done, and, you know, either legislation or rules are enacted or rules are adopted and the resources are allocated to do it correctly, I think that we would be fine with that; but I think all of those things need to fall into place.

I mean, like you said, practically speaking that infrastructure is not there. You are going to have to -- if that's the route the Commission goes, you

are going to have to create that infrastructure, which is another challenge in and of itself.

MR. KOVNER: Am I correct in understanding that it is the position of the trial lawyers that notwithstanding the public interest and the interest of litigants' access, remote access to information about corporations and government agencies and others, that those valuable interests are outweighed by the privacy interests of the individual claimants that you were concerned about?

MS. VELAZQUES: Okay. Just to be clear, you are asking me if the privacy interests for our individual clients outweigh these other concerns? No, that's not our position at all.

Our position is that there is a balance. And that's what this Commission is here to do, to balance the presumption that court records are a matter of public record. They should be readily accessible and we should rely on enhanced technology to do this, but there are competing privacy interests.

In particular, as a plaintiffs' bar we look at interests that are particular to our clients and that might be issues to our clients, and we raise them for you to consider as you're molding your policy, as you are developing policy.

It is not our position at all that one outweighs the other. We want to make sure the balancing starts and reaches it's logical conclusion and that the policy, whatever the policy is and whether you decide to implement something statewide, whether legislatively, or whether it is done -- you know, whether individual courts decide to do it with the guidance of this Commission; we don't have a position either way on that, I think. It is just about making sure that a balancing is done and that all of those factors are considered, which was why I raised the guidelines.

MR. ABRAMS: Plaintiffs are sometimes benefitted by having more information available, more cheaply.

MS. VELAZQUES: Absolutely. Absolutely. And, you know, we have members who are solo practitioners and that would really welcome having more access to trial court proceedings and the like. But there is also the competing interest that a client has in keeping certain information confidential.

MR. ABRAMS: Thank you very much. Ms. Velazques. Thank you for coming.

(Continued on next page)

MR. ABRAMS: The next organization that is represented here today are the people who own the building we're in. The Association of the Bar of the City of New York.

We asked for their comments on the questions that I posed earlier. And the Bar Association has provided us with five members of a sub committee who looked into this and have already submitted to us a statement on behalf of a sub committee of the Bar Association and a separate statement by three members of the sub-committee.

The Association itself has advised us that they have yet to take a position as an Association on the issues we are addressing. The individuals who are here will respond to questions. They've advised us that, rather than even summarize their submissions, that they would rather spend their time responding to questions from us.

I'd ask whoever answers the questions to come to the podium and identify herself or himself.

I'd like to begin with page four of the submission of the sub-committee which, at the bottom, has the following paragraph, which I'll read into the record: "Thus while Internet access to court records is still relatively new and while this sub-committee

cannot state with certainty that it has reviewed all of the systems available to date, the capability of carrying out full text Internet searches of court records does not appear to exist anywhere in the world today. However, if a given body of court records (for example those in New York State) were to be open to unrestricted Internet access, then it would automatically become technologically feasible for commercial vendors to copy and manipulate such records, thereby providing such full text search capability, regardless of whether or not the court system itself chose to provide such a capability as part of its Web site. Alternatively, large litigants or law firms could set up proprietary systems allowing full text searches, which would not be available to other lawyers or litigants or to the public at large. This fact raises consideration of a quality of access to public records that the commission may wish to address."

I wanted to ask whoever wishes to answer one or two questions with respect to that, first: Are the considerations of equality that are referred to here anything more or different than the already existing considerations of equality that might be raised because large litigants or law firms have the capacity already, without regard to the Internet, to have more man power,

more time spent, more money devoted to a particular litigation?

Could you identify yourself?

MR. SCAROLA: Rick Scarola. I'm one of the sub-committee members who spent a considerable amount of time on the issue that you've identified.

I think, to answer the first question you posed, it is an issue that's different in character from the general proposition that those with more resources may have more access. And that's so for the following reason -- let me take a step back and explain, as best as I can, as nontechnical person, what our committee ascertained in the process of our own investigation.

It appears -- and I can't swear to this as a technical matter, but we did have on our sub-committee a number of information technology personnel from some of the large law firms in New York City who were able to assist us with this. It appears that it would be probably a project that would cost in the few millions of dollars but certainly not the tens of millions of dollars to do something as follows:

Write a computer program that in effect crawls through all of what is publicly available on any system, such as the Pacer System, or other state by

state system where court records are publicly available; then captures an image, even though those documents may be in a so-called PDF format or otherwise non-alterable. Still, the image could be captured, all done by a computer program, operating on a document by document basis, in effect, copy those images to ones own substantial computer database and then, with relatively available modest manipulation, make that database searchable in a way that it wouldn't be searchable to the public at large by approaching the Court system records so that, as a practical matter -- In other words, whether it were to be done by a public vendor such as a Lexis or Nexus, or by a private party, someone for a cost of a few million dollars could take whatever isn't posted on the Internet, capture a copy of it and have something that is searchable; in the same way as lawyers think of Lexis Nexus and Weslaw as being searchable.

That's a relatively modest cost, in light of the expense of significant litigation today, but it's a cost outside the reach of many. Certainly, many law firms. And certainly, it's outside the reach of most private litigants. It's within the reach of large litigants. It's within the reach of large companies. And that's why I say it is different in character.

It will allow a kind of access to those with resources that would be tremendously powerful, if one had a private, searchable database of that sort. And it would be simply unavailable in the same form, if it were in fact private --

MR. ABRAMS: I think I'm missing one element.

I understand, I think, everything you've said. How is that different in kind from the advantages that money and person power and the like have always given large law firms, large clients over smaller entities and smaller clients? What's new?

MR. SCAROLA: It's a matter of degree. But I think what's new is this: If a large company or a large law firm were to do it, it would have it and it would simply be out of the reach of anyone elsewhere as today by comparison. If one has enough resources, one can by hand turn enough pages, search enough files and perhaps find what one is looking for. And, as a matter of degree, one might throw a thousand paralegals at such a project but for a relatively modest cost. It would be absolutely available to some and absolutely unavailable to those who couldn't achieve that cost.

In that sense, I think it is different. Whereas, today, you certainly do have advantages by

having more resources. There isn't such an absolute black and white difference in availability.

MR. SIMS: I suppose one possibility is for a relatively modest layout, it would be done by some company, Lexis or whoever, and just charged out the way the creation of the case data base was charged out beginning 25 years ago. So at that point it's not an equal.

I guess the next point is, none of us sitting here knows which way it would go. It would always be open, I suppose, to a private company to do it. But more importantly, have you done any research or drawn any conclusions with respect to whether, as a legal matter, it would be possible -- consistent with the first amendment -- to make records available but to bar the use of computer programs such as you hypothesized?

MR. SCAROLA: We have talked about the possibility as a remedy. We haven't researched the reliability. I'm certainly not --

MR. SIMS: No view as to whether it would even be constitutional to even try to do that?

MS. ABRUTYN: I have a question about something on page seven of the submission.

This is the portion where you discuss types of personally identifying information that deserve

consideration, including: Custody cases, juvenile cases, matrimonial cases, mental health proceedings and probate cases.

And then the next paragraph of the submission goes on to say: "In noting that such cases may raise issues that are worthy of consideration, the sub-committee is not prejudging or advocating that Internet access should be blocked in any or all such cases. In general, the sub-committee believes that restrictions on Internet access should be the minimum necessary to prevent significant harm to privacy, financial or physical security."

I would like whomever is prepared to address whether or not you're advocating that those lines ought to be drawn in advance by this Commission or that the issues you raise could be addressed on a case by case basis by the individual judge in any one proceeding.

MS. KENNEY: My name is Alfreida Kenny. I'm sure other members of our sub-committee will want to comment on your question.

Number one, I'd like to point out we put that part of this in for your information, to let you know how others have -- in other jurisdictions, what they have done. We're not advocating that in this jurisdiction that any types of cases be excluded.

And I'm going to speak personally now. And my personal opinion is you start with everything that's available in the courthouse is available on line. And then you begin to move back. And you move back by looking at security issues, not issues dealing with embarrassment or it's a private fact. Issues dealing with security.

So, if you look at these types of cases, in my opinion, it would be inappropriate for this State to say that certain types of cases that are presently -- where your records are presently available in a courthouse would now be unavailable because of easy access. I don't think that the fact that we now have easy access should be the determining thing that says what I get access to or what the public will have access to.

So, we would not suggest that juvenile cases or certain types of cases necessarily would be excluded but would suggest that you look at the security issues.

I certainly would not suggest that it be done on a case by case basis and certainly not by a judge by judge basis. I think that would be dangerous, create havoc in the court system and people would not know what to do from case to case.

And so one of the things I think is

important -- or two things I think are important are, I think, standards and uniformity.

When thinking about standards and uniformity, I think it's also important to consider what the backlash will be too. And I'm talking about sealing of court records.

What may happen, because of the access to the public, you may have more motions to seal court records.

Now, we have standards with respect to what is required to seal court records. But because people don't like private information out in the public, I believe you will have more motions for sealing court records.

So you have to consider what the backlash is too. And to the extent this Commission would have any jurisdiction saying let's continue to enforce the rules as they are now with sealing of court records and the fact that something is private or embarrassing should not be the subject of a seal.

Have I responded to your question?

MS. ABRUTYN: I think so.

MR. KAHN: Let me just add to that.

MR. ABRAMS: Give your name.

MR. KAHN: Steven Kahn, a member of the ad

hoc committee.

What Alfreida said is correct. Our committee did not intend to suggest that classes of cases should be excluded or included at that level. I think all we were trying to point out there was that it's relatively simple to exclude or to facilitate the exclusion from Internet data of cases. Particular kinds of docketing systems could be used. We spent time figuring out how to implement some degree of Internet access.

In helping you understand our submission, I should say that we took our mandate to be extremely broad. That is, we took the Commission and Judge Kaye's statements to mean that the New York State courts are considering the broadest form of Internet access to records. In other words, not just to what I'll call summary case information; the docket numbers, judges names, litigant's names and docket sheets.

There is a fair amount of that available on line now. But we took the issue to be much broader than that, to cover full text searching capability of pleadings, briefs, transcripts, opinions, all of which can be prepared in electronic form.

But in addition, I think Rick alluded to this earlier, through the use of scanning of paper documents and then optical character recognition processing, to

include exhibits and attachments to transcripts, to testimony of all kinds. In other words, the full content of a case being potentially made available on the Internet and full text searchable, perhaps through the intervention of a third party, if the court systems didn't themselves give that capability.

So that was the mandate we took to be ours and that's what we tried to give some guidance to this commission about.

MR. ABRAMS: I'm still not clear though as to where you come out on what we should do and what we should conclude, based on your testimony.

The passage from page seven my colleague read to you sounded -- read to me as if you were more inclined to a case by case analysis of this rather than the establishment of categories of material that ought, per se, not to be made available for the Internet.

MR. KAHN: That's exactly right. That is our view.

There is, in any kind of categorization, a danger of being over inclusive on the one hand, under inclusive on the other. The more granular the decisions about excluding or protecting information can be, I think the closer we'll get to whatever the right balance is between the clear public interest, which we

took as a given to maximize public access to the extent consistent with these potentially countervailing interests.

It did seem to us, as has already been said, that the technology is available today to make court records -- all of them -- full scope of what I said, available in searchable format from anywhere in the world with a click or two of a mouse.

And it seems to, I think, all of us -- although I don't want to speak for the people making the additional submission -- that this is a qualitatively different kind of court access than has existed to date, including the ability to search docket names.

Therefore, as we saw it, it was really your job, although we were trying to help in assessing what kind of legal framework should be put into place, to decide what to exclude and what not to exclude. And that the existing framework that the New York State courts already have would not necessarily be appropriate in this new -- in our view -- qualitatively different world of information availability.

I should also say, while I have the podium, and Alfreida mentioned this, there is a question of uniformity or not at this point. And speaking for

myself and at least some members of our committee, I think this is a perfect example of where federalism has a very useful role to play.

I don't agree with these other submissions that there should be a uniform standard, at least off the bat. There's so much unknown. We could find no example of full text, case wide Internet access out there today. It seems to us that this is a perfect case for one court to try one thing and another court to try another thing and build up a body of knowledge before uniformity --

MR. ABRAMS: I understand that as a federalism principle. Are you saying within the State one court should try one thing and one try another?

MR. KAHN: That's something your Commission ought to consider. There are so many unknowns here. I think you would all agree trying a small scale experiment like the one in Ohio we alluded to in our papers, that wasn't full texted but try a number of smaller examples might be a path worth taking.

MR. GRIFFIN: Mr. Kahn, I'm assuming that you're a member of the majority of the group and I want to ask you a question by citing something from the minority or the three person report, which I will then ask later to address.

On page four of the second report that we have from the three persons, there is a statement made: "Safeguards for information on the Internet should only be imposed where required, to protect financial security and safety, not to avoid embarrassment or shame."

I have a couple part question.

Number one: Whether you would agree to that limitation. I'm assuming you would not but I'd like to hear what your view is. And whether, under the category of embarrassments, the disclosure of medical information for example, as was discussed by the first speaker today, would be an example of something that we have to deal with that doesn't come under the category of financial security and safety.

MR. KAHN: I don't mean to duck your question but we try not to go beyond what we thought was our mandate.

I think the answer -- certainly the answer I would get was that financial and physical security was one category of information as to which at least the majority of the committee felt strongly. But there was another category. It was not what the submission you're pointing me to cause embarrassment. I notice that word appeared a number of times.

In our view, privacy was a legitimate area for concern. I don't equate necessarily embarrassment with privacy. I'm far from an expert in that area but I think there's a difference.

The majority felt privacy was the other area for concern.

MR. GLEASON: Do you have a point with respect to a point in time when something is filed, when the constitutional protections attach or the right to public access attach? Is this something that occurs simply the instant that it hits the courthouse step or County Clerk's office or is there -- would you object to some period of time for evaluation, if somebody perhaps had an objection to something becoming public?

MR. KAHN: In fact, our report, in getting down to the mechanics of how this might be done, suggested a period of time before posting on the Internet.

I'm not speaking now to posting in court records, as is done in the current world, but we felt because the -- because as I think we all agree, the masking, however it's done, is likely to be imperfect, that there should be an opportunity for the other side to check whether the proper masking was done.

And, therefore, in answer to one of the later

questions, I'm not sure if it was four or five that we suggested that there be a delay before Internet posting to accounts for possible oversights.

MR. ABRAMS: I have a question from one of the drafts-persons of the other or dissenting, different view report. And it relates to material on page four of your report, which states: "We urge that concerns about privacy for electronic records are best dealt with in the same manner as courts in the State currently manage them in connection with paper records."

The argument is then set forth that in a given case, there might be particular consideration given to particular privacy interests, vis-a-vis public dissemination interest.

The paragraph concludes: "The courts are experienced in balancing the interests appropriately on a case by case basis and there is no reason that they cannot continue to do so with electronic records."

Do I understand that correctly? You recommend to us that we should not have categories of material that should be treated differently across the board -- the identification of social security numbers, bank record information -- but that the entirety of this issue ought to be dealt with on a case by case

basis in which a judge engages in balancing of the particular interest as set forth in that case?

MS. BARON: Sandra Baron.

I think my answer to you on that is yes, that isn't the position that this is best dealt with on a case by case basis.

MR. ABRAMS: One of the witnesses we had on behalf of a press group in Albany stated that there was never any newsworthiness and never any -- this is my language -- never any social advantage in disseminating, say, the identification of a social security number. Do you disagree with that?

MS. BARON: I think I would disagree.

I recognize, by the way -- I don't want you to think I don't -- the concerns that legitimately exist for identity theft. I want to put a pin in that because I think there are other ways of dealing with that.

But social security numbers are used today by journalists and, probably, people better than me to talk about how journalists operate to distinguish between individuals in the court system.

It's my understanding that one could imagine many John Jones' in New York City. But to the extent cases involve a specific John Jones, then, if not all,

at least a portion of the social security number may be the mechanism by which you distinguish between one John Jones and another.

It is not always an incident where it is not useful information for news gathering and other purposes.

MS. BRYSON: It would be helpful -- again, I'm not sure who should respond to this, respond to the earlier question about the burden on attorneys and the ability of attorneys, on a practical basis, to comply with any specific rules in this area.

I'm familiar with the federal filing systems that have been -- as is the commission -- have been created and -- but the access to those systems, as was pointed out in the Association's submission, are significantly different than the access that is contemplated by a fully open system.

So, I'd appreciate it if the appropriate people from the Association could comment on the practical implications of trying to come up with rules in this area.

MS. BARON: I'll speak from my own personal knowledge, based on this, and then be glad to turn it back.

I think, in our submission, we make it clear

we're not technologically savvy. What I do understand is systems, as they are today, word processing systems, can be used to help tag information that the court system can then read as information it should not put on a Web site.

That works for those documents that are being created on word processing systems. It does not answer your question, which I think is a legitimate one, about attachments and exhibits.

As we wrote in our paper, we believe that this should be the role of lawyers not the role of court personnel and should be dealt with, at least initially, through certification, which would require counsel to take responsibility for it.

It may sound too facile -- I hope you don't take it that way -- that I believe that as technology begins to march forward, so will the ability to tag information that needs to be redacted.

It's hard to imagine that five, ten years ago we would be standing here talking about this. And, therefore, I believe --

MS. BRYSON: Doesn't your case by case methodology for handling this engender a tremendous additional amount of mechanical and, maybe, pro forma motions that are going to have to be made, while in

this case it should be this way, this way, this way? It seems like the mechanics of it become very cumbersome in a case by case analysis.

MS. BARON: Let me take that as two issues.

One is: Will there be additional motions?

Of course there will, in the beginning at least, until people settle down and see the rules are being generally applied, we hope, by the judiciary, in a consistent manner and a manner consistent with the last ten, 20, 30 years of rulings of what is to be allowed in a public -- in the public record and what isn't.

In terms of will it put more burden on lawyers to tag information? Yes. Yes.

We found that in a document creating a brief, for example, one motion, the tagging was as simple as a search and replace, which existed in our Word software. That doesn't strike me as a particularly difficult burden or one that's likely to cause any major disruption to ordinary counsel.

MS. BRYSON: Someone else from the team wanted to respond to the same question.

Thank you.

MS. NEUNER: Lynn Neuner from Simpson Thatcher Bartlet, as a member of the committee.

Allow me to respond first to your question.

At page ten of the submission by the sub-committee, we attempt to deal with the practical realities of this situation.

In the first instance, I think the consensus of the sub-committee is that it would be untenable to expect court personnel to be the lead identifiers of information, that perhaps the Commission may achieve a consensus should be protected, such as social security numbers.

We envision a system in which it is incumbent upon the moving attorney to file a certificate of compliance with what may be a promulgative court rule that sensitive information, however that is come to be defined by the courts, has been appropriately redacted from the submission. I think that we also expect there could be a period of some delay -- for example, two or three days -- in which that certificate and the pleading was provided to opposing parties and they had the opportunity to provide an immediate objection.

There does, however, raise -- there is raised the question of protection of parties who neither litigant has an interest in protecting. And for this, the sub-committee does not have a firm answer. There may need to be a level of court personnel review.

Similarly, there could be, however, a countervailing check on the moving party in the form of sanctions for failure to undertake a diligent search of ones' file documents for protected information.

While we were on the subject of practical realities, we do think it is useful for the commission to consider what may be unintended consequences of allowing full Internet capability and full text searching.

From our own diligence, looking at different court systems, we found the situation in Ohio to be very helpful in coming to grips with unintended consequences.

As you all know, from the New York Times article, many of the court documents became not full text searchable but searchable with a much stronger search engine than others have seen publicly available.

Unintended consequences were seen in the following:

From traffic tickets, there became identity theft. Because not only did every traffic ticket have social security numbers, it had the height, age, weight and physical characteristics of the individual.

From county appraisals and real estate filings, there became the situation of every neighbors'

floor plan being available on line. Not only for interesting perusement of what your neighbor's indoor house looks like but also the potential for burglars to become very effective in targeting the inner workings of the homes they are looking at.

MR. ABRAMS: Were there any burglaries?

MS. NEUNER: We don't have direct information of that but this is one point we needed to make. There may be harms never known because it does not come out that the source of the information was in fact the court records.

One point that is potential is for the commission to consider a pilot program in one court of the State, to allow a first look at what may happen in terms of actual consequences; to work through, for example, in a pilot jurisdiction. Education of the local bar, so that they can learn compliance with these new forms of rules that are being adopted.

And in fact, you do see, in the Ohio legislature, proposals now by the former County Clerk, James Sissel, recommending attorney education programs. But also, you'll see recommendation of a far greater use of motions for seal. Now, that may be something the commission would not like to see as a kind of unintended consequence of its recommendations. But our

suggestion is really that the Ohio example may be the best forerunner to look at for practical realities and implications.

MR. SIMS: I have a question for Sandra Baron.

Your answer to Floyd, with respect to social security numbers. My question is: Was that your view of wise policy or would it be your view that the line of first amendment cases dealing with publication of truthful information would bar any effort by us or the legislature to, say, social security numbers presumptively must be tagged, subject to later court ruling? I hear your question. I think that an argument could easily -- easily, an argument could be made that, in fact, any kind of blanket redaction of information or denial of disclosure does have constitutional consequences.

In fact, going back to Judge Sissel, who is the Cincinnati -- was clerk in Cincinnati. He pointed out some cases to us which, I'm embarrassed to say, I've not followed up on, in which courts of this nation have indicated that social security numbers are not private information and the publication of it should not be deemed to be private information.

So I think the answer to your question is

yes.

MR. GRIFFIN: I'd like to follow up the counterpart of the question asked to Mr. Kahn. And that is that in your report you said that the safeguards should only be imposed to protect financial security and safety, assuming whatever safeguards there are. And I wonder if you'd mentioned what the reasons are not to deal with other areas of privacy?

MS. BARON: I think we came to the conclusion that categorical -- that dealing with information on a categorical basis was likely to be unconstitutional and more importantly was probably bad policy. That it has proven to be probably the better way of handling information to do it on a case by case basis. That that allows for the judgment of time, it allows for the judgment in context.

If I can back off from the medical question that may be implicit in that to the fact that the bankruptcy courts, as I understand it, have had -- Alfreida can talk to that better than I can. She talked to the bankruptcy clerk on behalf of our Committee.

The bankruptcy clerks have put all of the information coming into the court on line and in the public record for a very long time. Now, one could

argue the reason why one shouldn't have categorical determinations about information that's private or not is because one can understand in the bankruptcy context why it might matter less, number one, in protecting bank accounts and might matter more to those who are potential creditors or those who wish to deal with potential fraud or other issues in the bankruptcy area to have that information available.

It was that kind of experience and that kind of information that we got within the Committee that led us to conclude that dealing in categories was probably not a wise way to go.

MR. CAMPBELL: I had a question to the general panel.

Should the public be charged a fee to access court records on the Internet? You seem to go both ways.

MR. ABRAMS: Do you have a three to two vote on that?

MR. KAHN: Our position on that was fees should be minimal.

We do recognize no matter how the implementation comes about, the Court system is going to bear some costs. We were looking at practical realities and realized that the court system's not

going to be able to bear much cost.

With that said, for all the reasons, I think our entire committee we feel the cost should be minimal, the cost to the public should be minimal. And if there's no fee, should there be a logging system to get access to the court records.

MR. KAHN: I don't believe there's sentiment for a logging system. In dealing with commercial enterprises, LexisWeslaw, Westlaw, Google, which should be mentioned, the court system might impose some fees or some limitations in connection with the full text searching capability being implemented.

MR. ABRAMS: Thank you to the Association for the abundance of richs.

Kenneth Dreifach.

MR. DREIFACH: My name is Kenneth Dreifach. I am the Chief of the Attorney General's Internet Bureau, Office of the New York Attorney General.

I have earlier today submitted testimony, which I will abbreviate. Some of the points have already been made very well and others are summarized in my testimony.

By the way, on behalf of the Attorney General, I'd like to thank the Commission members for this opportunity to address this issue of public and

crucial concern.

The Attorney General recognizes at the outset that for very good, well documented reasons, court records are and should be presumed to be public.

I have been asked to address issues of privacy and security. That might arise out of place in court documents on line with unfettered access. And in doing so, I would address two separate, distinct but overlapping concerns: One of security, often involving financial security. The other, more general privacy issues that arise when sensitive or personal or medical information is made available en masse.

As to the security issues, as others have already testified, identity theft can and probably will arise from the greater accessibility of information, such as social security numbers, bank account information, credit card information and the like.

No doubt, the incidence of identity theft is on the rise. It rises every year. About half a million cases were reported in 2002 and this number surely will increase this year.

All members of society, rich or poor are susceptible to this crime. In addition, victims may find that they will not or cannot be made whole after being victimized in this way.

MR. DREIFACH: (Continuing) And I should say that I am going to briefly address the identity theft issue before getting to the other issue that I sense some of the panel members have particular concerns about regarding sensitive, personal and medical information.

The exposure of social security numbers, credit cards and banking information places consumers at particularly great risk of identity theft.

For instance, with a social security number an identity thief can usually obtain a birth certificate. And with these in hand, the thief can obtain or convincingly counterfeit your passport, utility bill or a replacement driver's license. The thief may also even access your financial assets which often use your social security number as a de facto password and identifier. What then follows is usually limited only by the thief's energy and creativity. The thief may transfer your funds, open new bank accounts, telephone accounts, Internet service accounts, obtain car loans, lines of credit. A savvy identity thief might even, as many have done, contact your local post office or phone carrier and divert your mail or unlist your telephone number so that, for instance, his creditors cannot contact you.

A word about the social security numbers, which probably of everything places consumers in the greatest jeopardy.

They are right now available for purchase online from some online vendors. However, this practice has been very widely criticized, and there is a very vigorous effort in Congress to ban or severely restrict these sales. The tide is with those who are seeking to restrict these types of personal identifying numbers.

Mr. Sims, you had posed a question about the laws surrounding such transfer, and I just wanted to point out that the New Hampshire Supreme Court in the case involving the information broker Docusearch recently held that Docusearch had violated a common law duty when it sold a stalker the social security number and workplace address of his target, Amy Boyer, whom he then fatally shot at her workplace. And here i a quick quote from that Supreme Court. The Court reasoned that, "A person's interest in maintaining the privacy of his or her social security number has been recognized by numerous federal and state statutes. As a result of the entities to which this information is disclosed and their employees are bound by legal and, perhaps, contractual constraints to hold social

security numbers in confidence to ensure that they remain private."

In short, to facilitate the ready accessibility of such information seems to be swimming upstream against a tide of legislators, courts and advocates who are awakening to the importance of protecting this information.

I would like to say now a couple of words about the somewhat more general privacy aspects as distinct from the security aspects.

Other sensitive information beyond simple personal identifiers such as social security or banking numerical information and related information may merit some type of protection. And, of course, I am not here to presume to strike the precise balance or suggest the precise procedures that should apply. That having been said, for many people the disclosure of personal, medical, familial information can be undesirable, disruptive and potentially harmful and may even in the end chill many citizens from trusting and participating in the justice system.

For instance, class action lawsuits against pharmaceutical or asbestos companies may, for a number of reasons, contain the names and addresses of claimants suffering from a variety of ailments ranging

from cancer to depression. Often these may be hidden ailments. These claimants may have very good reasons beyond what you call embarrassment or shame -- because there is no embarrassment or shame to having a debilitating or physical ailment -- to avoid universally exposing their chronic conditions.

In the hands of an employer, the information may provide a basis for discrimination; in the hands of an insurer, it may provide a basis to deny coverage; and in the hands of a financial institution, a basis to deny a loan.

Again, as with social security information, this type of personal information may be available today in various forms to those willing to pay for it. That said, if such information becomes more cheaply and readily available and accessible -- in other words, orders of magnitude more accessible than it is right now -- information brokers can and will aggregate it and find a cheap market for the data. Large employers will purchase the data to run searches on their employees, including regarding their medical conditions, as will banks and insurers. And so the lives of those with difficult, often hidden, conditions may find fair treatment even more elusive than they find it now.

Another example, victims of predatory lending schemes or other consumer scams. If they file claim forms, if they are listed in reports by claims administrators, if they are otherwise contained in court records, sometimes within large accumulated lists en masse, these lists may fall into the hands of unscrupulous marketers and scammers and essentially provide these marketers with potential victim lists to mine. This, again, can have a chilling effect against people participating in and trusting the legal system.

In the testimony that I have submitted I further address the six questions that you have posed, but I sense that there may be some questions. So given the time constraints, I would be more than happy to answer any questions you may have.

MR. ABRAMS: Thank you very much.

MR. SIMS: I have two questions.

First, you mentioned what you call a rising tide of opposition, or the tide is in favor of those who are against the disclosure of social security numbers and such. But when I looked through your testimony and listened to it, I see one case from New Hampshire and a lot of statements by officials and legislators who would like to pass a legislation rule but haven't.

Does the tide you talk about really consist of anything other than one decision and a lot of talk?

MR. DREIFACH: Absolutely. There have been a number of bills proposed in Congress.

MR. SIMS: But they have not been enacted?

MR. DREIFACH: They have not, no. They have not been enacted.

The policy issues and the policy debates include an awakening awareness of the fact that identity thieves are finding it. And there is, I think, very little disagreement about this, that it is much easier and much cheaper to run their scams. And it is placing burdens on the financial markets, on the financial institutions, on insurers, and on consumers. And the 500,000 cases of identity theft will rise. It will rise to a million, it will rise to two million, and it will affect ultimately -- potentially everyone in this room. And I think that's the basis behind these enactments.

Sometimes legislators are slow to act, and sometimes legislators when they are addressing new issues want to get the balance exactly correct. I don't read in their failure to enact it any sort of widespread acknowledgment that this is not a problem. I think it is a problem, and, obviously, that's

something that all of you have to grapple with.

MR. SIMS: The other question is, I guess, that at two points in your testimony you refer to the possibility of rules we might suggest the Legislature might implement purporting to bar wholesale extraction or spidering or other kinds -- or full text searching; and the question is whether you or anybody in your office has done any legal research that would suggest that a rule barring certain kinds of use of court files, barring private companies from installing full text searching, for example, would be constitutional?

MR. DREIFACH: I don't have a particular position on the constitutionality, but I would provide an analogy to other public goods.

I do know that certain databases that exist now that are run by the government such as job and resume databases do provide certain terms and conditions. In other words, they ask that if you are going to use the database that you use it for the purpose provided; that you submit your resume and you see other people's resumes as an employer; that you not, if you are a recruiter or headhunter, pull out the data using these types of spidering programs because that is not the purpose that public money and effort went in to setting up these types of databases. That's

one analogy.

And I think something underlying that analogy is the fact that if everyone had the right to run these types of spidering programs to their heart's content over government resources, well, we know that the sites would crash. And this has come up, for instance, in some private litigation involving eBay and Verio and Register dot com. And the courts there recognized that fact, that it is fair to place certain limits on even generally opened and generally accessible websites. And I do think the analogy to the Botanic Gardens is a good one. Any public resource has particular purposes, and although we are not used to thinking of information as something that should be restricted, I think it is reasonable to at least consider the possibility of imposing certain user conditions to somehow regulate the potentially unfettered and harmful extraction of data.

MR. ABRAMS: Is it the Attorney General's view that court records that contain bank account numbers, social security numbers and confidential medical personal or family information should be made public or not, without regard to the Internet?

MR. DREIFACH: Well, obviously there is a balance. I don't want to duck the question.

Ultimately it probably will be most prudent to have some sort of process whereby these items can be redacted. There may be exceptions to that. And it has to be weighed against the public necessity to have those identifying numbers, but there is a very significant concern about identity theft. These numbers can be and will be used for mischievous and illegal purposes.

MR. ABRAMS: I want to make sure we are on the same wavelength. I meant the last phrase in my question very deliberately, that is to say: Without regard to the Internet.

Addressing now the question of whether this material ought to be public in the first place, is it the Attorney General's position that court records which contain social security numbers, bank account numbers, confidential medical, personal and family information should ever be made public in the first place?

MR. DREIFACH: I'm sorry. I had missed that.

We do draw a distinction between the types of efforts that people have to go through right now and the type of expense that people have to go through right now to get this information with the far more minimal efforts that they would have to go through on

the Internet. And the reason we draw that distinction is simply because there comes a point, practically speaking, where if the information is accessible enough and cheap enough it will have a direct effect on increasing crime. Right now it is simply, as a practical matter, not cheap enough or accessible enough that there is a burgeoning problem arising.

MR. ABRAMS: So I understand the answer to my question is yes, the Attorney General believes that court records that contain bank account numbers, social security numbers and confidential medical, personal and family information should remain public?

MR. DREIFACH: Yes. We have confined our testimony to the placement of all of this information online. We have not advocated any change in the way the current offline system in the courthouse records is set up.

MR. GLEASON: In New York State, as you know, we have pretty wide rules on ability of information and the pre-trial discovery process, and there is some usually hazy line before that actually gets into court records, part of a motion or something the Court might consider.

Would the Attorney General take a position on the types of lines that ought to be imposed on

attorneys, perhaps, before they put stuff into court records and whether there should be any general restriction on privacy matters coming from pre-trial discovery and how relevant they might be in the litigation context of a particular case?

MR. DREIFACH: We have thought about that. And ultimately it may be less cumbersome to consider rules where certain information is not placed into the court files but either submitted in another way or made available for in camera usage, or, perhaps, there might be two sets of papers, one for filing in the courthouse for courthouse usage or anyone who feels the necessity to access it and another set that may be redacted that is placed online.

There are a number of ways to go, I think, and we don't have a particular suggestion as to which of those would be the best balance.

MR. SPIVEY: If we concede that information made available electronically can be abused, why isn't it sufficient to address that abuse through criminal prosecution, through civil litigation rather than suppressing the information in the first instance?

MR. DREIFACH: It is appropriate and we do address it, but there are not enough prosecutors out there to prosecute a million cases of identity theft.

It is a labor intensive type of case to prosecute, and there are other types of crime that sometimes take precedence, such as violent crime.

I would have the same answer as to, you know, if you pose the question: Why not permit people who have been or who suspected they have been discriminated against because of a health condition, why not just let them seek redress under the ADA? The fact is it is difficult to do that. It is costly and it is time intensive. No one wants to go through that. No one wants to go through being an identity theft victim even if a prosecutor may somehow be able to catch the perpetrator, albeit not necessarily make restitution to you. And it is just not quite a proportionate response to say: Well, you know, maybe you will get some satisfaction from jailing the perpetrator.

MR. CAMPBELL: Considering the nature of the Internet, would it be problematic from a jurisdictional standpoint to prosecute some of these people, for example, someone in Germany who accesses the Internet?

MR. DREIFACH: This is one of the reasons I say it is extremely labor intensive. It is also very difficult to get jurisdiction, and it is more difficult to get enforcement power.

We get complaints, as I am sure the district

attorneys offices do, from people who, for instance, in a recent case, traced the source of the person that had stolen her identity to Australia and then it turned out they weren't there. They had a web hosting company out of Germany but rented a post office in New York.

It is very labor intensive and it involves, very often, people oversees.

MS. ABRUTYN: Obviously the Court records containing this information aren't yet on the Internet. Also, obviously the identity theft has been talked about as a problem in a lot of different places. We have seen in other contexts that a lot of the information you are concerned about is already out there on the Internet in one form or another.

My question is: Can you cite us some examples or specific cases from your experience where the identity theft occurred because the thief got the information from the Internet, what information it was that the person got from the Internet, and whether you have any reason to know one way or the other whether that information would have otherwise been available if it wasn't on the Internet?

MR. DREIFACH: Well, of the hundreds of thousands of cases of identity theft that have occurred, the thieves absolutely got their information

somewhere. I will give you one example.

We have seen a surge in phony e-mails by scam artists who somehow learn where people bank and then send them e-mails posing as their bank asking them for security purposes to re-enter their account number and pin number. They take them through a link in the e-mail to a perfect copy of the bank's website that resembles the website and even has a similar URL.

A large number of people have fallen for this scam, both account holders at large banks and people who have accounts through financial intermediaries and aggregators.

The most publicized case of identity thieves doing actual harm, or I should say people who access information brokers doing real harm, is the Docusearch case where someone obtained this woman's social security number and workplace address and then stalked and killed her.

Now, to some extent people are -- if people are willing to work hard enough they will find you and they will do what they are going to do, but there is no question that the more accessible this information becomes, the more the incidence of identity theft is.

MS. ABRUTYN: Should I take it from that that you don't have a specific case that you can tell me

about where you have learned through your investigation, your prosecution, that the information that the thief obtained they actually obtained from the Internet? I am looking for specifics.

MR. DREIFACH: We have the e-mail cases in our files which we don't -- the cases are under investigation. We don't make that public under the Freedom of Information Law.

The Docusearch case is a publicly-available case. And I will cite you to a website. Go to Dunhills dot com, D-u-n-h-i-l-l-s, Marketing Company, one of many that offers vast mailing lists, telephone and e-mail lists of, quote, consumers with ailments, literally ranging from acne and asthma to ulcerative colitis and everything in between.

That particular company ties access to hundreds of thousands of people who have everything from Crohn's Disease to hidden heart ailments, people in cancer recovery, people who have been on depression drugs, you know, and dozens and dozens more.

The problem is that these lists are expensive. They are between $1.00 to $2.00 per individual profile; and they are generally not sold right now per person, they are sold in bulk.

There are investigative services that, for

instance, your employer can certainly hire, and for thousands of dollars can find out a great deal about what diseases you may have. They can even track you. That's publicly accessible. Someone follows you for a couple of weeks to your doctors appointments, and they can learn a great deal about you, but they have to be willing to spend thousands of dollars for that and your employer may not find it economically feasible to do that. If it were $50 instead of thousands of dollars to get that sort of information resource, your employer might do that.

MR. ABRAMS: Thank you very much for your testimony. We appreciate it. We have one witness who has to leave a little early to catch a plane. I received a request that he be moved up a bit. That's David Bralow.

MR. BRALOW: Mr. Chairman and members of the Commission, I am David Bralow, senior counsel for Tribune Publishing, here today on behalf of Newsday. I have provided written comments and I will summarize them at this point.

Besides Newsday, the Tribune Company publishes 11 publications including the Chicago Tribune and the Los Angeles Times. It also operates 26 television stations, including WPIX here in New York

and WEWB in Albany.

I think that it is clear that everyone agrees to the principle that -- everyone agrees that any debate about access to judicial records on the Internet is informed by the same presumption as the access to records. Discrimination between a byte and paper, the imposition of restrictions on one but not the other requires a demonstration that access to the electronic record causes a qualitatively different effect than access to the paper record. And that difference itself, not simply the nature of the information but the difference between those two forms of access must jeopardize some the compelling State interest.

It strikes me that we spent some time today talking or thinking about something that I labeled the practical obscurity concept. The idea that if you increase the transactional costs of getting a public record or judicial record you somehow change the nature of the information itself. And it strikes me that that practical obscurity doctrine is really threatening that presumption of access at its very basis.

If access to judicial records is presumed to be in the best interest of the community -- and that's not doubted throughout these proceedings -- how can permitting more convenient or more accurate access to

those same records create a compelling threat?

Furthermore, I think if you remove the barriers of access to judicial records, what you are doing is renewing a core First Amendment constitutional value of direct and public observance of the judicial system. By providing records electronically, we can restore that direct citizen's contact. But let me get more pragmatic.

Newsday believes that the press's ability to fulfill its mission improves with electronic access to judicial records. Such access increases timeliness and accuracy and offers reporters tools to look at trends that they wouldn't necessarily have the ability to do without that kind of access.

For daily news coverage, the present way of storing and retrieving judicial records creates news barriers that burden both the newspaper and disadvantages its readers. Reporters cannot get information when the court file is in a judge's chambers, for instance, or in the possession of attorneys. If access were permitted online, a newspaper could rely on the court file rather than the exigencies of extrajudicial statements that occur every day.

Reporters often have logistical problems. In

Suffolk County there are state courts in five locations, some 30 miles apart, and the court clerks' offices are in two locations. Court personnel often can't even say where the files are, and oftentimes they don't even know what courthouse they are in. Our reporters have driven back and forth trying to find particular files. And that is as true for individual citizens as it is for reporters.

Reporters are often affected by zealous clerks and attorneys. Clerks, prosecutors, attorneys remove documents from files, even criminal cases, simply because they believe without the benefit of court order or legislative authority that it is in the public interest to remove those. An electronic records retrieval system will compel trial participants to seek appropriate sealing orders rather than exfoliating the file.

Also, access to online records creates a certain amount of uniformity. In a recent examination by Newsday of Surrogate Court files here in New York to document fees attorneys received in trust and estate cases, a Newsday reporter found in some cases that the petition for fees and the judge's order establishing those fees were missing.

If we have a system where these documents are

put online, there will be, by necessity, additional uniformity of files. But besides enhancing the accuracy and timeliness of these records, our ability to serve the community would improve with in-depth analysis that would come from full text searching. That type of functionality permits the public to locate records applicable to a particular subject.

For instance, Newsday published a series about Catholic priests allowed to continue ministries despite accused sexual abuse. Another series focussed on inmates beaten by correctional officers and the medical care of inmates at county jails. The reporters that did that work all will testify that that kind of work creates a significant dedication to man hours and a commitment to just troll through judicial files in such a way to create and to discover the trends. With online access, we can get to that greater depth and have greater insight.

Let's talk about privacy and identity theft for a second. First, privacy must be defined with specificity before it can be meaningfully addressed. It is an elastic concept, you heard that here. It is distorted to unrealistic expectations of anonymity, including common information found on streets and in phone books.

Before the existence of any so-called private fact can meaningfully restrict access to a judicial record, we have always had the standard that that private fact should be examined in the relationship to the harm caused by permitting it to reside in an open court file. It doesn't change that that file would now be available electronically. This is just the way -- it is an old-fashioned way of saying that a judge is in the best position to protect whatever rights exist in any specific court file. There has always been adequate measures for litigants and third-parties to request sealing of information based on well-established, albeit difficult to establish or to meet, standards.

Let's assume a lawsuit is filed in Nassau County against a chemical company that involves personal injury claims. The court file will, by necessity, contain medical information. A motion to seal that medical information would balance the harm to that particular individual against the need for the information or the subject. Furthermore, medical information that might be considered private in one context is no longer private if that medical information becomes an integral part of the judicial decision-making process. Without a demonstration of a

specific compelling reason for the sealing, there would be no ground for the sealing itself. To seal automatically would simply ignore the dictates of Craig versus Harney, that what transpires in a courtroom is public property.

If there is some change in status that arises from greater access, that harm must be established or evaluated in the same precise and nonspeculative way for both Internet access and paper records.

That leads me to a concept of identity theft. As a practical matter, I am not aware of significant problems that have arisen for identity theft out of judicial records and out of the use of judicial records. Indeed, many causes of identity theft are relatively low tech and don't involve court files or the Internet.

Jodie Bernstein, the director of the Bureau of Consumer Protection for the FTC, testified that among the common causes of identity theft is simply rummaging through the trash for bank statements and stealing a purse or wallet is another.

As I was sitting here listening to the testimony I pulled out my wallet, my Blue Cross/Blue Shield card and my drug prescription card, all of which have my social security number on them. In fact, the

Supreme Court case that most recently addressed identity theft dealt with the factual scenario that a death occurred when a secretary in a doctor's office copied a patient's social security number from a woman's initial referral form.

The idea that social security numbers create a significant and palpable risk may be true, but until we think about the concept of limiting the ubiquitousness of the social security number as an individual and identifier, removing them from the court file is not going to be effective.

MR. ABRAMS: Your time is about up, sir.

MR. BRALOW: Okay. I would like to answer some questions. That would be fine.

MR. ABRAMS: Okay.

MR. LELYVELD: The point about ubiquitousness is well taken, but would you agree with the argument made earlier that it might be unconstitutional to remove social security numbers from court filings, that reporters have a constitutional right?

MR. BRALOW: I think certainly there can be an argument that blanket prescriptions of information in a court file fails to meet that standard that we are familiar with. I think also there are times that the legislature can, upon sufficient factual findings, make

certain determinations with respect to information. I do believe, however, endorse what was said before, that my reporters routinely use social security numbers to make sure they are not reporting about the wrong person. When there is a case of 16 John Smiths, that identifier becomes a germane and important piece of information.

I also think we tend to burden information because of conduct. And the conduct isn't simply the conduct of the bad guy, the conduct is that we have as a nation chosen to use this form as the discrete identifier of people; that the fair credit reporting act has chosen to make this identifier or the credit card companies have chosen this identifier as the sole means of checking who the individual is.

MR. GLEASON: I have asked a couple of questions of some witnesses regarding the tension that you have between the wide open discovery that you sometimes get in civil actions and the openness of court records, and so I have this question for you because I think you said there should be no difference at all between an electronic record and a paper record. The difference arises out of a fact scenario such as the following: For example, consider a case where there might be trade information that is very

sensitive. In one instance it is filed in the courthouse, it is served on all the other parties, and they realize the Heinz Ketchup recipe is in the court filings. So the parties make motions, get a protective order, and the court file is adjusted so that it's sealed.

Now, compare that situation with an Internet situation where the motion papers containing the sensitive information are filed and immediately available to the world. You can have a court protective order after that, but we all agree that the toothpaste is out of the tube and the remedy might well be too late.

Don't you see that as a possible reason for treating electronic records as, in some sense, qualitatively different than paper records?

MR. BRALOW: I think most litigants deal with trade secret circumstances by creating protective orders prior to the time that the material hits the court file. So in the majority of cases in which you have proprietary information, the possibility that that proprietary information would hit a court file has already been discussed and there have already been procedures put in line. I think you are talking about a third-party or someone that is not a party to the

matter.

MR. GLEASON: Proprietary information is one category of sensitive information. Let's talk now about somebody's medical history that might be the subject of some dispute in depositions but ultimately is not really very relevant at all to what the judge is going to act on in the case. And yet because of some dispute over discovery, we find one day that motion papers are filed that include some rather sensitive personal information about somebody that really doesn't have anything at all to do with what is ultimately going to be litigated. It would just be another category of information that might be generically sensitive.

I don't know that I would agree that you can always say that parties are going to put up the firewall before the information hits the court file in a successful way. That's the thing that troubles me. And an electronic file has vastly more opportunities for immediate and permanent dissemination than a paper file.

MR. BRALOW: I would take a hard line and say that it would be the attorneys that have to practice before the bar that have an obligation to refrain from putting scandalous or impertinent information into a

court file, material that isn't otherwise relevant to the actions before the Court. And once the file or the pleadings hit the court file, then it really becomes part and parcel or up to the judge on a case-by-case determination.

MR. GLEASON: Do you view the temporal point in time when constitutional protection attaches as being simply the act of it hitting the file or is the time when protection attaches when the material becomes potentially part of the judicial process?

MR. BRALOW: I would view either the Constitution or the Common Law Rights, depending on what place you are at, to hit or attach at the time that the material hits the court file.

MR. GLEASON: As soon as it hits, it is then public?

MR. BRALOW: Yes.

MR. ABRAMS: Thank you very much. We appreciate your testimony. Have a good flight.

(Continued on next page)

MR. ABRAMS: Ms. Watson.

MS. WATSON: Charlotte Watson, Executive Director for the New York State Office for the Prevention of Domestic Violence.

Chairman Abrams, esteemed Commissioners, I want to thank you for the opportunity to address you this afternoon on the most important and challenging issue of public access to court records. The New York State Office for the Prevention of Domestic Violence is an executive level state agency, created by the governor and legislature to improve the response of the State and local communities to domestic violence.

Great strides have been made in the past 30 years in response to domestic violence, along with the vasely increased use of the civil and criminal justice system. The lion's share of change in the criminal justice system's response in the State of New York has occurred over the past ten years under the incomparable and synergistic leadership of Governor George Pataki and Chief Judge Judith Kaye.

MR. ABRAMS: Do you speak for the State of New York in saying that?

MS. WATSON: Yes.

MR. ABRAMS: Thank you.

MS. WATSON: At the same, time the use of

computers and access to the Internet has exploded. What we innocently put on the "Web" a few years ago is now being used in ways we never considered, including invasive crimes such as identity theft. We've heard horror stories of how stalking victims were tracked and harmed through information posted and available to all for good or bad intent. We've all seen those annoying pop-up adds on our computers, advertising the ability to find literally, anyone. As a domestic violence advocate with more than 27 years in the field, and one concerned about privacy in general, those ads, and the open, easy access to so much personal information in what we term the "information age" are truly frightening.

Nowhere is this more of a concern than when considering the safety and security of victims of domestic violence, sexual assault and stalking. We know that domestic violence is pervasive, on-going, life-changing reality for millions of women and children in this country, and stalking is an integral part of the dynamic of domestic violence.

Domestic violence victims know all too well their abusers will use any means to control and terrify them and keep them from escaping. It is not unusual for a batterer to monitor the odometer on a victim's

car, record the victim's phone calls, or use hidden cameras. Imagine what it would be like to have a Global Positioning Satellite unit attached to your car and monitored constantly by someone in authority over you. This is the daily reality of many victims of domestic violence with the state of technology today. What will tomorrow hold?

It's extremely difficulty and often dangerous for battered women to escape their abusers. Many find it necessary to flee the area entirely in hope of finding safety. Those who are able to get away live with the extreme fear of being found by their abuser. A losing battle for approximately 1,100 U.S. women each year who were murdered by their intimate partners after fleeing, as well as, countless others who are re-assaulted.

There have been many attempts to help victims find safety. Recent changes in law make it a federal crime for an abuser to stalk and abuse a victim across state lines. There are processes by which victims can change their names and social security numbers, sacrificing their identities just to be safe. Unfortunately, at the same time we are recognizing the needs of domestic violence victims, the trend toward "open government" and access to information has become

an easy, affordable and valuable weapon for abusers.

As advocates for victims of crime, however, we do recognize the need to find ways to increase the accountability of systems, including the courts, in their responses and decisions. It's vital that these interests are balanced against victim safety and the privacy of users of our court process. In the effort to increase accountabilities, the court must be mindful of even the appearance of culpability, should granting easy access to information result in harm to a victim. It should never be the case that potential consumers of the courts must weigh the need for safety through court intervention against the need for privacy and anonymity which may also impact safety.

In light of these concerns, I will outline a number of recommendations regarding open access to court information. In addition for our own experience in responding to domestic violence, we received assistance from the National Network to End Domestic Violence in researching this important issue. The following critical issues must be addressed before moving ahead with this process.

The negative implications include, as has been mentioned:.

A chilling effect on victims who are

considering using the court for legal relief.

While we applaud the fact that family court and matrimonial records will not be subject to open access, I must emphasize that under current law, criminal court is the only court in which many victims may seek relief. Consider, for example, a victim who's being abused or stalked by a boyfriend. To obtain an order of protection, that victim will have to disclose significant personal information and potentially embarrassing details about the abuse in criminal court. Under the Conference of Chief Justices and the Conference of State Court Administrators Guidelines, this information would readily be accessible by the public and the offender. It's not a leap to say the victims will be reluctant to pursue an order of protection under these circumstances. Is it fair to ask a victim to sacrifice her privacy for the safety she's entitled to under the law?

Imagine the heyday the pornography and smut industry will have with such easy access to crime scene photos of horribly violent rapes and homicides. Imagine the websurfer who accidentally opens a porn site or the errant adolescent going to sneak a peak only to discover the crime scene photo of his naked mother lying in a pool of blood. At what point would

the balace tip from accountability at this point to culpability? At what price? Who and how would these decisions be made as to where to draw the line?

There are safety risks for crime victims and witnesses. As I noted earlier, abusers often track and monitor their victims as a means of maintaining control. These behaviors typically increase when a victim leaves the abuser. Whenever a victim becomes involved with the court system, whether voluntarily, as a result of mandatory arrest or pro-prosecution policies or for some other reason, precious information about her location, status, current name, phone numbers and other circumstances is disclosed. Such disclosure is a major concern for my agency and victim advocates across the state. We know that abusers will access this information and use it every way possible to stalk, threaten, assault or kill the victim and maybe her children.

This can be a problem even when the victim is using the court system for something unrelated to domestic violence. For example, if these involved in a motor vehicle accident resulting in legal action and the information, includinging simply the location of the Court is posted on the Internet, her address would be posted making it all too easy for her abuser to find

her. Perhaps she relocates to escape the abuser and later becomes the beneficiary of a probated estate. As a result, identifying information could be posted creating similar safety risks. Ironically, if the victim is seeking a legal name change, even this information could be posted on the Web, making her efforts at anonymity fruitless.

It's important to note she may not be a victim at the time of her interaction with the court on the myriad of non-domestic violence related actions that could bring her to court. After one date with a stalker, she would be vulnerable to his gaining valuable information about her that could lead to her demise.

There's an increased opportunity for identity theft. Destroying the victim's credit and reputation is a tactic already used by batterers. Open public court records will only increase the opportunity for accessing and misusing personal information.

We're concerned about the secondary uses of the information. Information stored by the courts will most certainly be used for purposes that move far from the original public policy intent of governmental accountability. It will be gleaned and sifted and compiled along with other information to create

entirely new databases that can be misused and misinterpreted. Once the information is gathered for another database, it can never be taken back or corrected. In domestic violence cases, false or misleading information could be deliberately planted by the batterer in spurious legal filings that include slanderous material against the victim which are then posted on the Web for all to see and use.

Internet access could undermine the victim in custody proceedings. Seeking custody is one of the most powerful tactics used by abusers to access control their victims. Abusers will use every means available to discredit the victim and prolong a custody battle. The proposed guidelines actually aid abusers in this process. Open public access to court information provides abusers with cheap and easy access to all records of any criminal proceeding, regardless of whether such information was relied upon we the court. This poses serious ramifications for victims who ultimately leave their abusers and seek custody. Economic survival or the abusers threats or false promises often compel victims to minimize or deny the events or later recant earlier statements of abuse that form the basis of a criminal prosecution. The fact that such records from a criminal proceeding and many

civil proceedings will be within easy grasp of an abuser in a subsequent custody proceeding essentially re-victimizes the victim, rewards the abuser's use of coercive tactics and facilitates the abuser's use of custody as a weapon of control.

Finally, there's a dangerous reliance on individual discretion. In many instances, courts will possess far more personal information about a victim than might be held by a State agency subject to FOIL. The proposed guidelines heavily rely on human discretion and information management in an effort to protect personal privacy which will undoubtedly result in human error. Unlike many other types of crimes, in domestic violence cases, one simple failure to redact an address or social security number could have, literally, fatal consequences. Even the most competent offices may find themselves outmatched by an abuser determined to discover the whereabouts of his victim.

Under the proposed guidelines, victims of domestic violence will likely be hunted down, harassed, stalked, assaulted or even killed with greater frequency. Government exposure to legal liability will increase. It's deeply troubling for us advocates to contemplate a system so completely depends on individual discretion and competence at the risk of

harm to victims and their children.

We whole heartedly agree that as much information as possible should be available to the public regarding governmental actions for systems accountability to be achieved. However, this should not mean full and open, cheap and easy access to everything that happens within the walls of the courthouse. We must hold this system accountable in the same way that we hold the healthcare system accountable without violating the patient's right to privacy.

MR. ABRAMS: Miss Watson, your time is up and we do have your statement. And I don't want to loose the chance for people to ask you questions.

MS. WATSON: May I make one more point?

MR. ABRAMS: Briefly.

MS. WATSON: If indeed the objective is governmental accountability, we have to agree on what the objective is. Yet we concur with the recommendation of the Privacy Rights Clearing House that case information be gathered but posted only in the aggregate, making personal identifiers unnecessary.

So we can know that in a given courthouse, the Family Court judges, who have certain number of orders of protections before them each month, which --

you know what percentage are granted. Maybe you have five judges, four of them grant 75 to 85 percent of the orders of protection petitions that are before them; maybe one judge routinely grants only 30 percent.

That would help you to identify, in terms of the court's accountability or an issue that needs to be looked into. Aggregate information might be helpful without having to identify all the personal information and put victims at great risk.

MR. ABRAMS: It seems to me that a good part of what you're saying would apply to public access, regardless of whether there's an Internet or not.

When you say that "open public access -- on page five -- to court information provides abusers with cheap and easy access to all records of any criminal proceeding, regardless of whether such information was relied upon by the court." The fact is that now, without an Internet -- before we had an Internet, there was open public access to court information, regardless of whether the information was relied upon by the court.

Does your office favor limiting access to the information itself, regardless of whether it's going on the Internet?

MS. WATSON: Our concern is the same one

expressed many times today; that's the cheap, easy affordable part of it.

You can actually be sitting in your bedroom, walk over to your computer and find the information. It's very different from having to go down to the courthouse and go through the records and find the information, being able to sit in California, sit on your computer, pull up your victim, your target's information on a court record in New York.

MR. ABRAMS: Is there any benefit to having such information public? If your position is the only purpose of access is accountability and that making information like this available doesn't really relate to accountability, unless you're aggregated or take some other steps, why make it available at all?

MS. WATSON: I think, if you're talking about a local community and you make the information available in the community interested enough and willing enough to pursue that information, it could help them understand what's happening in their system and help the system improve.

In individual cases, you have the right to get as much information as you possibly can, if you're litigating a case.

But I think the idea of public now really --

"public" being defined as the entire world. A gentleman before was talking about public access, meaning information available to the citizens. We're talking about every person in the world having access to this information.

At the time the constitution was crafted, we didn't even have California. You know? So the idea of getting information from -- at that point in time from a place as distant as California would have meant days and days of travel to come and review a paper in a file somewhere. Now we're talking all the way from Hong Kong, Russia, all parts of the world in a matter of seconds having access to the information.

MR. ABRAMS: Do you think newspapers should be banned from publishing the information or broadcasters barred from broadcasting it?

MS. WATSON: I think we always have to think first about what is the potential harm that's possible and I think that we would -- at least I would hope we would all agree if there's a clear avenue of harm, we would want to avoid that.

I'm not saying that newspapers shouldn't publish information or really describe what's happening to our clients and our families. But we already have an agreement. By and large we don't publish the names

of rape victims. The problem there is that if she happens to be murdered, that confidentiality requirement is gone.

What if she's raped and severely beaten and in a plea agreement or through the course of the trial, if rapist is not convicted of rape, he's only convicted of assault, she is no longer a rape victim then her name can be published. It can be very damaging to the person.

We always have to weigh what's the public interest against the harm to the society and to that individual.

MR. FARLEY: I was wondering -- you may have addressed this to some extent. Could you identify the kinds of information that you think would be most damaging to have publicly available for victims of domestic violence? And I'd also like you to give me your thoughts on the extent to which that same kind of information but about the potential or possible abusers might be of some value to their victims. For example, I would think that it would be of interest to them to know that the abuser lives in Oregon instead of New York or something like that. So if you could address that as well.

MS. WATSON: I don't think where the abuser

lives is particularly that important to the victim.

It doesn't mean -- he might live in Oregon, she might live in New York. If he decides to come after her he can find his way to New York.

So what's more important to protect is her information. Where does she live? What's her phone number? And also other information that can be offered up to a court that may or may not be true that disparages her in some way, that then can be used in another proceeding, like a custody proceeding, an attempt to cause her to loose her job.

Abusers attack their victims on many different levels. In many ways, information they can have to use against her in other venues is a tool for them.

MR. SIMS: If I understand your testimony, the protection you want is not limited to any category of domestic violence case, it involves every court case, including every criminal case, because every case may have something that could eventually harm a potential victim. Is that the point you're making?

MS. WATSON: The point I'm making is, any time you have an individual appear before the Court and have to give their name and address, you now can be placing them potentially at some risk. Of course, most

people won't be be harmed but we can't preselect where the high risk is.

MR. SIMS: Would you be willing to trade away the protection to the potential victims that comes -- somebody sort of made this point but I think not in quite this way -- from having access to cases in that state and other states about potential attackers? In other words, part of your assumption seems to be every alleged victim is a victim and every alleged attacker is an attacker. That may be true. Then a woman could find out someone dating her has been accused in seven other states through seven other cases for the same thing. Wouldn't that be information she'd want to know?

MS. WATSON: Not necessarily. You can never broadly generalize and cover everything. There are certainly exceptions to this rule. I don't know how many of you had relationships that weren't the best; weren't necessarily abusive, violent or threatening but you've had a few of your friends, other friends tell you this person is not really the best one you want to let into your life. You think, I know better. I have the relationship with this person. Our heart rules our mind, sometimes and we go forward.

Having access to that information to her, I

don't think most folks will go on line to see whether or not this person has ever been a danger to someone else. If they did, they might make up reasons, excuses for why that would be. And the heart may win out.

MR. SIMS: There are also cases in which people have been convicted of various kinds of abuse. I think of teachers, students, for example. Then it's turned out, through reporters researching open court records, the convictions are unfair, based on improper convictions and the availability of court files has led to the exoneration of people improperly convicted.

Is that a benefit you'd be willing to trade away from this sort of super protection you're seeking?

MS. WATSON: I'm never willing to trade away the safety of the victim. If there is a way to get at some of this other information without jeopardizing that person's safety, that would be my preference.

MR. KOVNER: Miss Watson, in some courts in New York State you want to access records today, you have to go to the courthouse and you have to fill in a form and say who you are in order to get it. We've heard some testimony from people that say if, to the extent it should be remotely accessible, that you shouldn't have to log on or provide any identifying information to access court records that are otherwise

public. Would it be material, as far as you're concerned, if to the extent this Commission were to propose that there would be remote access available, that that -- to condition remote access on logging on and providing some identifying information so that it would be ascertainable as to who had obtained particular records at particular times?

MS. WATSON: It's an interesting question because you can create any identity you want on the Internet. I could log on as Mickey Mouse. I can create a pass word. Usually, they are asking you to create your own identity when you log on. I don't know that you necessarily are going to have the information about who is logging on.

Honestly, I don't have a strong opinion about it one way or the other. But I don't know that it provides any sort of security that we might hope that it would be a deterent to anyone.

MR. KOVNER: Doesn't even a fabricated entry contain within it information that provides some identifying information to authorities who would wish to pursue the person or persons who had access to that information?

MS. WATSON: Honestly, that's a very technical question and I don't understand the

technology well enough to answer it. I'm sure some prosecutors who are prosecuting some of these Internet based crimes, child pornography, those sorts of things, might be able to say that.

Would that level of scrutiny be applied to all the folks who are accessing information, how would we ever provide enough resources to do that?

Again, would it be an after the fact now that a crime's been committed, an individual's been harmed? Would we be going back to prove the case against the perpetrator of that if in fact we didn't prevent it when maybe we could have?

MS. ABRUTYN: There's been some discussion earlier about potentially handling these kinds of issues on a case by case basis. And what struck me about the issues that you raise, the concern over the victims, is that in those instances the person involved in the proceeding -- the victim who is at risk -- would always know that they had been the victim of a stalker or domestic violence or whatnot. And do you think that the concerns you've raised could be addressed by having that person put those facts before the judge in any specific case and presumably, I think, if one were to go before a judge, that there's a likelihood that a request would be granted, if their safety and security

was actually at risk as opposed to some sort of blanket prohibition that would keep all records off? As you said before, maybe 80 or 90 percent of the people wouldn't be at risk but to handle the 10 percent that would by having them make an application to have their case treated differently or specially. And if that would not address the concerns, why not?

MS. WATSON: I don't think it would address the concerns because, first of all, any time you do things on a case by case basis and you're involving individual judgment, you're going to end up -- I don't know how many judges we have in our system -- you have the potential of that many different ways to view a particular case and to make a decision. You don't have consistency in that regard.

And I might know that I was a stalking victim, I might know that I was raped or I might know I'd been battered. When I show up to court on my traffic ticket or my father's estate or whatever, but what I if I don't know that? What if that hasn't been my experience? I've been lucky, haven't had any real bad problems and I go through this process. The first question is state your name and address for the record, please. I do that. It's on the record. Then two or three years down the road, I'm mugged or I'm assaulted

or I meet someone for a date and by the end of that date, I know that there's a serious problem here, I don't want to see this person again. He doesn't want to give up. So he goes on the Internet and boom, there's the information. There's my address. I didn't give my address. In a matter of seconds, he can have access to it. We don't know prospectively who the victims are going to be. We don't know how many victims there are in the United States in terms of violence against women. We know there are estimates, at least one out of every four women will be physically assaulted by an intimate partner in their lifetime. That's a lot.

There are similar numbers on women who will be raped. It's a fairly significant part of our population we're talking about putting information on the Internet. For what purpose? I'm not certain. This particular information, for what?

MS. BRYSON: I want to make sure we understand the scope of what you're recommending.

On the one hand, it sounds like we basically should recommend that there not be any personal information of any kind, demographic or potentially embarrassing or personal information, medical information, et cetera, should basically be barred from

those court records that are going to be filed electronically.

On the other hand, it seems there are certain specific pieces of information that trouble you more, such as name, address and perhaps certain identifying numbers. Can you be a little clearer about exactly what you're recommending we do?

MS. WATSON: I'm recommending that you not use personal identifying information, that you not put that on the Internet. I'm recommending if the goal of this -- I understand this to be the goal, from the Conference of Chief Judges mono policy guidelines. From what I understood Judge Kaye to say when she announced this initiative, the goal is accountability of the court system.

If that's the goal of it, then why does it matter what my name and address is? What matters is what did I petition the court for? And what result did I get out of it.

And not only me in my individual case. Are we looking for a pattern where we might have problems that we need to resolve? A place where maybe someone's not as accountable as they might need to be? We can come in and bring a fix to that problem.

MS. BRYSON: Do you mean literally not to

put names on the Court papers?

MS. WATSON: No. On the court papers, of course. I'm saying -- in a way, you could say that the Internet is much more akin to a publishing house, newspaper, magazine than it is to a filing cabinet because you're publishing information. If I come in to the court, this is my whole court file. There's a lot of stuff in here. My name, a lot of facts about me. Maybe some untruth about me are all in this particular file. And this is in the filing cabinet in the courthouse. You come in and if you want, you can read everything in there. That's very different than if you put this in the New York Times and everybody can pick it up and read it tomorrow.

MR. ABRAMS: So what are you saying, that it shouldn't go on the New York Times?

MS. WATSON: I'm saying if there is an interest that serves the public that the Times identifies, of course it would go in the New York Times. But what I'm saying is would you take every single piece of information that comes before the court and publish it to the world? That's what we're doing. We're publishing it to the world. We're not simply putting it in the world's filing cabinet.

MR. ABRAMS: Thank you very much.

MS. WATSON: Thank you very much.

MR. ABRAMS: I want to say, for the witnesses who are waiting, we appreciate. This is really very important testimony for us. We're hearing a lot of views we haven't heard before. I apologize for making you wait around but this material really matters to us.

Next person is Hillary Sunghee Seo.

MS. SEO: How much time do I have?

MR. ABRAMS: You have five minutes. Maximum of ten minutes. Five minutes we will smile more broadly.

MS. SEO: A lot of my testimony does overlap with Charlotte Watson's testimony.

I believe you have copies of my testimony?

MR. ABRAMS: Yes.

MS. SEO: I represent Sanctuary For Families' Center For Battered Women's Legal Services. It is the oldest and largest legal services organization in New York State, dedicated to domestic violence victims.

Last year, our staff and voluntary attorneys provided direct legal representation and advocacy services to 3,000 battered women. We also lead community education and public advocacy efforts to help

promote healthy relationships free of violence.

We also believe, based on our experience advocating for thousands of domestic violence victims, that posting case files on the Internet, making generally available to the public without significant restrictions would really endanger our clients. And I'd like to explain a little about why we're so concerned.

Let me outline my basic reasons and, as I have time, I'll try to elaborate on some of those points.

First, we find in our work, batterers and stalkers are extremely obsessed with monitoring and controlling their victims. They terrorize victims over many years, even after their victims have managed to escape and often spend countless hours really trying to track down these victims, using any means available to them.

(Continued on following page.)

MS. SUNGHEE SEO: (Continuing) Second, we find in our work that the batterers and stalkers of our clients are often very savvy technologically; and we have no doubt if sensitive material is made available to them on the Internet, they would spare no effort to harass, track down and endanger their victims using that information.

Third, as referred to previously, while records from Family Court and matrimonial proceedings are not available to the public at this point, court files from criminal and other cases, other civil cases are publicly available. And one of the difficulties that we had in, sort of, formulating recommendations is that while there is a category of information that is more sensitive and obviously harmful like name, address, phone number and things like that, identifying information, in a large number of cases I think it would be difficult to predict beforehand how some of the information in seemingly unrelated cases would be used as a weapon in the hands of abusers; one scenario being that you are not a victim of domestic violence stalking at the time that you were involved with the court system in a case and then you become a victim in the future.

Then finally, a point that many people -- you

know, once this information is out there, it would be really difficult to undo the damage. Just to give you an idea of the number of women we are talking about, one in four women in the United States are victims of some sort of violence. That translates to about 26 million women nationwide. And according to the National Institute of Justice, about 8 percent of women are stalked sometime over their lifetimes, and that would translate to about 8.2 million women. So we really are talking about large numbers of women. And you have to take into account children because often the stalkers and abusers also attack their families and lawyers and other support community members. So this really is a problem. I think it really affects all of us.

I would like to give you just two stories of women who have stories that are typical of the types of clients that we encounter. The first one is J.S. -- and I give you these examples to give you an idea of how resourceful and persistent and aggressive the abusers that we see on a daily basis are. The first woman was physically and emotionally abused by her husband. Besides beating her regularly and forcing her to have sex while he slapped and verbally abused her, he isolated her by preventing her from working,

forbidding her from leaving the house without his permission, calling her multiple times a day from his workplace keeping tabs on her, becoming angry if she talked to her friends or family over the phone, and not giving her any money so she would have to ask his permission to buy such incidental things as toothpaste or feminine hygiene products. When she fled the house, he called every one of her relatives and friends until he eventually tracked her down.

I give you this example as, sort of, a typical example in terms of how these -- you know, the lengths that these abusers will go to track down their victims and to sort of illustrate why we really have no doubt that if sensitive information is made available on the Internet, these abusers will misuse them.

The second woman S.H. was a stalking victim. She was stalked by someone she met briefly while volunteering at a community organization in South Korea. He followed her to her home and asked her out. When she said no, he started stalking her outside her home. He found out her work phone number and called her incessantly at work. He also stalked her at a workplace. After about a year S.H. moved to New York to pursue graduate studies. To her dismay, her stalker found out the name of her school in the U.S. by

contacting a fellow volunteer at the community organization and took a plane and came to New York after her. He showed up at her school in New York causing her great fear. He also found out her phone number, e-mail address and home address over the Internet and began to harass her. After a while, S.H. became so scared that she moved to a new location. But she is still afraid her stalker may again succeed in tracking her down.

About 10 percent of stalking victims relocate, actually physically relocate to get away from stalkers because they find that's really the only way to make the stalkers go away.

Another point that I would like to highlight -- though I elaborate on each of the points in my written testimony -- is again this point that it would be difficult to predict beforehand exactly where some of the sensitive material that would ultimately harm victims would be in the case files. So, for example, if a woman is battered and relocates, she is stalked and she relocates and she gets a new job in a new location and then she is terminated after she complains to her supervisor about sexual harassment and decides to seek redress in the court, her employment files which contain the name and address of her

employer would, you know, if these files are made available on the Internet, would become available. Her batterer/stalker who is intent on finding her may spend, you know, one night out of every two or three days looking for her on the Internet. If he comes across this case by just putting in the search code of her name, he would find out who she is working for now, and it would be much easier to track her down.

In a similar case, we have seen people where not only does he find out her address and try to track her down and begin to threaten her that way, but he will threaten to humiliate and embarrass her by posting all the details from her sexual harassment case on the Internet and by mass mailing the link to her friends, family and colleagues.

This is, sort of, an Internet hypothetical, but we have seen abusers who go to great lengths to create elaborate websites where they gather information about the purporting sex lives, and the abusers then try to either mass mail to people he knows or to some of her friends to embarrass her.

And again, sort of -- I am giving you these examples to really underscore who these people are and why we are so concerned.

MR. ABRAMS: Your time is up, ma'am, but I do

want to save time for my colleagues to question you.

Could I ask you generally, what is your recommendation to us, what would you like us to recommend to the Judiciary about this subject?

MS. SUNGHEE SEO: Two points. The first point is that we have had a hard time coming up with, sort of, specific recommendations because one of the points that we are making is that you are not really going to provide adequate protection by just sealing, you know, domestic violence cases or matrimonial actions and things like that. As Charlotte Watson mentioned, New York does have a statute that protects the victims of sexual crimes, but that doesn't apply unless the perpetrator is prosecuted under very specific sex crimes under the Penal Law. So that's the first point.

Having said that, I think there are categories of information that would be more predictably harmful and would be relatively easier to isolate, like name, address, social security number, you know, telephone number and the like. And in terms of some of the suggestions before about redacting such information and then giving a few days so that people can check for clerical mistakes and things like that, I think those steps would be -- I don't think it would be

a complete remedy but it would be helpful.

I do want to note that many of our clients are pro se. We help them, but they proceed on a pro se basis.

There was a question from the panel before about, you know, whether it would make sense in individual cases for the woman victim, since she might know at that point that she has, you know, been a victim of domestic violence or stalking, that she could potentially be in danger, and why don't we have her make a petition before the Court on a case-by-case basis?

My response to that is, you know, yes, an opportunity to do that could be helpful in some cases, but in a case, especially of a woman proceeding pro se, I think in many circumstances she just wouldn't have the resources or the foresight to really be able to make such petitions and, frankly, persuade the judge that what may seem on its face harmless material could potentially harm her. Also, again, the point that if you have never had these bad experiences at that point but become a victim in the future, obviously it would be really hard to predict what is going to be done with some of this information by an abuser in the future.

MR. ABRAMS: You mentioned your prepared

statement, and I want to let you know and everyone know that all the prepared statements will be set forth in the record of these proceedings. They will be on our website together with a transcript of the testimony. So people will be able to read the entirety of what you prepared even though we are necessarily cutting you off to some extent in terms of presenting it all.

Any questions?

MS. BRYSON: Once again, I just want to be sure that we understand the scope of what is being recommended.

Do you agree with the previous speaker that we really should not have -- it is almost as if we shouldn't have any electronic filing of court papers, or are you prepared to say that there should be some electronic filing but that there should be a distinction between what is filed electronically and what is filed in the courthouse? It seems that the previous speaker was perfectly comfortable with that information in the courthouse. But it seems to me if they know where the person lives, they can go to the New York County Court, do a search on the person's name, and if they are that dogged and that determined, they can hunt them down and locate the same information on paper. But there seems to be a distinction then

between that and putting it out electronically. What is your group's view on those distinctions?

MS. SUNGHEE SEO: On the first point, the first question, I realize that this is not a black and white matter. We are talking about degrees of danger and balancing it against other interests. And so -- I mean, in a spectrum of possibilities it is going to be better if court records, for example, are defined more narrowly than was defined in the national guidelines. If there is more restriction in some cases to who can access these files electronically, whether there is a fee, for example, all these things, I think, will matter. The worst scenario being you make everything available to everyone for free, you know, with a very broad definition of "court records" so that it even includes exhibits that are not entered into evidence. I think that was one of the suggestions or considerations within the national guidelines. So I would urge the Commission to think about domestic violence victims and stalking victims as you consider balancing these interests. I realize that, again, you know, it is not really a black and white matter, but as you balance these interests, I think there are ways, maybe by going to a multi-tiered system in terms of the type of cases that would be available electronically

and to whom, you know, that if you go -- if you sort of divide up the cases between categories, the highest protection being given to identifying information, I think that would probably make it safer. Although I think one of the points we are making is that it really is difficult when we think about how this will affect our clients, it will be difficult to predict -- you know, we can't say if you get rid of this, this and this information our victims will be safe.

On the second question, we read the guidelines that the Commission published and understand that it is not your job right now to reconsider existing policies, and so the testimony does not include our information about what to do about the public access rules on paper court filings.

MR. ABRAMS: Thank you very much.

Mr. Solomon, you are next.

MR. SOLOMON: Thank you. I am Richard Solomon. I am a graduate from Georgetown Law School of 1985. I am a published author. I wrote a book called Winning in the New York Small Claims Court, and I regularly teach people on how to use the public courts and public records to get information in their own cases. And you would think that I would be very much in favor of unfettered access, but the truth is I am

not, probably because of my own experiences.

Even though I teach and talk about public records, there is a big difference between taking your ID, showing it to somebody at the clerk's office, signing a little form, having your face there, and telling the clerk, I want this file. It's just like the difference with check fraud. If you have to go to the bank and actually cash the check, you are on video camera. Because when you go into the bank, you are exposing your own problems.

One of the problems that we have in the litigation system is that there is so much private information -- and I couldn't help agreeing 100 percent with the Attorney General's office.

I brought with me a Bill of Particulars from one of my own medical malpractice cases from 1995. In this case, just like in every other med mal case and every other case, they ask your salary and your date of birth. And over here they ask for a social security number, and they ask for your resident address. It is all right there. And I have reluctantly never filed these kinds of papers in the courthouse because it is not required. And I do that to protect my own clients. Also, it is to protect me. I don't want to be responsible for revealing the privacies and intimacies

of my clients who come to the court system. And they shouldn't have to pay for motions for protective orders, which are expensive. Invariably there will be a fight between the lawyers and clients about who is getting paid for their privacy. After all, I brought a lawsuit and now I have to file a protective order. There goes a couple of thousand dollars because you have to make motions and it has to go on the record. There is an appearance and whatever. They don't want to spend a couple of thousands on that. So all this information is out there. And I agree with Ms. Watson, I think, who talked about the difference between a filing cabinet and everywhere.

One of the things we really need to think about is 9/11. No one mentioned anything about terrorism in New York. Since there are people out there who are committed to jeopardizing the safety of public officials and whatever, who is to say that when officials or various people are the subject of litigation, that somehow when an officer of government has to give a personal piece of information that that somehow is not going to be jeopardizing their own personal safety or their family's safety or using people to get to other people? It truly is different to be able to go to a courthouse in person, hand in an

ID and say, I want this specific file, to actually go there. It is another thing for anyone around the universe to anonymously and for relatively no money access everything about you. The criminal justice system will not be able to track those people down in foreign jurisdictions. I agree with the Attorney General's comments on that point.

The one thing that no one has talked about -- I will raise this hypothetically -- is do you even know what it is like to be the victim of identity theft? In 1999 one of my oldest clients, a really nice man named Mike, had his identity stolen. I was his lawyer and figured I would help him out. The amount of damage it did to him, a nice elderly man, was unbelievable. Do you know what it took to fix his credit, to get to the credit reporting agencies, to get the information cleared up? Do you know the cost involved in that? Now, I was his friend so I basically did it for nothing. But if he had to pay for it, it would have been enormous. It probably took 15 straight hours to hunt down the right places, explain, show his real identity to everybody and undo the mess. That was 1999. That was only one case and I figured okay. But last year I had about fifteen cases. Not because I am an expert in identity theft, but it is because it

really is exploding. It is a very easy crime.

I wrote the article entitle, "Protecting Yourself from Identity Theft." Even the Attorney General in the State of Arkansas talks about this in their website. All you need is a social security number, date of birth, and maybe even a phone number, and you can grab someone's identity. It is that simple.

Now, of course, I went on Google on the Internet and looked up "identity theft" and with a date of birth found -- you can locate anyone's e-mail address, find unlisted numbers. You can discover new and old romantic interests, verify death, marriage property, snoop for secrets your neighbors don't want you to know, locate hidden assets, and check for unclaimed monies in your own name.

Well, the problem is identity theft is exploding. If you looked at the New York Post from this week, you would have seen an article about identity theft causing about $35,000 worth of damages when a loan was taken out. And the question is: Once you let the toothpaste out of the tube, is it a problem? You betcha.

Look at the list from the government's own website on what you have to do to clear the problem.

You have to contact all creditors involved, file police reports. You have to contact fraud departments. You have to make a victim statement to your own credit report. You have to then regularly check your credit report. And most likely, if you have credit, you have to hire an attorney to clear it up because I have seen the resistance in clearing this up because there are a lot of problems out there. Debtors say their identity was stolen just as a way of delaying bankruptcy.

Just in closing I have some quick points. One is that the burden on attorneys shouldn't really be made greater. We have enough problems with compliance and CLE requirements. And to become the keepers of whether information is going to subject our clients to identity theft creates malpractice problems for us. If anything, we are going to have to make motions pro forma in every case to preclude things to protect ourselves. That is going to cost money. And the clients won't want to pay for it, and the court doesn't want to see thousands of motions on identity theft. They will be flabbergasted.

What probably really makes sense is to keep the system as kind of what we have but enhanced somewhat. What we have in the courthouse is fine. I don't have any problem with that. What I do have a

problem with is everything being on the Internet. If we really need to have information out there, people can hire people to go down. The gentleman from Newsday was talking about how they have to send people down. Well, they have runners do that. If you really want the information, you can go get it. The real difference between getting that information and getting it from Germany, Switzerland, from Osama Bin Laden is that somebody has to go in person through metal detectors and hand an ID to someone.

One of the things I criticize the court system for is when you fill out that white sheet at 60 Centre Street and hand it in, or the yellow one at 111 Centre Street, you just fill out your name and you hand it to somebody. No one even checks to make sure that's your name. If you really wanted to, you could put down Bob Jones, Lake Success, New York. You don't really put an address and they will hand you the file anyway. If anything, there should be some check inside the court building like showing a driver's license or your secure pass. All attorneys now have the secure pass. That was one of the post-9/11 things, a security enhancement. That should be recommended. When people access the public records inside the court building, show some identity, some real identity, provable

identity. So if the information taken out is misused, you know exactly who it was. Otherwise it is a bunch of scribble and they throw it in a big pile.

MR. ABRAMS: Mr. Solomon, your time is up.

Does anybody have any questions?

MR. KOVNER: I take it it is your position that the present system could be tightened but it works pretty well, and the court records ought not be remotely accessible at all.

MR. SOLOMON: Well, it is not that court records shouldn't be remotely accessible at all, but what do you need is maybe the complaint, maybe an answer and an opinion.

MR. KOVNER: But beyond the sort of skeletal --

MR. SOLOMON: Why do Bills of Particular really need to be on the Internet? Why should the court system scan all the documents, the motion practice? If I was in a motor vehicle accident, what good does that serve the public, all my private information about my back injury or whatever is in there? If anything, the insurance companies will want to look at it. And the telemarketers are going to send me prescription pain medication. Don't we have enough of that? Look at all the spam you get. Mortgage rates

have never been lower, you get that every day. All the things about personal things that they send, legal marijuana. It is only going to be enhanced by the fact that the telemarketers, insurance companies and identity thieves are going to be out there harvesting the information and reselling it.

MR. ABRAMS: Thank you very much.

Ed Klaris.

(Continued on next page)

MR. KLARIS: Good afternoon. I'm Edward Klaris. I'm here on behalf of the New York State Bar Association's Media Log Committee. Not, as stated in your form, the New Yorker; although I work there.

I thank you for permitting me to make a presentation on behalf of the Media Law Committee of the New York Stat Bar Assoiation.

The Media Law Committee is comprised of attorneys who specialize in issues relating to the First Amendment and privacy. We represent news organizations and reporters and we firmly believe that online access to court records will allow for more quality journalism and improve the public's knowledge of the court system and court proceedings without comprising New York's protection of privacy interests.

Currently, searching court records is something of an ordeal; many people work during the hours when records are available for examination and many work or live miles away from the courthouses. Tracking down the correct courthouse in New York City can be overwhelming for reporters and members of the public trying to find information about particular cases.

Electronic access to court records would

allow for meaningful and efficient searches of important information about attorney and medical malpractice, deadbeat parents, corporations charged with fraud, products claimed to be defective and other information that is currently very difficult to find.

Moreover, there are many organizations beyond the mainstream New York press that, with sufficient access, could engage in more direct public oversight of the courts and contribute significantly to discussions of public issues.

Alternative news organizations, out of state newspapers, broadcasters and Web sites, public interest organizations, lawyers associations and many others could make valuable use of these records.

An on-line database would give private citizens the same access, as the Supreme Court noted in the Richmond Newspapers case, "People in open society do not demand infallibility from their institutions, but it is difficult for them to accept if they are prohibited from observing.

Making court records available on electronic networks would increase the fairness of the court record sytem facilitate greater scrutiny, meaningful access to important cases in the system and continue to enhance the tradition of openness that is part of the

culture and law of the New York court system.

These benefits are best achieved with full-text searching and easy access to all cases rather than having to input the name of the case to conduct a search.

In the context of electronic access to court records, the doctrine of "practical obscurity" and concerns over privacy are misleading and do not apply. The current system of open court records works quite well and it would be a mistake to impose a new system of court secrecy in which categorical and preemptive determinations limit access. These decisions are best made on a case-by-case basis, upon a motion by the party seeking to either seal the records entirely or to curtail their availability.

The Commission is by now well aware that the U.S. Supreme Court made clear in Nixon v. Warner Communications, that the public enjoys a common law access to judicial records. The "presumption of openness" can be reversed only by showing an "overriding interest based on findings that closesure is essential to preserve higher values."

New York Rule of Court 216.1 requires judges to consider not only the parties but also the "interest of the public" and provide a written finding of "good

cause" before sealing court records. The rule undergirds New Yorks' strong public policy in favor of open court records.

New York courts over the past decade, have consistently relied on 216.1 to deny requests to seal court records even where all the parties were in favor of sealing the case. For example, in a case decided in 2001 involving the proprieties of an estate accounting and personal finances, the First Department upheld the Surrogate Court judge's denial of a joint motion for protective order to seal the settlement agreement.

In that case, named In re Hoffmann, the court, in denying the motion, noted that even where all parties agreed to seal the records, "Confidentiality is clearly the exception not the rule and the court is always required to make an independent determination of good cause."

Would the Appellate Division's analysis in In re Hoffmann or other cases change if court records were available electronically? We do not think so.

For decades, New York courts and the legislature have rebuffed privacy advocates' attempts to create generalized privacy torts, such as one for publication of private facts. On the other hand, where the benefits of confidentiality in court records

clearly outweigh the presumed benefit of transparency, New York already has several rules and statutes to cover this.

For example, State statutes currently permit courts to seal records in family law, matrimonial and juvenile cases. The New York Public Health Law and New York Mental Hygiene Law are the principal statutory sources of New York law that require health information to be held in confidence. Additional health-related statutes cover specific situations, like HIV and AIDS patients, disclosure of health records in litigation and the collection of statistical information by various governmental agencies. These rules would continue to apply in the electronic environment.

Congress has also passed a number of federal laws that protect certain kinds of information. HIPPA protects health information. Gramm-Leach-Bliley protects financial information. FERPA protects education information. COPPA protects information about children. The Driver's Privacy Protection Act protects drivers' license applications and information. And there are more.

With all these privacy-related laws, the chances that highly confidential information would be filed with the court in litigation have been

significantly reduced. Even where such information may be turned over in discovery, only a tiny percentage of discovery information and materials are actually filed with the court. And, of course, the first amendment does not require that non-parties be given access to discovery material that has not been filed in the clerk's office.

Perhaps the greatest fear of electronic access to court records is that information may be used in identity theft, where a person's social security number, credit card and bank account information are appropriated and used illegally. While identity theft is a serious concern, blocking access to certain electronic records is not the answer. Strict enforcement of the existing criminal laws and the proper implementation of state and federal privacy legislation will deter such behavior.

In addition, there's no evidence that court records would ever be a good place for would-be criminals to obtain social security, credit card and bank information, while there's ample evidence that such information can be obtained elsewhere on the Internet and through criminal rings that collect the data from co-conspirators at banks and retailers.

Speculative and remote fears about deviant

behavior should not cloud this Commission's recommendations. This Commission should support electronic access to court records and endorse the current rule of law and good public policy in New York, which already properly balances privacy in court records with the First Amendment.

In conclusion, we suggest that this Commission recommend the continued implementation of the New York court system and that New York court records be made available electronically. Doing this will increase the efficiency of the judiciary, while also democratizing the system, giving citizens journalists and other interested parties access to information they need to monitor the fairness and efficacy of the courts.

It's worth emphasizing that we do not request New York expand the types of records available to the public. Rather, we simply would like New York to provide broader and more efficient access to records that are already there.

MR. ABRAMS: Thank you.

I'm interested in your reaction to the conclusions and the concerns expressed by the last two witnesses who pointed out that while Family Court proceedings are closed, criminal and civil cases, of

course, are not. They expressed concern, therefore, about providing information that might make it easier for stalkers or others to commit criminal acts on individuals whose names were mentioned in court records.

MR. KLARIS: The Media Law Committee, those kinds of hypothetical concerns are unfounded because there's really no evidence that anybody would use the records for that purpose. And also, it seems there are many other ways to get the information as well.

MR. LELYVELD: Your argument is the the cat is out of the bag and therefore it's not a concern? Why wouldn't they use it, if it were easily available?

MR. KLARIS: The testimony that was stated before pretty much indicated that the reason people are stalked or found by predators is that they called the families and get the numbers through family and friends. They used means of obtaining the information typically that is also available publicly and not from the public records.

Court cases involving people who might be victimized are probably relatively rare. And there's no systematic way of knowing that there's a certain case that a person has been named in. It would be much more logical for a potential predator to call the

family or call the friends who they know to find out where this person is.

MR. LELYVELD: Would you apply the same argument to the identity theft concerns that have been mentioned?

MR. KLARIS: Yes. I think there are other places that collect that kind of information in broad ways where there's hundreds or thousands of credit card accounts collected by retailers and banks where it's much easier to get that information and use it in identity fraud as opposed to piece together particular cases where somebody's identity or information might be stated some place in a record. That seems far less efficient for criminals than actually going after broad based databases, which are already available.

MR. CAMPBELL: In following up on his question, in attempting to locate someone if, in fact, the court system implemented a searchable database that was discussed earlier, wouldn't it be easy just to plug in the name, address or name of someone and locate it very easily rather than having to go to a particular county?

MR. KLARIS: I think that the on-line white imagines are probably the easiest way to find somebody.

There are many other ways to get somebody's

information, including calling their area code and 555-1212, which will typically give someone's phone numbers.

Where somebody's unlisted because they are afraid of being stalked, which is, of course, a legitimate concern, if somebody has that problem, I can imagine if they are involved in litigation where that kind of information might be in the public record, their lawyer would work hard to get that information sealed.

And there may well be good grounds to seal it. But to do it in a preemptive way, this Commission, to suggest that that kind of information should be across the board exempted from filing in the public court system seems, to the Media Law Committee, to be a mistake.

MR. CAMPBELL: Do you feel that people will now tend to move away from using the court system to bring their grievances to be resolved in the Court system because of this open access to court records?

MR. KLARIS: No, not at all. The Media Law Committee thinks there should be no reason to change the way litigation strategy is, other than perhaps in the beginning there might be some more motions to seal records that people are concerned their corporate

documents might be an open -- get more scrutiny in an electronic environment. I don't see any evidence that there would be a change in litigation strategies --

MR. CAMPBELL: I'm not saying a change in litigation strategy. What I'm asking is if someone is afraid of their medical records being posted on the Internet, would they be a little less inclined to commence an action and have their medical records and bill of particulars and so forth and so on be posted on the Internet?

MR. KLARIS: I have no idea.

MR. GLEASON: I'd like to ask you if you could comment on the timing of when you think a record should be absolutely open and whether that perhaps could conflict with what you said about a sealing motion because, presumably the sealing motion implies that there's something out there that you want to keep confidential. In an electronic filing system, you might actually have something out there and publicly available to the world before you even had an opportunity to make a sealing motion.

MR. KLARIS: From my understanding of the way the system works, when you're going to provide something to your adversary in discovery that you believe is confidential, you can move to have that

information sealed prior to the discovery.

MR. GLEASON: That's true. But there are sometimes situations where the information would be used in a court filing. It may not even have come from discovery. It might have come indirectly through discovery and the adversary, who has the interest in confidentiality, might not immediately appreciate that somebody else is going to put this thing in a court document and file it.

Would you agree that there's a reasonable expectation that somebody should at least have an opportunity to argue for confidentiality before it's on the Internet?

MR. KLARIS: No. The Media Law Committee agrees with the Newsday statement earlier that once records -- court documents hit the courthouse and are publicly available in the clerk's office, they should also be publicly available on-line and I think the way the system currently works, there's no delay when you file records in the courthouse.

MR. GLEASON: That's why we want to know if the Internet is different because of the fact it's practically obscure in the courthouse but when it's on the Internet it's immediately available to the world.

Should we appreciate some difference because

of that?

MR. KLARIS: We think there should be no difference. And you're talking about a miniscule number of cases which, in fact, this Commission we don't think should let the tail wag the dog, in terms of the public benefits to media, public access to Court filings and permit some hypothetical fears about a tiny number of cases that might have some private information where the parties haven't gotten a chance to seal the information to wag the dog.

MR. GLEASON: Would you also take the position that the critical event that gives constitutional protection is your adversary filing it as opposed to perhaps some later point in time when the judge actually deals with the issue?

MR. KLARIS: We believe that at the time you file the papers, they should be available publicly.

MR. GLEASON: In other words, your adversary will control the timing of the attachment of the world's right to know?

MR. KLARIS: Right.

MR. KOVNER: Mr. Klaris, would the Media Law Committee object if we were to impose a recommendation for remote access, a requirement that somebody log on and provide identifying information, just as many

courts do, in terms of when you get a file from the New York County courthouse?

MR. KLARIS: The Media Law Committee believes that the rules that apply on-line should be in tandem with those that are being instituted in the courthouse.

MR. KOVNER: So if there's a requirement of identification that some courts impose, there's no reason why that shouldn't apply to on-line access.

MR. KLARIS: Correct.

MR. KOVNER: You would agree, would you not, that the information that would be available on-line would be far beyond that which is available today in the courthouse?

MR. KLARIS: Because of full text searching, the information would be more available. The benefits to being able to search the record are so great, because you can track down things like I mentioned in my statement -- defective products, abusing spouses, dead beat people in society, which is really important information.

That greater access, on balance, is going to far outweigh any kind of harm that may occur, speculative and hypothetical harm that may occur.

MR. CAMPBELL: I want to raise one issue.

This is not a hypothetical.

Under the new HIPPA law, when the patient fills out an authorization, they have to specifically delineate what records are being released. They have to indicate what purpose the records will be used for.

Following up on what Mr. Gleason said, if a defendant makes a motion for summary judgment, let's say, in a personal injury action, threshhold motion, they now have the right to attach all medical documentation to that motion. Under the HIPPA authorization, they are given authorization to receive those documents for a limited purpose.

Now you're going beyond the scope of that authorization because now you're publishing it on the Internet. If it is made available at the time it hits the clerk's office, as you suggested, how would you balance that?

MR. KLARIS: I would balance it on a case by case basis. So would the Media Law Committee, on whose behalf I speak.

We believe that you can -- the plaintiff's attorney, in a medical malpractice type case or case involving private medical information, where the information itself is put in issue by the plaintiff and the question of their health and well-being, whatever

it may be, is in issue, if in fact there's a concern about it being available publicly, the plaintiff's attorney will have perhaps good grounds, depending on the case, to move for a protective order.

MR. FARLEY: If I could ask you a question that probably will sound like it's coming from left field and that's about the copyright status of materials that might be introduced into the court record.

If an article from the New Yorker or a book or something of that sort is included as an exhibit to a court filing and it's just left in the court file, that is a different copyright situation than if it is then reproduced and disseminated on the Internet, which might result in a publication or public display.

What thoughts would you give us about dealing with items that may be copyrighted or otherwise be protected and what the court should do with such documents? Should they be disseminated on the Internet? How would you over come the copyright issues?

MR. KLARIS: I'll answer as an attorney and from the New Yorker, not from the Committee.

That's a good question. The way we handle it and most copyright holders is that you worry about the

infringer. You don't worry about the possibility that your magazine might be scanned and is available, because you can't stop the scanning.

We would always go after those who might be using it improperly, not the court file that was available whether electronically or in court.

If it goes from there to a Web site that is distributing it widely for commercial gain, in our opinion improperly, we would go after that Web site or individual publisher.

MR. FARLEY: From the prospective of the court system, the court system would be maintaining this on some database and making it available. The court system would be the entity disseminating the copyrighted material. Are you saying that you would be suing the court system?

MR. KLARIS: It's a good question. One could analyze it in many ways. Each time somebody logs on to the system, one could argue it's a copyright infringement. I haven't thought through that scenario. It's difficult to answer.

MR. ABRAMS: One possible result would be it would be treated -- consistent with your testimony -- in the same way as each time someone went to the courthouse to look at the book, or it was a magazine

article, to say there was no violation by the judicial system in allowing viewing of the material. But if someone went out and then published it or used it or abused the copyright --

MR. KLARIS: The difference is, there's no copy when you're looking at that. It's the copyright you're talking about. So if someone goes to the courthouse and makes a photocopy in front of the Court Clerk, is the Court Clerk and courthouse somehow contributing to the infringement because they make available a copy machine? That seems far-fetched.

It's the same with the hypothetical with the courthouse being responsible for the collection to see on-line court records.

MR. ABRAMS: Thank you very much.

MR. KLARIS: Thank you.

MR. FREEMAN: I am George Freeman, Assistant General Counsel of the New York Times Company.

I would start today by urging the Commission to ensure we do not inadvertently use the opportunity technology is giving us to take a step backwards. What I fear the most is that because of the ready access computerized judicial records would bring, a possible, and certainly ironic, result might be to tilt the balance we now have with respect to all court records, hard copy or electronic, to more closure, to more redactions and to more sealings. While our privacy interests certainly ought to be respected, they are amply taken into account in the balance we have in the current regime. With the increased focus on privacy interests which the electronic world inevitably brings, we should be vigilant to ensure no pushback on the openness to judicial documents which are the very hallmark of our wonderful judicial system. The very possibility that because of the opportunity to disseminate judicial records through the new technologies, access to records should somehow become less public and more shielded is not only ironic, it is antithetical to the very advantages which the public go gain from the Internet.

It should also be borne in mind that any

regulation aimed at electronic files in relatively short order may amount to regulation of all court files, as paper records may well disappear entirely in our lifetime. Any tilting of the balance between privacy interests and openness towards the privacy end of the spectrum, even only with respect to electronic records, may achieve the very opposite result of the advantages to public access which the new technology offers. Since it is possible that in the future the only files that exist will be computerized, we should be wary of creating new rules for that medium which differ from those currently applied in the courthouses, because ultimately the Internet may be the only game in town.

Assuming, then, that we agree that the new technologies and this new initiative should not result in the diminution of openness in our courthouses, what are the advantages of transition to electronic case files? The practical importance of the change could not be overstated, and in most cases it is entirely uncontroversial. A paper copy of a document filed in court, (1) requires a trip to the courthouse to inspect or copy, once one figures out the correct courthouse to visit; (2) is available for inspection and copying one person at a time; (3) is available only during business

hours; (4) may be archived in a dusty warehouse and hard to find years after it is filed; (5) may be in use at trials or in chambers and not available in the clerk's office; (6) typically can be copied only by very patient people with vast amounts of pocket change on an antiquated photocopying machine; (7) must be manually searched for relevant information by, generally, uninformed agents for the parties actually seeking the information; and then (8) only truly retrievable if the party knows the exact caption or case number of a specific litigation.

Clearly this is only for the very determined and very resourceful. Electronic records solve all these problems and we applaud the judiciary for its efforts in this area.

The notice for these public hearings suggests a limited number of areas in which restrictions on electronic access are being considered where no limitations currently exist with respect to paper records. We view these suggestions as unwise, unwarranted and constitutionally suspect.

First, there are adequate measures available for litigants and others to request the sealing of such information in the current procedures, although the standard is, properly, a difficult one to meet. What

seems quite problematic is to set up a scheme of discriminatory access where the rules with respect to hard records are different than those with respect to electronic records.

Before discussing why we believe the same rules ought to apply to both media -- that is, why any system in which two standards don't mirror each other is unwarranted -- my statement makes the points I will skip right now. That there are an awful lot of advantages to openness in our system such as those cited in the Richmond Newspapers case. And I know the Commission is well familiar with that, so I will pass on that. But I think it is important to note that the advantages of openness are all the greater if they truly can be brought to the public rather than only to those members of the public with the time, the knowledge, the inclination and the money to actually go to the clerk's office, a place where I, a New York litigator of 27 years, still fear to tread.

But beyond the advantages of openness set forth in Richmond Newspapers and the other Supreme Court cases, I would make this point: That many times, given the tension between privacy interest and access, and indeed in the now 16-year battle in the state about cameras in the courtroom, the participants in these

struggles forget about what we have in common, and that's an interest in the fair workings of the judicial system. But I would submit it is more critical how the public perceives the judicial system as working fairly. That really ought to be paramount in any inquiry such as this, particularly in today's environment where lawyers, judges and the judicial system in general are not thought of terribly highly by the public, not much more than even lowly journalists. Whether it be O.J, bribe-taking state judges, the perception that LA Law is the law, whether it be lack of understanding of the adversary system and why the defendants are entitled to due process, the judicial system is not held in high esteem. And for the very reasons articulated by Chief Justice Berger for a unanimous Supreme Court, more openness is one way is to improve that very paramount problem.

There has been testimony about privacy interests, and we believe that much of the fears of openness on the Internet is more speculation than reality. And we underscore, especially from a newspaper's point of view, the great advantages of electronic access and full text searching capabilities.

First, it allows better reporting on the judicial system. A paper like The Times reports on

cases throughout the very large Empire State from Dutchess County, home of the Tawana Brawley case, to land issues in the Adirondacks. And timely and accurate reporting, relying more on court records rather than on the spin of lawyers and phone calls would be greatly aided if a reporter in New York City had access to a court file in Poughkeepsie.

Second, electronic access would improve reporting in a variety of matters. As one who comes from a building currently in turmoil, a problem created in part by the lack of checking with respect to an employee's background, it seems obvious that the ability and the press and the public to have better access to check upon the background of potential employees is a good thing. Whether it is a newspaper being able to get access to court records without a candidate for the judiciary or any person running for public office, for a newspaper or any employer to have the ability to more easily check the true and sworn background of potential employees in executive positions, there is a myriad of advantages to get more information more easily about such high-placed people in sensitive jobs, or, for that matter about the past history of those charged with crime. Moreover it is not just about people. Newspapers could better report

about companies deceiving the public, about products claimed to be injurious and so on.

I note that the New York Times very recently won a Pulitzer Prize for -- by Clifford Levy for his reporting on abuses in private nursing homes. That reporting was largely based on very, very painstaking research into a whole number of court files and in a wide variety of courts in the state. That reporting would have been more quickly, more efficiently, and more deeply had electronic searches on the owners of those homes and the homes themselves been available.

Against these types of advantages it is hard to see disadvantages of intrusiveness. First, one who wants to get background about an individual can probably do so without this new initiative. The Internet already provides access to personal information about people often well beyond what would be filed and not redacted or sealed in court. And in a very real sense, the cat is already out of the bag.

Second, the balance has already been struck with privacy and openness in the standards which currently exist for protective orders, seals and the like.

Third, of course, is the case that in many of the fora in which potentially private information

exists, the law currently permits courts to seal such records, such as in family law and juvenile cases. And I also point out in another area often mentioned as one area of concern is the bankruptcy courts. They are federal and beyond the purview of this rule.

I close by saying we believe the balance that exists now properly takes into account privacy interests as well as the great public advantages to openness, and that in embracing the new technologies we should not alter that balance but should welcome the added public access the Internet brings. To the extent the Commission believes it should not exactly mirror the current rules with respect to paper documents generally, we think they should. We submit, consistent with the Supreme Court cases, the burden must be on those favoring more restrictive rules to show a compelling reason based on real evidence and not mere speculation on why a system that discriminates between media should prevail. If the Commission believes such a burden has been met, the exceptions should be extremely narrowly tailored to include only a closed specific set of so-called identity data -- social security number, credit card, bank account and nothing else -- and should be blocked from access not automatically but only upon appropriate showing.

I reiterate, we do not think that any such discrimination is warranted, but if realistically the only way to achieve the progress the Internet makes available is by such a narrowly and clearly-defined restriction after clear evidence has been shown that it is substantially probable that real damage will occur, we could understand why such a trade-off might be made.

MR. ABRAMS: Thank you.

I would like to ask you the same question I asked Mr. Klaris about the testimony of the two witnesses about stalking and the avoidance of domestic violence in which they both testified that while Family Court proceedings may be closed in New York, criminal and civil proceedings in which potentially sensitive information is revealed are not. And on that basis, at least in part, they urge that we ought to avoid recommending anything which would permit almost any information which could be a benefit to a potential stalker to go on the Internet with the assistance, at least, of the Office of the Court Administration.

MR. FREEMAN: Let me start by answering that with a short anecdote that Mr. Kovner's presence reminds me about.

A month ago we were in a trial sponsored by the Office of Court Administration. Judge Kaye was

there and Judge Rosenblatt of the Court of Appeals was there. And the hypothetical they created for that particular occasion was one which really focused on this exact problem and on the issue you are dealing with. The hypothetical itself was of an old boyfriend stalking an old girlfriend through records he somehow obtained through the court process. In fact, the information came out of records from Bankruptcy Court, which isn't even within the purview of the state court system. So even in the hypothetical created to make the point, there was a problem here. They seemingly weren't able to make the hypothetical with the real facts open to us because since Family Courts are closed they took a bankruptcy case that had the private information that supposedly was the genesis of the stalking, which isn't even in our state court.

So I do think that the harm is speculative, and I have to agree with Mr. Klaris that so much of this information is already available on websites and on the Internet, that the thought that it somehow becomes really beyond the breaking point because there will be a website with court information, I just don't think holds. Also I point out -- and I really am not an expert in this, but my understanding is that we have the same kind of rhythm, same kind of scenario with the

Driver Protection Act. That was essentially passed because of a fear of stalking and a supposed incidence of one situation where stalking of an actress occurred; although it is my understanding that occurred not through the Internet but through a private investigator.

So obviously the incidents which the witnesses gave are terrible things. I do think, though, that a number of cases where it is an old boyfriend stalking an old girlfriend, where that old girlfriend lives is easily obtainable by the old boyfriend through many, many means. And I don't think that it being available because maybe the old boyfriend is involved in litigation and so maybe the address is in the court record, I don't think that is the way we are going to find where the people live. It is kind of self-evident from much more easy methods.

MR. GLEASON: I would like to ask you the same question I asked Klaris.

Would you also take the position that constitutionally the instant your adversary files something with the court it becomes a matter of public record; and are you at all discomforted by the prospect of having your adversary, who may have relatively wide access through discovery or through other means, having

the ability to place within the public domain whatever they might wish to place there?

MR. FREEMAN: My understanding, and certainly the procedure in New York, is that for the most part discovery documents are not part of this inquiry because we are only talking about those documents gotten in discovery relevant to a motion being filed.

MR. GLEASON: Right.

MR. FREEMAN: Not discovery in general. That's important.

MR. GLEASON: I am talking about through the filing of a motion and attaching exhibits. Your adversary would have the opportunity to place something in a court record that might have a trade secret, medical significance or other kinds of things like that.

MR. FREEMAN: You know, the example given earlier in the afternoon was, I think, of the Coca Cola trademark recipe. If it was available in a court file three days before someone made a motion to close it, presumably that would be a problem in and of itself.

I guess I do agree with Mr. Klaris that we think a mirrored approach is workable, and, you know, if something dangerous is in the court file for three days and Coca Cola is going to survive that, then they

will survive it on the Internet too. I assume once it is sealed in the court file, then it will be sealed on the Internet in some manner that I can't logically deal with.

So I guess the question that maybe I bagged that you are really asking is: What happens? I am not sure of the answer. What happens if something is filed under seal, if the file is made under seal? If the rules allow for that, then I assume the Internet filing would be under seal as well in order to be consistent with the analogy.

MR. GLEASON: My question is: Is there constitutionally a big problem if, because of the nature of the Internet and the immediate worldwide availability of whatever is filed there, is it really a constitutional problem if you have some period of time after a filing that gives the adversary in the case the opportunity to make an objection? Do you have a real problem with that; and if so, what is the constitutional basis for that? Because presumably a judge hasn't even seen it yet.

MR. FREEMAN: I guess my answer is whether it is constitutionally a major problem is hard to say. I rely on the Commission for that answer who has more experience than I do. But I do think it is hard for me

to see the great harm if, in your scenario, that information is available in the courthouse in any case from the time of filing until the time a judge hears a motion, etcetera. And let me just say that, you know, if your question is that people can then attach documents just to harm other people, the fact is they can do that today on a website, they don't need the court's website to do it. They can have their website. For example, I just heard an instance, you know, this morning, where a restraint has been issued because someone put on their website the sexual proclivities of his former girlfriend, and so the girlfriend came in and got a restraint against that website.

So this is being done from time to time. You don't need to do it through the court processes. You can just put the stuff on your own website and the effect would be the same.

MR. KOVNER: I think Mr. Gleason is suggesting if there is something inadvertently contained in someone's papers or attached to someone's papers which will be noticed by the adversary party who will see right away something that they should not because, perhaps, the other party didn't think about it, that it should have been under seal or confidential and that an application should have been made for that.

Within a short period of time, nobody is immediately going to go to the courthouse anyway, unless they have been alerted to do so; but shouldn't there be a short period of time where the other side can either ask the party to place it under seal by stipulation or ask the Court, you know, that Exhibits X and Y in the filing ought to be placed under seal so they don't go on to the net?

MR. FREEMAN: My answer is only -- well, if you are saying there is no great harm because it is only going to be in the courthouse for a couple of days with access to the public, why do we think somehow that even if it is on the Internet everyone is going to hit upon that?

MR. GLEASON: I will tell you why. I think there will be people who will create search mechanisms that basically download every single item of information that comes out of the court system every day; not looking at it, just cataloguing it. So as soon as it hits the Internet every day, it gets copied and made available, then it becomes public.

MR. FREEMAN: So you are saying if it is later sealed but it is already on the website, it is fair game and can't be put back in the tube. Yes, I understand that problem. I mean, I also don't know or

profess to know -- I assume that the filing will not be simultaneous.

MR. GLEASON: Actually, now on New York's electronic filing system, when it hits the web page it is public. And presumably an electronic filing system can operate the same way. If you want maximize the openness for reporters and everything else, you could have a system virtually having simultaneous publication with the filing. And our question is: Do we need to temper that because of possible harm?

MR. FREEMAN: I guess the question -- I don't think that it would be necessary were it not for the kind of secondary use that you just spoke of, of the people who then won't obey the seal once a seal has been enacted.

MR. GLEASON: It could be the New York Times getting the Pentagon papers becoming public or something like that.

MR. FREEMAN: Well, it would be good for us to be able to do that.

MS. BRYSON: I follow up on Mr. Gleason's point.

With all due respect, you are sort of talking out of both sides of your mouth. The reality is on Pages 2 and 3 you cite eight separate steps that

somebody has got to go through to get the file if they know it is there. And, in fact, if the Coca Cola recipe is sitting in the courthouse, unless you are one of the parties, you have to either know or you have to, sort of, luck into it that day and have a lot of pocket change and have the caption of the matter. So the reality is that if you have the knowledge to go down there that day, then it is accessible. But short of that, there is a realistic period of time built into the existing system which you like. There is an existing period of time that you have where you look at the papers that you just received from your adversary and say, Oh, my God, he released attorney-client privileged material that we all agreed was confidential and we all agreed would not be filed and yet they have attached it as an exhibit -- maybe out of accident or maybe out of malice. Or, perhaps, it relates to the privacy of a third-party who is not even a party. There are lots of reasons why and certainly lots of circumstances under which proceedings have resulted from the inadvertent filing or the intentional bad act of filing.

So I really want to challenge you on whether or not if you like the system as it is in terms of access, whether or not the system as it is already

includes the contemplation of the ability to remediate that without having it be all over the universe.

MR. FREEMAN: There are a lot of different durations of the problems that could come up. I think if it is malicious, as I say, it could be put on a website. Forgetting about the court system website, you could put it on any website. If it's Coca Cola, it seems the Dr. Pepper people will know it is filed and get a hold of the patents.

If it is inadvertent, sure, I don't deny that in certain instances it would be a situation where if no one is looking for it, the odds are that if it is in the courthouse for a week it is not going to cause great harm. But those are only odds. That's kind of luck and fortuity. You are saying and speculating that if that same week it is on the Internet, boy, that millions of people will rush to get it, which I doubt is true. But sure, in that sort of branch of the hypothetical, it is possible, you know, that one way something not particularly good will happen whereas the other way, if we are lucky, no one will see it in the courthouse and it will eventually be sealed.

MS. BRYSON: Mr. Freeman, at the end of your statement you indicated -- and I want to be clear about this on the record. I am quoting from your statement:

"If the Commission believes that such a burden has been met, the exception should be extremely narrowly tailored to include only a close specific set of so-called identity data -- social security number, credit card numbers, bank account numbers and nothing else -- and should be blocked from access not automatically but only upon an appropriate showing."

What would you believe would constitute an appropriate showing; and are you saying by this that we should not recommend to the courts that they adopt a rule that says the presumption is don't include a social security number?

MR. FREEMAN: I'm sorry, the last part of the question is what? The presumption is --

MS. BRYSON: It has been proposed to the Commission by several speakers that we include a recommendation to the courts that the rule be don't include identifying information unless there is a showing for a need for that identifying information.

It sounds to me like you are depositing the opposite, which says to include all information unless a showing is made not to. Am I correct in that understanding?

MR. FREEMAN: Yes. I am putting the burden on -- and I think that the usual access First

Amendment analysis puts the burden on the person trying to close the material rather than the other way around.

MS. BRYSON: But can't the Court determine --

MR. FREEMAN: Let me add one more thing to clarify.

I do think that with respect to those three distinct identity data situations, it is fair to say that the burden on the person trying to close that, to redact that, as it were, ought to be easier. It ought to be a lighter burden than with any other type of information where the current balances would take place. I do understand that that type of information, that the showing ought to be a lot easier with that type of information.

MR. ABRAMS: Let me follow up, though.

When you said on Page 8: "To the extent the Commission believes that the rules for openness of electronic records should not exactly mirror the current rules with respect to paper documents generally," let's turn back to the rules about paper documents generally.

Do you have a view as to the wisdom of the judicial system urging or requiring counsel, when counsel files paper documents or electronic documents, not to include social security number or the equivalent

type of information absent some sort of special circumstance?

Some people have argued at our Albany hearing that maybe a way to do this would be to keep the standard the same for paper filing and electronic filing and Internet posting with respect to this subject, but that the way to do it would be, in effect, to urge or require counsel, whatever the form of filing, not to put in certain types of especially sensitive data without some special permission.

MR. FREEMAN: Again, that has the jeopardy that I was warning against at the beginning; that in order to keep the mirror image of an electronic and paper filing, we are going to create less openness overall in the system. That's a risk I really don't want to have happen, and that's a risk we ought not undertake.

So despite my stress and my presentation, I am for this -- for the mirror image concept. And with respect to the very narrow identity data information, I wouldn't object to some different standard with respect to the electronic filing of that data. But I am troubled about the fact that that then could be automatic, and I wonder -- and as Ms. Bryson pointed out, it is not perfectly formulated -- whether some

showing still should be made before that should be blocked, even in an electronic world.

MS. BRYSON: May I just ask you, did you respond with respect to the address question? Does the Times take a position with respect to whether address information as is proposed by the domestic violence advocates, that that is a type of demographic information that should fall into that social security number type --

MR. FREEMAN: No, it should not. I believe that the examples of address and phone numbers are inappropriate because they are so readily available. I think that really is flipping presumptions around entirely and flipping reality around. Addresses and phone numbers are just not very hard to find, and the notion that we should make exceptions to those, you know, I don't think is worth it.

MR. ABRAMS: Thanks very much.

(Continued on next page)

MR. ABRAMS: Robert Port.

MR. PORT: Hello, everyone. I would imagine you're very tired at this point.

I've submitted a statement of six pages and I won't waste your time by going back over all of that. Just a few brief remarks and I'd be happy to answer any questions.

I've been a newspaper reporter and editor for more than 20 years. In the past ten years or more of my career have specialized in a somewhat unusual area of journalism and that is using large electronic databases in investigative reporting.

For example, I have a copy of the entire New York State criminal records database in my house at home. I also have the entire civil system.

This data is available. It's not easily available. And I only use it for my work as a daily news reporter and restrict it to that. But I have it and it's great.

I would like to make one main point to you and that is this: I believe there's one and only one policy that makes any sense for electronic access to court records in New York or any other state for that matter. Information that is public at the courthouse should be available on the internet to everyone all the

time for no more cost than the cost, if anything, of its publication. To do anything less than that is to bar the common man from what will be the real clerk's office of the future.

A couple of years ago -- short story -- I visited Bankruptcy Court, here in Manhattan, for the first time. I don't know if any one of you have had occasion to stop at the clerk's office there. My advice is don't waste your time.

I got on the subway all the way down to Bowling Green. There is a room full of Court Clerks. One young lady, filing her nails, chewing gum. Another fellow reading a magazine. Someone watching TV. I was all ready with the case I needed, eager to see the big cart of files pulled out. And when I finally got their attention, a young woman pointed to a tube across the hall and said it's right over there.

Bankruptcy Court in Manhattan has had an all digital filing system for longer, I believe, than any other court in the United States, possibly. Certainly one of the longest. And paper records essentially don't exist.

I think this is an important point for you because you really are not debating policies that should apply to records on the internet, you are really

debating some very core questions: What are the basic rights of access for citizens to court records period.

I believe that whatever results from what you recommend is simply going to end up being the practice of the courts in New York. To me that makes your job very simple. Just keep the access the way it is right now at the courthouse.

The internet really does only one thing, I would say to you. It does it utterly democratically. It makes transmission of information exponentially more efficient. All else that it does that results from it would or could have occurred otherwise.

For court records, all it does is save trips to the courthouse. The court has the full power to seal whatever it wants to seal where it has a right to seal it and it can continue to do that with electronic records.

A few points: I believe our notions, our expectations of privacy really are foolhardy. Anyone who seriously believes that social security numbers are private is deluding himself or herself. They are not.

I could get any of your social security numbers easily, legally, without any trouble at all. Any journal list could and they often do.

The solution to identity theft that that

implies for us is very simple: Id cards that have biometrics, a concept that's been endorsed by many people, including a lot of prominent, liberal defense attorneys like Alan Derschowitz. Simply ends the problem of identity theft.

For every horror story -- and I've heard a lot this afternoon and every one of them has been purely hypothetical, I would argue to you that I could conceive of a hundred public record success stories.

The ability of citizens to quickly get answers to basic questions they need for know. A young couple shopping for a co-op, able to review the litigation on the co-op is on file, without having to trust the seller's assertions. That sort of simple, day-to-day access is tremendously valuable to our economy and it increases our productivity.

When it comes to personal identifying information, I would respectfully disagree with Mr. Freeman's suggestion of censoring bank account numbers and social security numbers and so forth, mostly on the grounds that it's a waste of your time because it has very little value. When it comes to personal identifying information, the horse -- the horses are so far, far out of the barn you will never bring them back.

It isn't the judiciaries' job to do that, to worry about that. That's a job for our legislature. Privacy concerns.

There is a growing -- it was discussed earlier, the hypothetical problem of the instantaneous filing of pleadings of documents in a civil case, the problems that can occur if information is inadvertently released, that sort of screening of filings is already occurring electronically.

A service company called Court Link was recently acquired by ***Nexis Lexus; purchases from the Unified Court System of New York, transmissions four times a day of all docket entries in civil cases.

I've had conversations with them simply to learn how their service works. A number of large clients, some large corporations, pay them upwards of a thousand or a few thousand dollars a week for instantaneous electronic monitoring of these docket entries.

Now, it's not the entire digital document. They don't have the thing in their hands yet. But they have only when they see something important to send a runner to the courthouse and make a copy. That's not that much quicker than would occur on the internet and yet chicken little, the sky has not fallen on us for

these sorts of mistakes.

In short, what I would say to you is my greatest fear as a citizen -- and it terrifies me as a journalist -- is that you will take the occasion of this construction of a new fax machine for court records to begin enacting restrictions on my ability to see public information that never existed before and have no good reason to exist.

I'd be happy to answer questions.

MR. ABRAMS: Thank you, Mr. Port.

MR. GLEASON: My same question again.

I think you raised the issue of sealing of court records. I think you take the position that -- correct me if I'm wrong -- that as soon as the documents hit the courthouse, they are public and available to the world. And in that instance, don't you see a concern of the possible misuse of or inadvertent use of sensitive medical, trade secret or other information that would immediately be made available in electronic form that would be impossible to recall after it hits the Internet, if the systems are identical in the sense that anything hitting the courthouse is immediately available to the world.

MR. PORT: I don't see any concern at all that doesn't already exist to essentially the same

degree in our current system of paper records. The only concern -- the concern might be amplified a bit because of the speed at which things occur. But I see no reason --

MR. GLEASON: The possibility at least exists, in a paper record situation, that if there is, for example, some medical information that's sensitive and irrelevant to a case, that you could seal the court record and it not be widely and publicly disseminated; whereas, if the court records are scanned every day, as I would assume they would be, after that -- perhaps the information could be copied and disseminated to millions of people with a few clicks of the mouse. Isn't that at least to some degree different in a qualitative sense?

MR. PORT: I don't believe it is. It's a fair question but I don't believe it is because I think you have to ask yourself the question: What is the potential harm?

MR. GLEASON: Well, if your adversary has it and wants to use the information for purposes of damaging your business in a commercial case, or if in a case where you have people who have an acrimonious break up of a business and they want to use things for purposes of creating harm, there's a possibility that

before any judicial action is taken on it, before it even becomes the subject of any judicial consideration, it's immediately widely available to the public and it is used in a tactical way by an unscrupulous adversary, perhaps in a way that has nothing to do with the ultimate disposition of the court case.

It's at least possible that would happen. And that risk certainly is, in my view, greater in electronic format, which we should at least consider.

I don't see them being quite exactly the same as I think you do.

MR. PORT: I think the only difference has to do with some degree of speed. I would say that an adversary in a civil case, as you hypothesize, who wants to embarrass the other side, should not waste their time filing it in court and putting it on the Internet, they should call me at the Daily News and I'll put it in the newspaper.

MR. GLEASON: It might not be something you'd put in the newspaper.

MR. PORT: It might not. It probably wouldn't.

This the thing about the Internet you might keep in mind. It's not some massive broadcasting system, constantly sending E-mails into everyone's box

where they will twitter over every embarrassing detail. It's just sitting there.

And I just think that most of these fears are exaggerated. Most people won't care. And in an intense emotional dispute and in litigation, those sorts of tactics will always be available any number of ways. And it is just not that hard for someone to set up a Web site already and publish documents.

Someone mentioned earlier fears of 9/11, you should be concerned about 9/11.

The federal litigation, the transcripts of the various criminal trials starting in the first World Trade Center bombing, through subsequent cases, the embassy bombing case, were all widely published on the Internet. The problem for us in New York was not enough people read them. That was really the problem. Not that they were there.

And I think that publishing documents in civil litigation on the Internet is simply going to speed up the whole business of getting to the bottom of who was right and who was wrong and who was to blame and should we care.

I see no reason to being particularly worried about adversaries any more so because we have a faster fax machine.

MS. ABRUTYN: A practical question, following up on that same theme.

I want to understand a little bit how the system works now. And let's assume that the -- an adversary in a case, a defendant or plaintiff in a case files a motion with a bunch of documents attached to it and it's either they are trying to embarrass you so they call you up and tell you they are going to file the motion, or it's on a case that you're interested in and you use this service or whatnot. How long between when it's filed and when you or your runner or whatnot can get down to the courthouse and read it? Is it days? Hours? How long would it actually be sitting there before somebody could get their hands on a copy of it?

MR. PORT: In the current system? A few hours. I think we're talking technologically the difference between four hours at most a day and less than an hour.

I think a very interesting example, I mention in my written statement, is the Enron bankruptcy case, which is all electronic. Reporters covering that case, all the lawyers on it, have to file everything electronically and read it that way.

It was on a Saturday that the committee,

appointed by the board of directors of Enron released it's very explosive investigative report describing its initial findings of what went wrong. We were very lucky the New York Times reporter was watching the Federal Court record system, Pacer, and monitoring new records saw it. Maybe someone called him and alerted him to it -- that may be more likely perhaps what happened -- downloaded it, wrote a story and there was the essence of the -- that whole report on Sunday morning when a lot of readers are most ready to absorb it. The healthy debate that followed got off to a running start.

If in the current system, I guess we would have had to wait until Monday and then Tuesday's paper to learn that.

That's maybe the extreme. But if a reporter is hot on a case, watching it day-to-day, the difference between electronic filing and having the document versus what it is now, runner, courier to the courthouse, is less than four hours.

MR. ABRAMS: Thanks very much.

Ms. Mortise.

MS. MORTISE: Good afternoon. Thank you for allowing me this opportunity to be heard.

I would like to spend five minutes to make a

comment and I would like to give my other five minutes to another member of our group, Pro Se Alliance.

First of all, I'd like to say, to put a face on this type of information, I've been in a Housing Court, Civil Court of Manhattan for approximately five to six years.

Although I've listened to your panel and you seem to have a respect of the majesty of the law, in the lower courts this is not true.

While all court officers, judges and some of the petitioners' attorneys are not that bad, there is a problem. And I believe this information that Judith Kaye is seeking might hurt a segment of the population that is not being considered. That population has a racial component, an economic component and class component. Poor people will be hurt by this.

My analogy is this: The jogger, the five teenage boys did not do the awful crime committed to that woman. Those boys were accused and persecuted for 13 years. If this was out on the Internet back on the day it happened, 1988, the whole world would have hated them. Fortunately, it was not on the Internet but it did go out into the world and it was a lot of hate.

Now, in this year, 2003, they are exonerated and we see there was some problem with the prosecution.

When you go into the Housing Court, it's the same thing. Ninety-five percent of the litigants in the Housing Court are unrepresented. These attorneys will do anything to objectify a neighborhood to steal property.

My property was stolen. I live on East 97th near Gracie Mansion. These attorneys will -- if you have children -- will get your records, they will make a false complaint to Children's Services that you're a bad mother. If you filed a bankruptcy petition, as you spoke earlier, they will get those records, the whole petition, put that into Housing Court; your money, your dependants, your social security. Anything you've done is put into the lower courts and exposed to be used and abused to anybody that wants to use it. As a lay person, I'm still down there.

As I said, I lost my property. This year, my landlord and his attorneys regurgitated a case and kept me in court for a very long time.

This year, one of the Housing Court judges deemed I needed a guardian. I didn't know what that was but when she said it, I was embarrassed. It was an open court of 30, 40 people. Never in camera.

I never had any history of mental illness. I thought she was helping me.

Unfortunately, a guardian takes over your life. You're not able to defend yourself, speak for yourself. Their guardian lived in another state, New Jersey. I had one trial one Court appearance. My equity -- my co-op of 175,000 is down the tube. I was evicted with my shoes and T-shirt, because of this guardian.

Court officers from the Housing Court that knew me said, Oh, Miss Mortise, would I want to sign in, make my appearance and let your guardian do it. I couldn't even get an Order to Show Cause form in the Housing Court because I was designated I needed a guardian.

I've known people who have come to our monthly meetings, since we don't have money for attorneys, and we help each other who have left their properties rather than be abused by a Housing Court's discretion of saying you need a guardian ad litem.

You cannot get a job. Someone says you need a guardian. You are stigmatized. It's like being a junkie.

If you do have mental illness, that's one thing. It should have been done in camera; should have been done with a professional.

A judge -- certain judges may have their own

bias. This is what's wrong.

I believe if you're poor, a minority in the lower courts, we do not have the sophistication of papers to put in papers to protect ourselves. If this is made public on the Internet, it can affect our lives.

Who's to say that someone fighting a Housing Court action that goes and is characterized -- mischaracterized as a bad person and these records are filed on the Internet, maybe they don't have an Internet to look at at home. It could ruin your life.

I hope whoever is looking, they are aware there will be a segment of population that won't be heard. The ones without lawyers and in the lower court Housing Court.

One other thing. Due to what happened to me this year as a pro se litigant, I should not have to be able to do this but my dignity has suffered and I've had to file a State claim against certain misconduct, certain information that was done about me, that cast me in such a bad light. So I now have a Court of Claims action against the Civil Court of New York.

Thank you.

MR. EISENSTEIL: My name is Irwin Eisensteil.

Although I'm a member of the same group, I have a different position in certain areas.

Before I continue, realize, I am or was a database administrator, managing extremely large databases for the City of New York. I also have had an interest in Court TV's brief. In fact, I think Mr. Abrams helped in presenting that brief in a case in Virginia.

Let me just cite from one thing. "The value of openness lies in the fact that people are not actually attending trials and have confidence a that standards of fairness are being observed. The sure knowledge that anyone is free to attend, gives assurances that established procedures are being followed and that deviations will become known."

Obviously, that was written for a Court TV brief. However, I've heard misstatements made at this forum that I'd like to address.

I really wasn't aware that this Commission was on and I was called down, so I really didn't have a prepared statement.

If someone wants to publish papers on a Web site prior to filing them, as the ACLU did, and certain First Amendment issues, I think in a Coppa case, they can.

So, as far as putting stuff and waiting until it hits the Court, obviously is a misnomer.

As far as spam and other information, you can control some information within the country. There are international issues and areas of law which you haven't touched on.

Scott MacNeely, the head of Sun Micro Systems said anything is available.

As for credit and as for identity theft, the FTC has a Web site. However, put the burden where it belongs, the people who are giving the credit should do credit checks. They have the information available. They are not doing it.

As to openness on court records, I think the court record should cost less or, in fact, should cost nothing, rather than restrict access to information to a segment who can afford it, in most instances only lawyers. You want everyone to have access to that information. You don't want people to have to drag to take a day off from work in order to get access to the information. You can get access to all of the records.

As to the cost, you're going to have reduction in costs because you're going to image everything. You're not going to have to store it, retrieve it. There are so many advantages of having

all records available.

Right now, you now, for example, the Federal Court system is talking about having all unpublished cases available on open and public sites. They expect to do that, I believe, in two or three years.

MR. EISENSTEIL: (Continuing) She started this guy. I have so much to talk about it is really too bad I wasn't aware, but if I went down the five points, in light of recognized public interest: (1) If you want to restrict certain information, you can. That's the duty of the Court, to put restrictive orders on individual attorneys. And, in fact, you have sanctions available if attorneys don't act appropriately. Perhaps look at your own profession and ask how frequently you have sanctioned attorneys for abuse. Very infrequently. I have seen lawyers lie so frequently that public trust in the legal system, they rate lower than used car salesmen.

A judge of the Fifth Circuit in front of the Harvard Law School class raised the issue of law as a business, it is no longer an honorable profession. I think it was Helene Jones, or something similar to that.

Cost should not, in fact, be an issue. Access to the information can, in fact, be controlled whether you want bank accounts or anything else. I think what you do have when you open all records and in fact, put more than just the filings online is you have an entire picture rather than a restrictive picture. You don't have the costs of putting in the 25 cent

piece for each page that you currently have to get at a courthouse. All of those records are available to no cost once they are online and available. I can afford it but many people can't afford the $5 or $10 or $15.

As far as keys to access, you can either use an entire document key or, for that matter, if the image of a document is online, you can convert that image to a test database. It happens all the time. There are so many tests, OCR types of programs that will take an image and do that. You could go to Adobe PDF files, for example, and convert them to a text base and then a searchable --

MR. ABRAMS: Sorry, sir. Your time is up.

MR. EISENSTEIL: Okay. If issues are related to cost or access, please address them to me. You raised issues as to privacy issues and to other issues, but, again, if cost is --

MR. ABRAMS: Let me add a final word, sir. If you do want to make a written submission, we would be glad to receive it.

MR. EISENSTEIL: Thank you.

If there are any comments or questions, I will answer them.

MR. ABRAMS: No? All right. Thank you.

Our last witness for the day is Eliot

Deutsch.

MR. DEUTSCH: Yes. Good afternoon.

MR. ABRAMS: Thank you for waiting the day out.

MR. DEUTSCH: Sure. I think I missed most of the day. You had to have been here all day.

I am a single practitioner practicing primarily criminal traffic law for 25 years. I have an office in Nassau County and an office in Suffolk County. And as far as runners are concerned -- I heard that word used -- I am the runner, the doer. I am a single practitioner. Everything that is done I do myself.

In making a mental note of things taking place between yesterday and today in my practice in relation to this presentation, I came across several items for which I would have found access over the Internet extremely useful.

Today I got a phone call from a 68-year-old gentleman in trouble and who has no copies of court papers. He is not even sure what he is charged with doing. I can't help him or even start to talk about his case until I go to the court and get a copy of the papers.

I also got a call from a Spanish-speaking

person who can't read the papers that he has, and, therefore, he does not know when his refusal hearing at the Motor Vehicle Bureau is. For all I know, it could have been this morning. But if he misses his refusal hearing he is going to have his license revoked due to non-attendance, and he'll lose his opportunity to be at that hearing because he can't read the papers. If I had Internet access, I could go immediately online and see the papers and have an answer to that question.

The court system predates electricity. To date, the failure of the court system to embrace technology has led to enormous amounts of time and money being wasted. Money and time is wasted in both the public and private sectors with the current system.

The subject of public access to records goes hand in hand with a future major revision in the way the courts operate. With increased public access through individual public access computers at the court itself and over the Internet, information could not only be obtained but in the future eventually exchanged. Once the ability to exchange information is established, more court business could actually be conducted over the Internet, thus less people would be needed to make our paper system and in-person system work.

Currently the courts waste an enormous amount of time on simple adjournments. The court staff: The judge, the court reporter, the court clerk and three or four court personnel are all in a courtroom all morning but half the cases are adjourned.

For example, a person has a suspended license charge and the license has to be cleared before the case can be done, so there's an adjournment. With a petit larceny, a shoplifting charge, a person might have to take a course but maybe that person hasn't take taken the course yet. So the case is called, we approach the bench, talk to the judge, I tell the judge that my client needs more time for the course. The judge says, Okay, I will give you have a new date. With a DWU various things have to be done. In Suffolk County you have to do community service work. So when the case is called you tell the judge and the judge says, Okay, I will give you a new date to do the community service.

All these things, these adjournments can be done over the Internet, and then the courts could be productive rather than spinning wheels.

An open system is a better, more honest system. If records were more easily accessible, more public analysis of these records could take place which

would result in more public scrutiny of the prosecution's system and the eventual reduction and possible elimination of inequities and questionable behavior on the part of the prosecution system.

For example, a system which would allow all arrests made by a particular police officer to be accessed would allow the public to analyze these arrests and see if certain patterns exist. Is there racial profiling going on? Did the arrest take place within the last fifteen minutes of the tour of duty of this particular police officer so that, perhaps, he is getting overtime for it? Are we seeing a particularly high number of questionable arrests from a police officer in the year before he is due to retire so that this year he is putting in a lot of overtime by making arrests during the last 15 minutes of his tour of duty to boost his income this year so he in turn will get a greater pension? I know it works somehow like that.

Privacy concerns. I heard a couple of the other speakers, and I agree with what they say in the sense that there are current ways in which privacy is maintained in the current system. I think those concerns should be brought over into an Internet access system.

Mr. Gleason, you asked the same question a

couple of times about records that are sealed and what happens if we first have a document on the Internet and then it is later order to be sealed.

From a criminal point of view, the same thing happens with criminal records all the time in the current system. Look at how OJ's reputation was ruined even though he was found not guilty. That could happen to many types of criminal charges. A local paper might report that someone was arrested for shoplifting and the neighbors will see it. But then maybe eventually that person will be exonerated. However, because it was already in the newspaper, already made public, even if later the record is sealed, the damage is already done. So that happens already in the current system, and I don't think there is a way to avoid that.

What is the role of the court? Any public information that could be available through a clerk or through the act of looking at a court file should be available on public access computer terminals at the court and over the Internet. I mention public access computers at the court because lots of people don't have access to computers. And we don't need the clerk to just give out information. The clerk can do something else.

Regarding fees, public access means public

access. It does not mean access when we get around to it or access if you fill out a form and come back in two days or access if you pay me money. Just as a file could be looked at for free, a file should be accessible on public access computer terminals at court and over the Internet for free. The public has already paid for the compilation of information in the court system. The government is the government of the people. The information in the court system is not the government's information, it belongs to the people. Charging fees for access to public information is nothing but a hat trick, and, in fact, it chills public information access. If we say it is public but you have to pay for it, it is not really public anymore.

If there would be fees -- if there had to be fees, I would suggest that accessed information on the outside of the file jacket be absolutely free; that there be no fee whatsoever charged for that information. If there were to be a fee for Internet access, then I would suggest that there be a subscription fee along the lines of a monthly or yearly fee designed to cover the cost of providing such access; not designed to make profit, but to cover the actual cost of providing access. Remember, the government is not a private company. It is not

Microsoft. If public information is public, then it is already paid for by the taxpayers.

Search methods. The ability to perform text-based searches is, indeed, a valuable thing to have. I can see the possibility of charging for a text-based search because it would save an awful lot of time. And so I would recognize that a text-based search specifically would be worthy of charging some type of fee for.

MR. ABRAMS: I am afraid, Mr. Deutsch, your time is up.

MR. DEUTSCH: And there should be no fee for searches based on name or docket number, only on text-based searches.

MR. ABRAMS: Thank you very much.

MS. BRYSON: I have a quick question about your suggestion about a subscription fee. Are you saying that should be in lieu of a per search fee, or could you please explain a little more about what you mean?

MR. DEUTSCH: AOL access -- of course, it wouldn't be the same type of thing, but 20 bucks a month is AOL, or 22. So if you wanted access to the court system you would pay X amount monthly or yearly or maybe you would get a discount if you paid the year

in advance. But it would not be on a per search basis. I think that is just too chilling and too extensive.

MS. BRYSON: Would you consider either alternative, because the pro se litigant may not have $20 a month?

MR. DEUTSCH: That's where the computer at the court, the public access computer at the court comes in. It's for a litigant to walk up and use. So that would come into play there and that would be free.

MR. ABRAMS: Thank very much. We appreciate your testimony. Thank you all very much for attending. We are adjourned until Buffalo.

Testimony of

Charlotte A. Watson
Executive Director
New York State Office for the Prevention of Domestic Violence

before the

Commission on Public Access to Court Records
May 30, 2003

Chairman Abrams, esteemed Commissioners, thank you for the opportunity to address you this afternoon on the most important and challenging issue of public access to court records. The New York State Office for the Prevention of Domestic Violence (OPDV) is an executive level state agency, created by the governor and legislature to improve the response of the State and local communities to domestic violence.

Great strides have been made in the past 30 years in the response to domestic violence, along with a vastly increased use of the civil and criminal justice system. The lion's share of change in the criminal justice system's response in New York State has occurred over the past 10 years under the incomparable and synergistic leadership of Governor George Pataki and Chief Judge Judith Kaye.

At the same time, the use of computers and access to the Internet has exploded. What we innocently put on the "Web" a few years ago is now being used in ways we never considered, including invasive crimes such as identity theft. We've heard horror stories of how stalking victims were tracked and harmed through information posted and available to all—for good or bad intent. We've all seen those annoying pop-up ads on our computers, advertising the ability to find, literally, anyone. As a domestic violence advocate with more than 27 years in the field, and one concerned about privacy in general, those ads, and the open, easy access to so much personal information in what we term the "information age" are truly frightening.

Nowhere is this more of a concern than when considering the safety and security of victims of domestic violence, sexual assault, and stalking. We know that domestic violence is a pervasive, on-going, life-changing reality for millions of women and children in this country, and that stalking is an integral part of the dynamic of domestic violence.

Domestic violence victims know all too well that their abusers will use any means to control and terrify them and to keep them from escaping. It is not unusual for a batterer to monitor the odometer on the victim's car, record the victim's phone calls, or use

hidden cameras. Imagine what it would be like to have a Global Positioning Satellite unit attached to your car and monitored constantly by someone in authority over you . . . this is the daily reality of many victims of domestic violence with the state of technology today. What will tomorrow hold?

It is extremely difficult and often dangerous for battered women to escape their abusers. Many find it necessary to flee the area entirely in hope of finding safety. Those who are able to get away live with the extreme fear of being found by their abuser--a losing battle for approximately 1,100 US women each year who are murdered by their intimate partners after fleeing, as well as, countless others who are re-assaulted.

There have been many attempts to help victims find safety. Recent changes in law make it a federal crime for an abuser to stalk and abuse a victim across state lines. There are processes by which victims can change their names and social security numbers, sacrificing their identities just to be safe. Unfortunately, at the same time we are recognizing the needs of domestic violence victims, the trend toward "open government" and access to information has become an easy, affordable, and valuable weapon for abusers.

As advocates for victims of crime, however, we *do* recognize the need to find ways to increase the accountability of systems, including the courts, in their responses and decisions. It is vital that these interests are balanced against victim safety and the privacy of users of our court process. In the effort to increase accountability, the court must be mindful of even the appearance of culpability should granting easy access to information result in harm to a victim. It should never be the case that potential consumers of the courts must weigh the need for safety through court intervention against the need for privacy and anonymity which may also impact safety.

In light of these concerns, I will outline a number of negative implications as well as recommendations regarding open access to court information. In addition to our own experience in responding to domestic violence, we received assistance from the National

Network to End Domestic Violence in researching this important issue. The following critical issues must be addressed before moving ahead with this process.

Negative Implications Include:

1. **A chilling effect on victims who are considering using the court for legal relief.** While we applaud the fact that family court and matrimonial records will not be subject to open access, I must emphasize that under current law, criminal court is the *only* court in which many victims may seek relief. Consider, for example, a victim who is being abused or stalked by a boyfriend. To obtain an order of protection, that victim will have to disclose significant personal information and potentially embarrassing details about the abuse in a criminal court. Under the *Conference of Chief Justices and the Conference of State Court Administrators Guidelines*, this information would be readily accessible by the public and the offender. It is not a leap to say that victims will be reluctant to pursue an order of protection under these circumstances. Is it fair to ask a victim to sacrifice her privacy for the safety she is entitled to under the law?

   Imagine the heyday the pornography and smut industry will have with such easy access to crime scene photos of horribly violent rapes and homicides. Imagine the websurfer who accidentally opens a porn site or the errant adolescent going to sneak a peek only to discover the crime scene photo of his naked mother lying in a pool of blood. At what point would the balance tip from accountability to culpability? At what price? Who and how would the decisions be made as to where to draw the line?

2. **Safety Risks for Crime Victims and Witnesses.** As I noted earlier, abusers often track and monitor their victims as a means of maintaining control. These behaviors typically increase when a victim leaves the abuser. Whenever a victim becomes involved with the court system, whether voluntarily, as a result of mandatory arrest or pro-prosecution polices or for some other reason, precious

information about her location, status, current name, phone numbers and other circumstances is disclosed. Such disclosure is a major concern for my agency and victim advocates across the state. We know that abusers will access this information and use it every way possible to stalk, threaten, assault, or kill the victim and maybe her children.

This can be a problem even when a victim is using the court system for something unrelated to domestic violence. For example, if she is involved in a motor vehicle accident resulting in legal action and the information, including the location of the court, is posted on the Internet, her address would be posted making it all too easy for her abuser to find her. Perhaps she relocates to escape the abuser and later becomes the beneficiary of a probated estate. As a result, identifying information could be posted, creating similar safety risks. Ironically, if a victim is seeking a legal name change, even this information could be posted on the Web, making her efforts at anonymity fruitless.

It's important to note that she may not be a victim at the time of her interaction with the court on the myriad of non-domestic violence related actions that could bring her to court. After one date with a stalker, she would be vulnerable to his gaining valuable information about her that could lead to her demise.

3. **Increased Opportunity for Identity Theft**. Destroying the victim's credit and reputation is a tactic already used by batterers. Open public court records will only increase the opportunity for accessing and misusing personal information.

4. **Secondary Uses of the Information.** Information stored by the courts will most certainly be used for purposes that move far from the original public policy intent of governmental accountability. It will be gleaned and sifted and compiled along with other information to create entirely new databases that can be misused and misinterpreted. Once the information is gathered for another database, it can never be taken back or corrected. In domestic violence cases, false or misleading

information could be deliberately planted by the batterer in spurious legal filings that include slanderous material against the victim which are then posted on the Web for all to see and use.

5. **Undermining Victims in Custody Proceedings.** Seeking custody is one of the most powerful tactics used by abusers to access and control their victims. Abusers will use every means available to discredit the victim and prolong a custody battle. The proposed *Guidelines* actually aid abusers in this process. Open, public access to court information provides abusers with cheap and easy access to all records of any criminal proceeding, regardless of whether such information was relied upon by the court. This poses serious ramifications for victims who ultimately leave their abusers and seek custody. Economic survival or the abusers threats or false promises often compel victims to minimize or deny the events or to later recant earlier statements of abuse that form the basis of a criminal prosecution. The fact that such records from a criminal proceeding and many civil proceedings will be within easy grasp of an abuser in a subsequent custody proceeding essentially re-victimizes the victim, rewards the abuser's use of coercive tactics, and facilitates the abuser's use of custody as a weapon of control.

6. **Dangerous Reliance on Individual Discretion**. In many instances, courts will possess far more personal information about a victim than might be held by a State agency subject to FOIL. The proposed guidelines heavily rely on human discretion and information management in an effort to protect personal privacy which will undoubtedly result in human error. Unlike many other types of crimes, in domestic violence cases, one simple failure to redact an address or social security number could have, literally, fatal consequences.
Even the most competent offices may find themselves outmatched by an abuser determined to discover the whereabouts of his victim.

Under the proposed *Guidelines*, victims of domestic violence will likely be hunted down, harassed, stalked, assaulted or even killed with greater frequency. Government exposure to legal liability will increase. It is deeply troubling for us as advocates to contemplate a system that so completely depends on individual discretion at the risk of harm to victims and their children.

We wholeheartedly agree that as much information as possible should be available to the public regarding governmental actions for systems accountability to be achieved. However, this should *not* mean full and open, cheap and easy access to everything that happens within the walls of the courthouse. We must hold this system accountable in the same way that we hold the healthcare system accountable without violating the patient's right to privacy.

There have been many recommendations made as to how to modify the proposal for open public access to court records, or to redact critical information, but we believe that none of these can ever adequately control for human error and poor decision-making, or justify the enormous expense that would be associated with such modification.

Before any final decisions are made regarding access, it is essential that there is agreement as to the goal. If indeed the objective is *governmental accountability*, then we concur with the recommendation of the Privacy Rights Clearinghouse that case information be gathered, but posted only in the aggregate, making personal identifiers unnecessary. Being able to see the number of orders of protection that a given judge issues on a monthly basis, or how many times domestic violence cases are dismissed or pled down to violations would be extremely helpful to the cause of offender and court accountability, without creating undue risks for the parties.

I would like to close with a story told by Fannie Lou Hamer that I'm sure some of you are familiar with. *Once there was a wise old man. He was so wise he could*

TRIBUNE

David S. Bralow
Sr. Counsel
(212) 210-2885

Law Department
220 E. 42nd Street
4th Floor
New York, NY 10017
Fax: (212) 210-2883
dbralow@tribune.com

HAND DELIVERY

May 30, 2003

Floyd Abrams, Esquire
Chairman
Commission to Examine Future
of Court Documents on the Internet
c/o New York State Unified Court System
25 Beaver St.
New York, NY 10004

Re: Statement of Newsday, Inc. and Tribune Company

Dear Mr. Chairman and Members of the Committee:

Newsday, Inc. and the Tribune Company are grateful for the opportunity to submit comments relating to issues that arise from providing access to court files electronically and through the Internet. Besides *Newsday*, the Tribune Company publishes 11 daily newspapers, including the *Chicago Tribune, Los Angeles Times, Orlando Sentinel, South Florida Sun-Sentinel, Baltimore Sun* and *The Hartford Courant.* It also operates 26 television stations throughout the country, including WPIX in New York and WEWB in Albany.

My name is David Bralow and as Senior Counsel for Tribune Publishing, I am pleased to take this opportunity to address the issues before this committee.

A. The Policy and Presumption of Access

As with any discussion about access to judicial records, particularly electronic copies of court records, the starting point must be the acceptance and reaffirmation of a commitment to an open and transparent judicial system. The United States Supreme Court described such openness of process as "an indispensable attribute of any Anglo-American" jurisprudence. Richmond Newspapers, Inc. v. Virginia, 488 U.S. 555, 569 (1980). But the tradition pre-dates modern observation. In 1820, when M. Hale wrote The History of the Common Law of England, (6th ed. 1820), he extolled the value of judicial transparency because: It discouraged perjury and the misconduct of the trial participants and assured that decisions were not made as a result of secret bias or partiality. Indeed, commentators as early as W. Blackstone in 1583 and J. Wigmore on Evidence in 1765 have recognized the important benefits of access to judicial proceedings and records. To Justice Oliver Wendell Holmes, the privilege that arises from reporting on judicial proceedings and access to those proceedings "stand in reason upon common ground." Crowley v. Pulsifer, 137 Mass. 392, 394 (1884).

This "prophylaxis" of access is acknowledged in every state in this country. Its recognition is rewarded by presuming access to judicial records and proceedings and by requiring those that seek to prevent access to judicial records to demonstrate a compelling interest to justify such closure.

It is our position that any debate about access to these same judicial records in an electronic form or through the Internet must be informed by the same presumption. Discrimination between byte and paper – the imposition of restrictions on one but not the other -- requires a demonstration that access to the electronic record causes a qualitatively different effect than access to the paper record. And the difference, itself -- not simply the information -- must jeopardize some compelling interest. See e.g. In re: Petition of Post Newsweek Stations., 370 So.2d 764 (1979) (this standard is a reiteration of a standard created when cameras were permitted in Florida courtrooms).

To recognize such a difference threatens the presumption of access, itself. If access to judicial records is presumed to be in the best interest of the community in which we live -- and that is not doubted -- how can permitting more convenient, more accurate access to those same records result in a compelling threat?

If anything, the removal of barriers to courthouse records empowers the citizen in a way that was arguably lost in America and reinvigorates a core value associated with public observance of the judicial system. As the United States Supreme Court recognized in Richmond:

> In earlier times, both in England and America, attendance in court was a common mode of "passing time." With the press, cinema and electronic media now supplying the representations of reality or the real life drama once available only in the courtroom, attendance at court is no longer a widespread pastime. Yet [i]t is not unrealistic even in this day to believe that public inclusion affords citizens a form of legal education and hopefully promotes confidence in the administration of justice. Instead of acquiring information about trials by firsthand observation or by word of mouth from those who attended, people now acquire it chiefly through the print and electronic media. In a sense, this validates the media claim as functioning as a surrogate for the public.

448 U.S. at 572-73, (citations omitted). By providing records electronically, the court system has the possibility of restoring direct citizen contact with the judicial system and removing a media filter.

B. Tangible Benefits to the Public and the Media

This is not to say that *Newsday* and Tribune believe that the Press's function will be made obsolete by any such direct citizen involvement. To the contrary, we believe that access to judicial records in an electronic form improves the media's ability to fulfill our mission. Electronic access increases timeliness and accuracy and offers the reporter tools to discern trends that affect society and the judicial system.

Timely examination of court records is an indispensable part of the newspaper's craft and access to the records electronically will allow greater accuracy and more complete reporting. This is true not only for long-term projects, but it is also essential for daily journalism and articles that get published on deadline.

For daily reporting, this cumbersome and out-dated means of storing and retrieving information on important judicial developments creates a news barrier that burdens the newspaper to the disadvantage of

its readers. In addition to the burden on the court personnel to retrieve and copy files, sometimes, the "hard copy" paper method makes it impossible for the reporter to gather critical information. There are numerous incidents when our reporters are stymied and the readers deprived because the court file is in the judge's chambers or in the possession of attorneys. If access were permitted online, a newspaper could rely on the court file rather than the exigencies of extra-judicial statements.

There are other logistic considerations. In Suffolk County, for instance, there are state courts in five different locations - some 30 miles apart - and court clerks' offices in two of those locations. Court personnel often cannot locate a file or even say what courthouse the files is in. A reporter or any citizen is forced to drive back and forth just trying to find the file. The same holds true in Nassau County, even though the courts are closer together - 15 miles apart at most - but anyone who has driven there knows that traffic eats up valuable time even more so than distance.

There are other problems that can be resolved by electronic access. Without the benefit of authority or a sealing order, clerks, attorneys and prosecutors remove documents from files, even in criminal cases, based on the mere belief that the document should not be public or will impair an ongoing investigation. An electronic records retrieval system will compel trial participants to seek appropriate sealing orders rather than exfoliating the file.

Electronic filing may also resolve problems with uniformity. For example, a Newsday reporter examined hundreds of Surrogate Court files to document the fees attorneys received in trust and estate cases. Sometimes, the petition for fees and the Judge's order establishing the fees were missing. While the Courts have recently revamped its rules to protect against such lapses, we believe a process whereby material submitted to the Court is immediately placed online would solve this problem.

In addition to enhancing the accuracy and timeliness of coverage of specific cases, our ability to serve the community with complete and accurate news is enhanced when full text searching is permitted. That type of functionality permits the public to locate court records applicable to particular subjects.

Access to judicial records have helped Newsday produce articles of profound impact. For instance, Newsday published a series about Catholic priests who were allowed to continue their ministries despite being accused of sexual abuse. Another series focused on the prevalence of inmates who were beaten by correction officers and the medical care of inmates at the county jails. Critical information for both series originated from court records that had to be reviewed at the courthouses by reporters. However, without access to the files online, the process was expensive and time-consuming, creating barriers both to the Press and the public. With online access and full text searching, we can do in depth reporting more often and with greater insight and accuracy.

If full search access is not economically feasible, at a minimum, we request the ability to search using names of the parties, the county, attorneys/law firms of record, case or index number. It is only with an index system that that an electronic filing system is useful.

C. Countervailing Interests in Privacy and Identity Theft

Against this backdrop which validates society's interest in an open judiciary, I do not ignore the concerns expressed about potential infringements on informational privacy and threats of identity theft. I have several observations.

First the notion of privacy must be defined with specificity before it can be addressed in a meaningful way. Privacy is an elastic concept. The unexamined trend is to distort that concept to unrealistic expectations of anonymity, comprehending even common information that is routinely found on the public street, in a phone book or on the Internet. Such an unspecified, generalized concern, cannot be the starting point for evaluating competing interests between access to judicial records and privacy. Furthermore, in New York, the notion that some information is private demands even greater attention because this State does not recognize a cause of action for disclosure of private facts.

As I stated above, before a notion of a private fact can meaningfully restrict access to a judicial record, the fact, itself, should be examined in relation to the harm caused by permitting it to reside in an open court file. This is nothing more than restating that individual judges are in the best position to protect whatever privacy right exists in any specific court files. There have always been adequate measures for

litigants and third parties to request the sealing of information based on well-established -- albeit difficult to meet -- standards. Furthermore, courts have been uniquely qualified to balance the harm against the presumption of access in case-by-case determinations. Requiring a court to determine the precise effect of online access to any specific judicial record neither significantly expands judicial labor nor requires a Court to make a decision without well-recognized standards .

A hypothetical toxic tort claim in context of Internet access to the judicial file illustrates the point. Assume that a lawsuit is filed in Nassau County against a chemical company that involves personal injury claims. The court file will, by necessity, contain medical information.

A motion to seal the file because of medical information would be evaluated on the particularized harm that arises to the individual and balanced against the necessity for public information on a subject of public importance. Furthermore, all courts recognize that when an individual seeks a remedy based on his or her medical condition, information that might be considered private in one context is no longer private when that medical condition is an integral part of the proceeding. Without some demonstration of a particularized and compelling reason for sealing, under these circumstances there would be no grounds for sealing such material. To do so, would be to ignore Craig v. Harney, 331 U.S. 367 (1947), that what transpires in a court is "public property."

The fact of the Internet and greater availability to the file cannot change the nature of the analysis. How can public information become private because a reporter now can review the court file at her office and his home? Can the public nature of this information change because of the technological advances that make access easier? I think not. But if there is some change in status that arises from greater access, the harm must be evaluated in a precise and non-speculative way. In other words, there must be some enunciated and demonstrated qualitatively different effect that arises from electronic access than that arising from access to the paper record.

This leads to the issue of identity theft. As a practical matter, I am not aware of significant problem of identity theft arising from access to judicial records. Indeed, the most common causes of identity theft are relatively low tech and do not involve court files, whatsoever.

Indeed, one cause of identity theft is rummaging through the trash for bank statements and discarded credit card offers. Identity Theft: Is there Another You?: Joint Hearing Before the House Comm. On Commerce, Subcomm. On Telecomm., Trade and Consumer Prot. And Subcomm. On Finance and Hazardous Materials, 106th Cong. 18 (1999)(statement of Jodie Bernstein, Director, Bureau of Consumer Protection, FTC). Stealing a purse or wallet is another common source of the problem. Other causes are taking out false driver's licenses, creating utility accounts under another's name, establishing false bank accounts. Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Senate Comm. On Judiciary, Subcomm. On Tech. Terrorism and Gov't Info., 106th Cong. 32 (2000). In TRW, Inc. v. Andrews, 534 U.S. 19 (2001), the first United States Supreme Court case addressing the issue, a secretary in a doctor's office copied the social security number from a patient's initial referral form. In a survey of literature available, there are very few anecdotes, if any, that make a connection between judicial records and identity theft.

This is not to say that the court system through judicial rule or the Legislature through statute may not find that some information is worthy of protection. Furthermore, it is equally possible that the judicial system may seek to reform what information should be required in the court file. But before limitations on access to court files on the Internet are imposed as a general rule because of fears of identity theft, this panel should seek empirical information that demonstrates that judicial records contribute to this risk and that risk is somehow greater because of access to the Internet.

This is simply a restatement of the initial standard discussed above -- that electronic access to judicial records should only be limited when it is demonstrated that there is a qualitatively different effect than access to the paper record.

I thank you for the opportunity to provide this input and I remain available to answer any questions.

Yours truly,

David S. Bralow

Copies to:

Commission Members:

Stephanie Abrutyn, Esq.
Tribune Company
New York, NY

Yochai Benkler
Professor, New York University.
School of Law
New York, NY

Elizabeth Bryson, Esq.
Corporate Vice President,
New York Life Insurance Co.
New York, NY

Joseph Lelyveld
former correspondent and
editor of The New York Times
Bronx, NY

Christopher E. Chang, Esq.
Law Offices of Christopher E. Chang
New York, NY

Julie Domonkos, Esq.
Executive Director, My Sister's Place
White Plains, NY

William P. Farley, Esq.
The McGraw-Hill Companies, Inc
New York, NY

Maria Imperial, Esq.
Executive Director, Association of the
Bar of the City of New York Fund, Inc.
New York, NY

Pamela Jones Harbour, Esq
Kaye Scholer LLP
New York, NY

Victor Kovner, Esq.
Davis Wright Tremaine LLP
New York, NY

Hugh Campbell, Esq.
Rodman and Campbell P.C.
New York, NY

David Miranda, Esq.
Heslin & Rothenberg, Farley & Mesiti, P.C.
Albany, NY

Hon. Gail Prudenti
Presiding Justice, Appellate Division,
Second Department
Brooklyn, NY

Charles S. Sims, Esq.
Proskauer Rose LLP
New York, NY

Thomas F. Gleason, Esq.
Gleason, Dunn, Walsh & O'Shea.
Albany, NY

Norman Goodman, Esq.
County Clerk, New York County
New York, NY

Hon. Victoria Graffeo
Justice, New York State Court of Appeals
Albany, NY

Richard F. Griffin, Esq.
Philips Lytle Hitcock Blaine & Huber
Buffalo, NY

Gary D. Spivey, Esq
New York State Reporter
Albany, NY

Charles A. Stillman, Esq.
Stillman Friedman Shaw, P.C.
New York, NY

Nadine Strossen
Professor, New York Law School
New York, NY

STATEMENT TO THE COMMISSION ON ACCESS TO COURT RECORDS

David Tomlin, The Associated Press

May 30, 2003

Members of the Commission, good afternoon and thank you for giving me the opportunity to appear before you today on behalf of The Associated Press.

My name is David Tomlin, and I am assistant to the president of AP at our headquarters here in New York City. Although I am an attorney and some of my work at AP is now performed in that capacity, I was admitted to the bar only a little more than a year ago. Most of my 30-year AP career has been as a journalist and news executive, and therefore much of what I will submit today for your consideration is offered from that perspective.

The Associated Press is a mutual news cooperative operating under the Not-for-profit Business Corporation Law of the state of New York. We trace our history and name to an association of New York City publishers formed in 1848. The members of this association believed they could reduce the cost of gathering news from distant locations by sharing it. It turned out to be an excellent idea that spread to other regions, and in 1901 newspapers throughout the country formed the corporation that has become today's AP.

The AP cooperative now numbers 1,700 daily and non-daily newspapers and 5,000 broadcast stations among its members. We have 147 bureaus and offices nationwide, at least one in every state. We also serve 8,500 newspapers and other customers outside the United States and maintain permanent operations in 95 countries.

We produce news reports in words, photos, informational graphics, audio and video. Our services range from international news reports in five languages, to reports that contain only the news of individual states.

Here in New York, we serve 72 newspapers and 150 broadcast stations with our New York state and New York City news reports. We have a large metro staff in New York, another substantial bureau in Albany, and smaller offices in Buffalo, Rochester, Syracuse, Garden City and White Plains.

I will begin by stating for the record that AP accepts and agrees with the general principles articulated already by other media representatives you have heard from.

We believe that constitutional, statutory and case law require a presumption of openness for all court records.

We believe that the showing demanded of anyone seeking to overcome this presumption is and should be rigorous.

We believe that when such a showing is successfully made, the restrictions to access should be narrowly targeted to the interests that have been shown to require such protection.

We believe that the appropriate way to assure that these principles are observed is on a case by case basis.

And finally, we believe that the manner of access to court records does not change these principles. What governs access to the paper records in the courthouse applies equally to electronic records accessed from a kiosk or across the Internet from a remote location.

AP recognizes that even if all these principles are accepted without qualification, the commission has many practical issues to resolve. The list of questions you have set out to frame these hearings capture many of the hardest ones.

But we see none that cannot be resolved, and we are excited by the rewards and opportunities that will ensue in the form of news reporting that can more powerfully serve both the interests of justice and the public interest.

With our statewide coverage of the news of New York city and state, and our national perspective arising from our operations in all 50 states and the nation's capital, we think AP is uniquely situated among news organizations to see where electronic access to court records can eventually lead.

We cover particular stories that emerge from proceedings in individual courthouses in every county and state. And we also produce stories that draw on information gleaned from records in dozens, or even hundreds of courthouses.

For example, AP reporters spent much of the year 2001 documenting the systematic expropriation of rural land owned by black families through abuse of the executive and judicial powers of government, and through barely concealed fraud.

The series required access to records from hundreds of courthouses throughout the southeastern United States, including civil and criminal court proceedings. It took months of reporter time and a large travel budget to do the job.

Much more recently, an AP reporter made extensive use of case files to help prove the innocence of three mentally disabled defendants in Alabama who were charged in the death of a newborn baby which it turned out never existed.

And an AP reporter is at work as we speak on a series that will examine whether changes in rates of specific crimes in the U.S. and abroad are being caused by deportation of aliens convicted of felonies. Because federal immigration authorities don't track the particular crimes that deportees committed, we need to search state court records for that information. As matters stand, much of the information we need will only be obtainable if we travel in person to where it is stored.

In all these cases and countless others, the time and expense involved is daunting. Projects that do not show at least the promise of compelling results are unlikely to attract the resources.

Simply put, electronic access to court records will produce more journalism of higher quality,

and the effect will multiply as such access spreads to more states.

Such stories are among the kinds of journalism that press freedoms are designed to encourage and protect. At their best, they can reverse injustice, increase public interest in and knowledge of the justice system, and help guide public policy makers to strengthen what works well and fix what doesn't.

We at AP know that electronic access of the volume and scope we envision will not come easily, that this Commission must consider the potential for harm to privacy interests, to public safety and to the integrity of the judicial process in developing its recommendation.

But great opportunities always come associated with some risks. Progress usually comes to those whose first determination is to seize opportunities, rarely to those for whom avoiding or minimizing risks is the paramount consideration. We hope the former spirit is the one that motivates this Commission.

Thank you again for giving AP a chance to be heard, and good luck to you in your work.

To: New York Commission on Public Access to Court Records

From: Media Law Committee of the New York State Bar Association

Date: May 30, 2003

I am Edward Klaris[1] and I want to thank the Commission for permitting me to make a presentation on behalf of the Media Law Committee of the New York State Bar Association.[2] The Media Law Committee is comprised of attorneys who specialize in issues relating to the First Amendment and privacy.[3] We represent news organizations and reporters and firmly believe online access to court records will allow for more quality journalism and improve the public's knowledge of the court system and court proceedings without compromising New York's protection of privacy interests.

Currently, searching court records is something of an ordeal; many people work or live miles away from courthouses, making it near impossible to visit the courthouses when they are open. Simply tracking down the correct courthouse in New York City can be overwhelming for reporters and members of the public trying to find information about a particular case. Electronic access to court records would allow for efficient searches of important information about attorney and medical malpractice, dead-beat parents, corporations charged with fraud, products claimed to be defective and other information that is currently very difficult to find. Moreover, not only the mainstream New York press would be able to search through court records. Out-of-state newspapers, broadcasters and websites; public interest organizations; and many others could make use of these records, causing more direct oversight of the courts and contributing to discussions of public issues.

An online database would give private citizens and non-experts access to the same material available to lawyers and government officials. As the Supreme Court noted in the Richmond Newspapers case, "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."[4] Making court records available on electronic networks would permit greater understanding of judicial decision-making, provide everyone in society meaningful access to important cases in the system and continue to improve the

---

[1] General Counsel, The New Yorker, Four Times Square, New York, New York 10036.

[2] This statement does not represent the position of the New York State Bar Assoc House of Delegates.

[3] The Media Law Committee is chaired by Slade Metcalf. The members include: Andrew Ian Bart, Richard A. Bernstein, Robin Bierstedt, Thomas M. Blair, Jennifer A. Borg, Zachary W. Carter, Jan F. Constantine, David T. Fannon, Alice L. Fradin, George Freeman, Kevin W. Goering, Michael J. Grygiel, David V. Heller, David J. Kerstein, Edward J. Klaris, Stefanie S Kraus, Richard A. Kurnit, Joel L. Kurtzberg, Matthew A. Leish, David E. McCraw, Elizabeth A. McNamara, Robert E. Moses, Eileen Napolitano, Lesley Oelsner, Nicholas E. Poser, Robert L. Raskopf, Muriel H. Reis, Madeleine Schachter, Elise S. Solomon, Katherine Aurore Surprenant, Susan E. Weiner, Jack M Weiss, Richard N. Winfield, David B. Wolf, David A. Schulz. Members serve on the committee in the their individual capacities, not as agents for their employers; views expressed herein or otherwise are not on behalf of members' respective employers, nor do the views necessarily reflect those of the employers.

[4] Richmond Newspapers, Inc. v. Virginia, 488 U.S. 555, 572 (1980).

tradition of openness that is part of the culture and law of the New York court system. These benefits are best achieved with full-text searching and easy access to all cases rather than having to input the name of the case to conduct a search.

In the context of electronic access to court records, the doctrine of "practical obscurity"[5] and concerns over privacy are misleading and do not apply. The current system of open court records works quite well and it would be a mistake to impose a new system of court secrecy in which categorical and preemptive determinations limit access. These decisions are best made on a case-by-case basis, upon a motion by the party seeking to either seal the records entirely or to curtail their availability.

The Commission is by now well aware that the U.S. Supreme Court made clear in Nixon v. Warner Communications, Inc.,[6] that the public enjoys a common law right of access to judicial records. The "presumption of openness" can be reversed only by showing an "overriding interest based on findings that closure is essential to preserve higher values."[7]

New York Rule of Court 216.1 requires judges to consider not only the parties but also the "interests of the public" and provide a written finding of "good cause" before sealing court records. The rule undergirds New York's strong public policy in favor of open court records. New York courts over the past decade have consistently relied on Rule 216.1 to deny requests to seal court records even where all parties were in favor of sealing the case. For example, in a case decided in 2001 involving the proprieties of an estate accounting and personal finances, the First Department upheld a Surrogate Court judge's denial of a joint motion for protective order to seal the settlement agreement. In that case, named In re Hofmann, the court in denying the motion noted that, even where all parties agree to seal the records, "[c]onfidentiality is clearly the exception, not the rule, and the court is always required to make an independent determination of good cause." [8]

Would the Appellate Division's analysis in In re Hofmann or other cases change if court records were available electronically? We do not think so. For decades New York courts and the legislature have rebuffed privacy advocates' attempts to create generalized privacy torts such as one for publication of private facts. On the other hand,

---

[5] Many people who fear electronic access point to the 1989 Supreme Court Reporters Committee case where the concept of "practical obscurity" was first articulated.[5] But that case has been misconstrued in the context of access to court records and ought to be disregarded by the Commission. The Reporters Committee case concerned a FOIA request for records of the executive branch, not an access motion for court records. Specifically, Reporters Committee involved FBI "rap sheets", which are multi-state summaries of an individual's criminal history and include "descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations."[5] Rap sheets are not documents filed in a courthouse. Rather, the FBI gathers this information from law enforcement agencies at all levels of the federal and state governments.[5] Here the public would simply have electronic access to "the source records themselves"—the same court files that are accessible today through physical inspection. Electronic access will make the inspection of public records easier. But making inspection of a public court file easier does not invade the privacy of any litigant.

[6] 435 U.S. 539 (1978),

[7] Press Enterprise Co. v. Superior Court., 464 U.S. 501, 510 (1984).

[8] In re Will of Renate Hofmann, 287 A.D.2d 119, 733 N.Y.S.2d 168 (1st Dept. 2001).

where the benefits of confidentiality in court records clearly outweigh the presumed benefit of transparency, New York already has several rules and statutes to cover this. For example, state statutes currently permit courts to seal records in family law, matrimonial and juvenile cases. The New York Public Health Law and the New York Mental Hygiene Law are the principal statutory sources of New York law that require health information to be held in confidence. Additional health-related statutes cover specific situations (e.g. HIV and AIDS patients[9], disclosure of health records in litigation[10], and the collection of statistical information by various governmental agencies). These rules would continue to apply in the electronic environment.

Congress has also passed a number of federal laws that protect certain kinds of information: HIPPA protects health information[11]; Gramm-Leach-Bliley protects financial information[12]; FERPA protects educational information[13]; COPPA protects information about children[14]; the Driver's Privacy Protection Act protects drivers' license applications and information[15]; and there are more.

With all these privacy-related laws, the chances that highly confidential information will be filed with the court in litigation have been significantly reduced. Even where such information may be turned over in discovery, only a tiny percentage of discovery information and materials are actually filed with the court, and, of course, the First Amendment does not require that non-parties be given access to discovery material that has not been filed in the clerk's office.

Perhaps the greatest fear of electronic access to court records is that information may be used in identity theft -- where a person's social security number, credit card and bank account information are appropriated and used illegally. While identity theft is a serious concern, blocking access to certain electronic court records is not the answer. Strict enforcement of the existing criminal laws and the proper implementation of state and federal privacy legislation will deter such behavior. In addition, there is no evidence that court records would ever be a good place for would-be criminals to obtain social security, credit card and bank information, while there is ample evidence that such information can be obtained elsewhere on the Internet and through criminal rings that collect the data from co-conspirators at banks and retailers. Speculative and remote fears about deviant behavior should not cloud this Commission's recommendations. This Commission should support electronic access to court records and endorse the current rule of law and good public policy in New York, which already properly balances privacy in court records with the First Amendment.

---

[9] N.Y. Public Health Law § 2134.

[10] In a court proceeding in New York, specific providers (physicians, dentists, podiatrists, chiropractors, nurses, professional corporations, medical corporations and other "person[s] authorized to practice medicine") are not permitted to disclose information which ws acquired in attending the patient and which was necessary to enable him to act in the capacity. CPLR § 4504 (rule of evidence).

[11] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (1996); 45 C.F.R. pts. 160 & 162.

[12] 16 C.F.R. § 313.

[13] Federal Education Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regs., 34 C.F.R. part 99.

[14] Children's Online Privacy Protection Act f 1998, 15 U.S.C. §§ 6501-6505.

[15] 18 U.S.C. §§ 2721-2725 & Pub. Law No. 109-69, §§ 350 (c), (d) and (e), 113 Stat. 986, 1025 (1999).

In conclusion, we suggest that this Commission recommend that New York court records be made available electronically, utilizing the same rules of openness followed by the current New York court system. Doing this will increase the efficiency of the judiciary and, correspondingly, make the records system available to all citizens so that they may monitor the integrity and efficacy of the courts. We do not request that New York expand the types of records available to the public. Rather, we simply would like New York to provide broader and more efficient access to records that are already public.

Testimony of George Freeman,
Assistant General Counsel of The New York Times Company,
to the Commission on Public Access to Court Records, 5/30/03

I am George Freeman, Assistant General Counsel of The New York Times Company, and am very appreciative of the opportunity to speak to you today. I am, of course, more than happy to answer any questions you may have.

I would start today by urging the Commission to ensure that we inadvertently do not use the opportunities technology is presenting us with to take a step backwards. What I fear the most is that because of the ready access computerized judicial records would bring, a possible -- and certainly ironic -- result might be to tilt the balance we now have with respect to all court records -- whether those in hard copy in court files, or those in electronic form -- to more closure, to more redactions and to more sealings. While privacy interests certainly ought to be respected, they are amply taken into account in the balance we have in the current regime. With the increased focus on privacy interests which the electronic world inevitably brings, we should be vigilant to ensure no pushback on the openness to judicial documents which are the very hallmark of our wonderful judicial system. The very possibility that, because of the opportunity to disseminate judicial records through the new technologies, access to records should

somehow become less public and more shielded is not only ironic, it is antithetical to the very advantages which the public can gain from the Internet.

On that point, it should also be borne in mind that any regulation aimed at electronic files may in relatively short order amount to regulation of all court files, as paper records may well disappear entirely in our lifetimes. Again, any tilting of the balance between privacy interests and openness towards the privacy end of the spectrum -- even only with respect to electronic records -- may achieve the very opposite result of the advantages to public access which the new technology offers. Since it is possible that in the future the only files that exist will be computerized, we should be very wary of creating any new rules for that medium which differ from those currently applied in our courthouses, because ultimately the Internet may become the only game in town.

Assuming, then, that we agree that the new technologies and this new initiative should not result in the diminution of openness in our courthouses, what are the advantages of a transition to electronic case files? The practical importance of the change cannot be overstated, and in most cases it is entirely uncontroversial. A paper copy of a document filed in court (i) requires a trip to the courthouse to inspect or copy once one figures out the

correct courthouse to visit; (ii) is available for such inspection and copying one person at a time; (iii) is available only during business hours; (iv) may be archived in a dusty warehouse and be hard to find only years after it is filed; (v) may be in use at trial or in chambers and, hence, not available in the clerk's office; (vi) typically can be copied only by very patient people with vast amounts of pocket change on antiquated photocopying machines; and (vii) must be manually searched for relevant information by, generally, uninformed agents for the parties actually seeking the information, and then (viii) is only truly retrievable if such party knows the exact caption or case number of a specific litigation. Clearly, access is only for the very determined and very resourceful. Electronic records solve all of these problems. We applaud the judiciary for its efforts in this area.

The notice for these public hearings suggests a limited number of areas in which restrictions on electronic access are being considered where no limitations currently exist with respect to the paper records. We view these suggestions as unwise, unwarranted and constitutionally suspect.

First, there are adequate measures available for litigants and others to request the sealing of such information in our current procedures, although the standard is, properly, a difficult one to meet. What seems quite problematic is to set up a scheme of discriminatory access, where the rules

with respect to hard records are different than those with respect to electronic records.

Before discussing why we believe the same rules ought to apply to both media, that is, why any system in which the two standards don't mirror each other is unwarranted, allow me briefly to underscore the advantages of openness -- advantages which of course are all the greater if they truly can be brought to the public rather than only those members of the public with the time, knowledge, inclination and money to actually go to a court clerk's office, a place where, frankly, I, who have litigated in New York for now some 27 years, fear to tread.

The Supreme Court's rationale in the watershed case of *Richmond Newspapers*, which stood for the presumption of public access to courtrooms and court files, applies equally to the benefits of making court records more accessible to the public. Thus,

- Ready public access to court documents promotes more discussion and understanding of the judicial system. 448 U.S. 555, 571-73, 577, n.12
- Ready public access gives greater assurance "that the proceedings were conducted fairly to all concerned" 448 U.S. at 569-70, and

serves as a check on corrupt practices by exposing the judicial process to broader public scrutiny. 448 U.S. at 570.

- Ready public access to statement made in court documents even about obsentsibly "private" matters can prevent perjury and other abuses 448 U.S. at 569 (Openness "discourages perjury, the misconduct of participants and decisions based on secret bias or partiality").

Many times, given the tension between privacy interests and access, and, indeed, in the now 16 year battle in this state about cameras in the courtroom, the participants in these struggles forget about what it is we have in common -- and that is an interest not only in the fair workings of the judicial system, but, I would submit more important, how important it is that the public perceives the judicial system as working fairly. That really ought to be paramount in any inquiry such as this, particularly in today's environment where, sadly, lawyers, judges, and the judicial system in general, are not though of terribly highly by the public -- indeed, not much more highly that even lowly journalists. Whether it be O.J., whether it be bribe-taking state judges, whether it be the perception that *L.A. Law* is the law, whether it be the lack of understanding of our adversary system and why defendants are entitled to all sorts of due process, the judicial system is not held in the high esteem it should be -- and for the very reasons

articulated by Chief Justice Berger for a unanimous Supreme Court, more openness is one important way to improve that very paramount problem.

While there has been testimony about privacy interests -- and we believe that much of the fears of openness on the Internet is more speculation than reality -- we should underscore, especially from a newspaper's point of view, the great advantages of electronic access and full-text searching capabilities. First, it would allow better reporting on the judicial system and on specific cases. A paper like The Times reports on cases throughout this big Empire State -- from Dutchess County (home of the Tawana Brawley case) to land issues in the Adirondacks, and timely and accurate reporting – relying more on court records than the spin of lawyers on the phone -- would be greatly aided if a reporter in New York had access to files in the clerk's office in Poughkeepsie.

Second, electronic access would allow improved and better reporting on a variety of matters. As one who comes from a building currently in turmoil, a problem created in part by the lack of checking with respect to an employee's background, it seems obvious that the ability for the press and public to have better access to, for example, check upon the background of potential employees is a good thing. Whether it is a newspaper being able to get access to court records about a candidate for the judiciary or any other

person running for public office; for a newspaper, or for that matter, any employer to have the ability to more easily check the true (and sworn) background of potential employees in sensitive and important professional or executive positions, there are a myriad of advantages to get more information more easily, about such high-placed people in sensitive jobs, or for that matter, about the past history of those charged with crime. Moreover, it's not just about people. Newspapers could better report about companies deceiving the public, about products claimed to be injurious, and so on.

Against these advantages, it is hard to see the disadvantages of intrusiveness. First, someone who really wants to get a lot of background about an individual, can probably do so without this new initiative. Thus, the Internet already provides access to all sorts of personal information about people, often well beyond what would be filed, and not redacted or sealed, in Court. Hence, in a very real sense, the cat is already out of the bag. Second, the balance has already been struck between privacy and openness in the standards which currently exist for protective orders, seals, and the like. Third, it is, of course, the case that in many of the fora in which potentially private information exists, the law currently permits courts to seal such records, such as in family law and juvenile cases; I'd also point out that

another area often mentioned as an area of concern, the bankruptcy courts, are federal, and hence, beyond the purview of the Commission.

Thus, I would close by saying that we believe the balance that exists now properly takes into account privacy interests as well as the great public advantages to openness, and that in embracing the new technologies, we should not alter that balance, but should welcome the added public access which the Internet brings. To the extent that the Commission believes that the rules for openness of electronic records should not exactly mirror the current rules with respect to paper documents generally, we would submit that, consistent with the Supreme Court cases, the burden must be on those favoring more restrictive rules to show a compelling reason, based on real evidence and not just speculation, on why a system that discriminates between media should prevail. If the Commission believes that such a burden has been met, the exceptions should be extremely narrowly tailored, to include only a closed, specified set of so-called identity data -- social security number, credit card numbers, bank account numbers, and nothing else -- and should be blocked from access not automatically but only upon an appropriate showing. I would reiterate that we do not think that any such discrimination is warranted, but if politically the only way to achieve the progress which the Internet makes available is by such a narrow and clearly

defined restriction, after clear evidence has been shown that it is substantially probable that real damage will occur, we could understand why such a tradeoff might be made.

Testimony of
Hilary Sunghee Seo, Esq.
Domestic Violence Advocate,
Sanctuary For Families'
Center For Battered Women's Legal Services

before the
Commission on Public Access to Court Records

May 30, 2003

Thank you for giving us an opportunity to testify before you today. Sanctuary For Families' Center For Battered Women's Legal Services is the oldest and largest legal services organization in New York State dedicated to domestic violence victims. Last year, our staff and volunteer attorneys provided direct legal representation and advocacy to over three thousand battered women. We also lead community education and public advocacy efforts to help promote healthy relationships free of violence.

As citizens, attorneys and advocates of domestic violence victims, we embrace the general principle that the workings of the judiciary and court records are matters of great public interest. In a democratic society, the public not only has an interest in but a duty to inspect and hold accountable the court system. We recognize that with technological advances, there are significant potential advantages of making case files available to the public electronically – one of the main advantages being the ease with which information can be accessed.

However, ease of access also raises very serious privacy and safety issues for individuals who use the court system. By making court files available to the general public through the Internet with no significant restrictions, the courts essentially would be publishing that material to a worldwide audience. Such broad publication would provide

batterers and stalkers with a potent weapon to track down, harass and endanger victims. This is not an alarmist statement, but reflects our measured judgment based on our experience with tens of thousands of domestic violence and stalking victims and their abusers.

Why are we so concerned? I will outline our basic reasons and then go back to each to elaborate. First, we find in our work that batterers and stalkers generally are extremely obsessed with monitoring and controlling their victims. Many abusers terrorize their victims over many years, even after their victims have managed to "escape" for the time being. They often spend countless hours trying to track down their victims using any means available to them. Second, we find that the batterers and stalkers of our clients are often very savvy technologically. If court files are made available on the Internet, batterers and stalkers would spare no efforts in misusing that information to harass and endanger their victims. Third, while records from family court and matrimonial proceedings generally are not available to the public, court files from criminal and other civil cases are publicly available. Whether it be a criminal assault case involving rape or a sexual harassment case, case files will often contain personal and sensitive information about women that their batterers and stalkers could use to locate, humiliate and re-victimize them. More mundane cases involving landlord/tenant disputes or a minor car accident will likely contain some identifying information that could be used to endanger the safety of domestic violence and stalking victims. Fourth, in many cases, it will be difficult to predict beforehand what information could end up in the hands of an abuser and be transformed into a dangerous weapon. Unfortunately, once

sensitive information is released and made publicly available on the Internet, it would be almost impossible to undo the damage.

Let me now take a few minutes to elaborate on each of these points.

First, domestic violence and stalking are crimes that, at bottom, involve a desire to control and exert power over the victim. I would like to share with you the stories of two women. Both stories are rather typical of domestic violence and stalking victims, and illustrate how resourceful, thorough, and persistent abusers can be when it comes to finding ways of terrorizing their victims.

The first woman, J. S., was physically and emotionally abused by her husband. Besides beating her regularly and forcing her to have sex while he slapped her and verbally abused her, he isolated her by preventing her from working, forbidding her from leaving the house without his permission, calling her multiple times a day from his workplace to keep tabs on her, becoming angry at her if she talked to her friends or family over the telephone, and not giving her any money so that she would have to ask for his permission to buy even small items like toothpaste or feminine hygiene products. When she fled the house, he called every one of her relatives and friends until he eventually tracked her down.

The second woman, S.H., was a stalking victim. The stalker was someone she met briefly while volunteering at a community organization in South Korea. He followed her to her home one night and asked her out. When she said no, he started stalking her outside her home. He found out her work phone number and called her incessantly at work. He also stalked her at her workplace. After about a year, S.H. moved to New York to pursue her graduate studies. To her dismay, her stalker found out the name of

her school by contacting a fellow volunteer at the community organization, and took a plane and came to New York. He showed up at her school in New York causing her great fear. He also found out her phone number, email address and home address through the Internet and began to harass her. After a while, S.H. became so scared that she moved to a new location. But she is still afraid that her stalker may again succeed in tracking her down.

Like J.S.'s batterer, most abusers we encounter are obsessed with controlling and monitoring their victims. When their victims attempt to escape their sphere of domination, they often become even more aggressive and will go to great lengths to track down their victims. Like S.H., many stalking victims live in constant fear of being found out and re-victimized.

Second, in our work, we often encounter technologically savvy abusers who show enormous persistence and creativity in using the Internet to terrorize and humiliate their victims. The National Network to End Domestic Violence has observed that "the World Wide Web is far and away abusers' best tool for finding and continuing to harm their victims." It is not uncommon for abusers to spend hours scouring the Internet for potentially harmful information and spend many more hours disseminating such information to publicly humiliate their victims. To give just one example, T.J., a domestic violence advocate, had a client whose batterer was very Internet savvy. He was able to locate the confidential address of the domestic violence agency T.J. works for, even though her agency had gone to great lengths to keep the address confidential. He then created a website devoted to humiliating and terrorizing T.J.'s client and her support community. He posted the confidential address of the domestic violence agency on the

website, endangering the thousands of clients served by that agency. He also posted stories filled with what he claimed were intimate details of T.J.'s client's sex life. He did not stop there. He found T.J.'s photograph on the Internet and posted it, along with defamatory statements about T.J. using information he found about her on the Internet. This is not an atypical story. The fact is that the Internet is already a favored and extremely destructive weapon used by batterers and stalkers to terrorize and harm victims.

Third, making court records available to the general public over the World Wide Web would infuse the Internet with a large volume of information that previously was practically inaccessible except to those people willing to invest considerable time and energy to access such information. Providing electronic access to court records through the Internet is markedly different from giving the public access to those records during set hours in a set location – allowing indiscriminate Internet access would be more analogous to publishing that material to a world-wide audience and would change radically the potential usage of such information. Is such publication necessary to attain the goal of holding courts publicly accountable? Is it consistent with balancing the competing goals of public accountability and individual safety and privacy? What recourse would individuals have when such information is misused? What if the abuser resides in a foreign jurisdiction? We would urge the Commission to consider carefully these and other questions concerning individual privacy and victim safety.

While it is true that in New York, court records of matrimonial actions and family court proceedings are generally unavailable to the public, the case files of criminal and other civil cases *are* publicly available. Court records in these cases may contain

personal and identifying information that could be used by abusers to seriously harm victims. Also, New York has laws protecting the identity of victims of certain sex crimes. However, the protection does not apply unless the victim is prosecuted under very specific sections of the penal law. The identity of domestic violence victims or stalking victims whose perpetrators are prosecuted under the assault, harassment, stalking or menacing statutes would not be protected. Nor are there existing laws protecting the identities and identifying information of domestic violence or stalking victims involved in civil tort cases.

Let me give two examples to illustrate some of these points. Sarah, a battered woman, who was stalked relentlessly by her ex-husband, flees him and moves to another location. To protect her identity, she de-lists her phone number and is careful about giving out her address. She gets a new job but is terminated after she complains to her supervisor about sexual harassment and decides to seek redress in court. Her employment files which contain the name and address of her employer become available electronically because they become a part of the court's records. The case files also contain detailed information about how her boss sexually harassed her. Her batterer/stalker who is intent on finding her spends every Saturday evening scouring the Internet for information about her, and one day comes across her case. He is not only able to locate her through her work address but also threatens her that he will humiliate and embarrass her by posting all of the details of her sexual harassment case on the Internet and by mass-mailing the link to her family, friends and colleagues.

Here is a second example. Jessica is raped when she is 22. Her rapist is charged and convicted under an aggravated assault statute. Jessica testifies at the trial. Two years

after that, Jessica is sued over a minor contractual dispute. Because she proceeds *pro se* on the case, her case files contain her home address and phone number. The case eventually settles and is closed. A year later, she becomes a victim of acquaintance stalking. She tries very hard to keep him from finding her home address because she lives on a relatively isolated street, but he is able to locate her by searching electronically through case files using her name as a search word. He also finds out that she had previously been raped and begins sending her letters recounting graphic details from that case. Jessica is terrified and emotionally traumatized.

As these examples illustrate, because a woman who is currently not a victim of domestic violence or stalking could become one in the future, and a past victim of domestic violence or stalking may find herself embroiled with the courts in the future, it will be difficult to predict at any given point what information may become transformed into a weapon in the hands of an abuser.

Moreover, even with respect to more predictably sensitive categories of information, such as name, social security number, direct or indirect geographic locators such as home and work addresses, telephone number, email address and bank account information, it concerns us greatly that the guardians of such vital information would be understaffed, albeit hardworking, court personnel who may be technological novices. Also, women who have in the past been battered or stalked may in some cases ask courts to seal potentially harmful information on a case-by-case basis. But in many circumstances, they may not have the foresight or the resources to make such a petition to a court or the ability to persuade a judge that information which appears harmless on its face could potentially harm their safety. Finally, future victims of domestic violence or

stalking would have no way to undo the fact that because of cases they were a party to or a witness in in the past, there exists a body of sensitive and personal information about them that is available to the public through a court's website. Once potentially harmful information is made available on the Internet, whether because of clerical mistake or because, at the time of the posting, there was no reason to believe such information would jeopardize anyone's safety, it would be impossible to undo the damage.

We believe that the public's interest in conveniently accessing court records should never take precedence over the safety of people. We also believe that a woman should never be made to feel that in seeking redress under the law, she may be jeopardizing her safety because personal and sensitive information about herself would be made indiscriminately accessible to anyone.

I would like to end by underscoring the fact that intimate partner violence is extremely pervasive in our society. The safety issues I have highlighted are of grave concern to millions of women and the numbers are even greater when the victims' children, family members, friends, advocates and other support community are taken into account. According to a recent survey co-conducted by the National Institute of Justice and the Centers for Disease Control and Prevention, nearly 25 percent of all women in the United States are physically assaulted by an intimate partner over their lifetimes. This translates into approximately 26 million women across the nation. According to a recent survey conducted by the National Institute of Justice, about 8 percent of women are stalked over their lifetimes, or about 8.2 million women nationwide. These numbers are staggering. And as Charlotte Watson testified before you earlier today, over a

thousand women are killed each year by their partners *after* fleeing. Countless more are re-assaulted after they have supposedly escaped.

We thank and commend the Commission for the care with which it is approaching this extremely important, complex and sensitive topic. We urge the Commission to proceed with care, being mindful of the safety of the millions of women that your decisions will affect.

Thank you.

Submission of the Office of the
New York State Attorney General to the
New York State Commission On Public Access To Court Records

(Testimony of Kenneth Dreifach, Chief,
Internet Bureau, Office of Attorney General, May 30, 2003)

The below testimony is respectfully submitted by the New York State Attorney General, in response to the Notice of Public Hearings of the New York State Commission on Public Access to Court Records (the "Commission").

1. The Purpose of this Submission

The Attorney General recognizes at the outset that court records are presumed public, and that vital public purposes are served by this tradition. Nonetheless, this Commission has the difficult task of balancing the traditional values of open records against real, practical concerns arising from the capabilities of new technology. As the former values are well-documented, we address only the latter, which reflect recent developments and trends.

The purpose of this testimony, however, is not to prescribe the precise balancing that should be undertaken as to these competing factors, or the specific procedures that should be implemented. Those determinations, of course, are for the Commission. Rather, we undertake merely to outline certain of the privacy and security interests that the Commission may wish to consider, such as the frequent use of personal information for identity theft or other potentially harmful activities.

We address two similar but distinct concerns, those of "security" and "privacy." In reaching its conclusions, we ask that the Commission consider basic security concerns that arise when personal identifying information is easily available to identity thieves – *e.g.*, data reflecting

banking information, social security and credit card numbers, or other similar personal and financial identifiers. But we also ask that you consider the independent concerns relating to sensitive information (such as medical, family, or other personal data) contained in court records, whose disclosure to information brokers may have undesirable practical consequences.

Any system that vastly broadens public access to these types of personal information -- as digitization and universal access unquestionably do -- should contain some effective means to safeguard such information. Otherwise, we risk chilling the public's willingness to access the court system, and even to assist the ends of justice.

2. Background: The Personal Data Identity Thieves Use, and How They Use It

The incidence of identity theft rises each year. Some 500,000 cases occurred in 2002, and this number will continue to rise. All consumers, rich and poor, are susceptible to this crime. Moreover, victims may not be made whole (*e.g.*, by the financial institutions involved) when someone hijacks their assets, identity, or information.

Identity thieves often combine "high value" personal identification, such as bank account or social security numbers, with "low value" information more readily available to the public, such as name, address, or birth date. Along this spectrum lies other data, readily available about some people, but not others: for instance, a prominent attorney's mother's maiden name, might be listed in Who's Who in America, along with his place and date of birth and his children's names (which may make his password easy to guess, as well); a CEO's signature might be accessible for forgery from her company's annual report (as attorneys' signatures are available in scanned PDF documents online).

Court records often contain the type of information most often used in identity theft,

especially records in consumer cases or class actions. Sophisticated corporate litigation records also may contain high-risk information: for instance, settlement papers may even list the bank account into which funds are to be wired.

Most obviously, accessible credit card information places consumers at risk. With it, a thief can order goods over the Internet, or launder money through an online payment aggregator. However, while many people consider credit card theft their major identity theft risk, it is far from the most pernicious, since the Fair Credit Billing Act and other laws traditionally have protected cardholders from most types of fraud.

The exposure of consumers' banking information causes even greater risks. With little more than a copy of your check (and thus your account number) an identity thief can scan, forge and cash checks in your name, and even set up a bank account into which to deposit (in your name) ill-gotten funds. In fact, simply knowing where you bank may be enough for a savvy con artist to trick you -- via emails and phony web site links that urge you, for "security purposes," to re-enter their account and PIN information through a phony web site – usually a copy of the your actual bank's web site.

The exposure of social security numbers also places consumers at risk, given the number's status as a universal personal identifier. With a social security number, an identity thief usually can, for instance, obtain a birth certificate. And with these, the thief can obtain (or convincingly counterfeit) your passport, utility bill, or a replacement driver's license.[1] He may

---

[1] See also Greidinger v. Davis, 988 F. 2d 1344, 1353 (4th Cir. 1993) ("Armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck.").

also access your financial assets, which often use your social security number as a *de facto* password and identifier. What then follows is limited only by an identity thief's energy and creativity: transferring funds, opening new bank or telephone accounts, obtaining multiple credit cards, car loans, and internet service accounts. (A savvy identity thief might even call the local phone carrier and unlist your telephone number – to make it more difficult for the thief's creditors to call you.)

Social security numbers are available for purchase from some online vendors.[2] However, this practice has been widely criticized, and there is a vigorous effort in Congress to ban or severely restrict these sales.[3] Further, the New Hampshire Supreme Court recently held that one such information broker, Docusearch, violated a common law duty when it sold a stalker the social security number and workplace address of his target, Amy Boyer, whom he then fatally shot at her workplace.[4] That court reasoned that "a person's interest in maintaining the privacy of his or her SSN has been recognized by numerous federal and state statutes. As a result, the entities to which this information is disclosed and their employees are bound by legal, and

---

[2] Some prominent Americans' social security numbers are already available in publicly accessible government databases. A cursory search on the EDGAR database (available both at sec.gov and on LEXIS/NEXIS) uncovers the social security numbers of some business executives, whose social security numbers appear on filings with the SEC -- stock agreements, reporting statements, employment agreements, and the like. However, in many other instances within that database, it appears that this information either was redacted or not placed online.

[3] For instance, the pending Social Security Number Misuse Prevention Act (S. 228, H.R. 637 sponsored by Sen. Feinstein, and Rep. Sweeney) would prohibit the sale, display, or purchase of social security numbers, with limited exceptions.

[4] Remsburg v. Docusearch, Inc., 816 A.2d 1001, 2003 N.H. LEXIS 17 (February 18, 2003).

perhaps, contractual constraints to hold SSNs in confidence to ensure that they remain private."[5]

To facilitate the ready accessibility of such personal data at a time when legislators, courts, and advocates are awakening to the importance of privacy and security would be a step backward, and would be welcomed by identity thieves.

3. Intrusions To Privacy Posed by Unrestricted Data Mining of Other, Personally Sensitive Data

Protecting our social security numbers, bank information, credit card numbers, and related information will make us more secure from identity thieves and other scam artists. But other sensitive information may also merit protection. For instance, sensitive medical, personal, or family information may be referred to – or, in class action or state enforcement suits, cumulated *en masse* – within records or settlement papers. For many, the disclosure of such information can be undesirable, disruptive, and potentially harmful.

For instance, class action lawsuits against pharmaceutical or asbestos companies may contain the names and addresses of claimants suffering from a wide variety of ailments, ranging from cancer to depression. However, such claimants may have very good reasons to avoid universally exposing their chronic conditions: in the hands of an employer, the information may provide a basis for discrimination; in the hands of an insurer, a basis to deny coverage; and in the hands of a financial institution, a basis to deny a loan.

Some sensitive personal information is available today, in various forms, if one is willing to pay for it.[6] But if such information becomes even more cheaply and readily accessible and

---

[5] Id., 816 A.2d at 1008 (citations omitted).

[6] For instance, the Dunhill International List Company offers vast mailing, telephone and email lists of "consumers with ailments," literally ranging from acne and asthma to ulcerative colitis. It

searchable online – in other words, orders of magnitude more accessible than it is now – information brokers can and will aggregate and find a cheap market for the data. Large employers will purchase the data, as will banks and insurers. And the lives of those with difficult, often hidden, conditions may find fair treatment yet more elusive.

Likewise, records that reveal lists of victims of predatory lending or other frauds and scams can expose these victims to further harm. In the hands of unscrupulous marketers or lenders, this information amounts to an easily mined potential "victims list."

These are but two examples of groups who, in seeking sanctuary in the courts, may merit protection from further victimization *via* universal exposure of their records. If such groups are afforded no control over their personal, sensitive information, they may simply opt out of the judicial process. Such a chilling effect should be avoided, or at least diminished, where at all possible.

In light of the above realities, we address the Commission's specific questions below. We have listed certain questions in combination, for efficiency of reference.

(1) **In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?**

and

(2) **Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers, or other personal identifying**

---

lists a profile "count" of 142,316 persons with high blood pressure, 51,963 with incontinence, and 135,240 with depression. See www.dunhills.com. However, this "marketing tool" is presently relatively expensive, costing $1.00 to $2.00 per name, for a complete profile.

information, should privacy concerns limit their disclosure on the Internet?

The accessibility of court records is of fundamental importance; the interests of justice, free speech, and democracy depend on a citizenry aware of and concerned about its justice system and how its courts serve the community. In a minority of cases, however, a competing set of privacy principles – with similar goals in mind – must be weighed against online accessibility and searchability of records.

As discussed above, the privacy/security concerns are twofold. First, certain identifying information that is commonly misused should probably be cloaked in some manner. Otherwise, identity thieves will use public court databases to mine cheaply for social security numbers, banking information, credit card information, and the like. Second, highly sensitive information that might be collected or aggregated, such as by information brokers, may also require protection. As discussed above, this might, for instance, include medical or financial information – particularly where the personal information is not central to the case; one example might be records (such as in an exhibit to settlement papers or a claims administrator's report) that cumulate hundreds or thousands of claimants' names and addresses in a suit against the makers of anti-depression drugs, or heart medication.[7]

The balance between privacy and open access can be substantively affected by the types of database searches that are permissible. For instance, if full-text, open field searches are permissible, an information broker or identity thief can more easily extract social security numbers or bank accounts from a database. By contrast, if users must submit the case name or

---

[7] There might be a substantive distinction between protecting the names of such class action claimants (particularly if they are not named plaintiffs) and, say, that of an individual plaintiff in an ADA suit, particularly against a public entity.

number in order to access each case, such mining is less likely to become routine. At least two caveats to this exist, however: first, such controls do not address the concern that a specific case (say, involving mesothelioma or anti-depression drugs) will be mined for mischievous or illegal purposes; and second, regardless of such controls, court administrators may wish to design the online database with the aim of limiting circumvention by "spidering" programs, which mine the site for personal and sensitive data.

As to such "spidering" programs, it might be worthwhile to implement both technical and legal remedies to monitor or enforce unbounded or burdensome web site and server usage. For instance, some web sites intended for general public access but not for wholesale extraction – *e.g.*, resumé posting sites, including the U.S. Department of Labor's job bank – post terms and conditions of usage that prohibit data mining by commercial recruiters.

While we are unaccustomed to such conditions on the extraction of mere information, society does place restrictions on many other public resources. The public nature and purpose of a web site or database may indeed justify certain use limitations, much the same way that a public park, to serve the common good, places limits on how citizens can use it. Just as we cannot pluck flowers from the Botanic Gardens, it may be reasonable to place limits on *en masse* data mining from a public web site. Otherwise, if everyone decided to mine data (at public expense), the entire system could fail: server capacity would be burdened and the system might crash; worse, citizens might hesitate to trust a court system that conditions their assertion of rights on their disclosure of secrets to anyone with access to a computer.

(3) If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

and

(4) **If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?**

As discussed above, the types of data that might potentially be cloaked from widespread digitized access are not confined to "personal identifying information," and might include other sensitive personal information, *e.g.*, relating to health, financial, or family matters. Most likely, technical and coding solutions will need to be combined with decisions by the attorneys of record and the court. A general, but not exhaustive list of the types of information that may be redacted as of right, for use online, would be helpful. It might be necessary in some cases for two sets of documents to exist – one for online reference, and one for courtroom, or courthouse, use. The court and the parties might work together to exclude particularly sensitive information from the online record, or from filing altogether, should privacy concerns arise.

A more difficult situation arises when personal or sensitive information is submitted by the adverse party. To address this, it might be necessary to formulate a similar "as of right" list of information (medical, familial, etc.) that must be identified and/or redacted absent consent by the underlying party; a certification might be required of adverse parties, or rules adopted regarding treatment of such information. Likewise, particularly in cases involving sensitive information, it would be prudent to delay online posting until at least several days have passed – giving the object of such sensitive information an opportunity to request redaction, as appropriate.

Whatever system is selected to safeguard particularly sensitive information, there are bound to be imperfections. But the system need not be foolproof in order to reasonably

safeguard privacy – just as the present system does not prohibit anyone from copying information from court records. Rather, the primary motive in designing the system should be to provide enough safeguards and checks so that identity thieves and others do not descend in droves to excavate a public resource for harmful purposes, chilling ordinary citizens from asserting their legal rights.

(5) Should the public be charged a fee to access court case records on the Internet?

This office's position is that, as a general rule, no fee should be charged for access. Otherwise, the information provided becomes a resource more available to the wealthy. In an age when, increasingly, information is power, such an imbalance is not worthwhile. Further, given that a credit card would likely be the payment option of choice, assessing such a fee would discriminate against those without a credit card.

(6) What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

As stated above, full-text searches raise considerably more serious security and privacy concerns than isolated docket searches, geared to a specific case. For the reasons also stated above, court administrators might also wish to consider whether any conditions (or obstacles) ought be imposed on commercial vendors who simply extract these records, and permit such searches.

1	Elisa Velazques NYS Trial Lawyers no written testimony yet
2	Panel of Speakers Association of the Bar of the City of New York already provided
3	Ken Dreifach NYS Attorney General's Office ✓
4	Charlotte Watson NYS Office for the Prevention of Domestic Violence ✓
5	Hillary Sunghee Seo Sanctuary for Families ✓
6	Richard Solomon Will not be submitting written testimony
7	Edward Klaris ~~New Yorker~~ Media Law Committee ✓
8	David Tomlin Associated Press ✓ (Did not speak at the hearing)
9	David Bralow Newsday/Tribune ✓
10	George Freeman New York Times ✓
11	Robert Port New York Daily News ✓
12	Ginda Mortise Pro Se Alliance No written statement
13	Eliot Deutsch No written Statement

Submission to the New York State Commission on Public Access to Court Records by the Ad Hoc Subcommittee on Internet Access to Court Records of The Association of the Bar of the City of New York

This submission is made in response to the Notice of Public Hearings of the New York State Commission on Public Access to Court Records (the "Commission") by the Ad Hoc Subcommittee on Internet Access to Court Records (the "Subcommittee") of The Association of the Bar of the City of New York (the "Association").[1]

The Purpose of This Submission

The purpose of the present submission is not to offer value judgments or definitive answers to the important questions that the Commission has been asked to study. Rather, the purpose of this submission is to share with the Commission the results of the Subcommittee's investigations and factual inquiries into the present status and future potential of Internet access to court records, which we believe may be helpful to the Commission in its deliberations.

Two preliminary observations are offered to provide context to our observations. First, although a framework for addressing confidentiality and

[1] The members of the Subcommittee are drawn from various interested committees of the Association, including the Council on Judicial Administration and the Committees on Communications and Media Law, Federal Courts, Government Ethics, Information Technology Law, and the Judiciary. The members of the Subcommittee are Sandra Baron, Terryl Brown, George M. Donahue, Joseph H. Einstein, Lori Goldstein, Marc Greenwald, Rajesh James (Secretary), Stephen D. Kahn, Alfreida B. Kenny, Todd L. Mattson, Michael Mills, Lynn K. Neuner, Robert C. Newman, Diana D. Parker, Richard J.J. Scarola, David B. Smallman, and Guy Miller Struve (Chair). While this submission is joined by all of the members of the Subcommittee other than Sandra Baron and David B. Smallman, it does not necessarily fully reflect the views of the individual members or those of their respective committees.

security of information already exists in the New York Court system, this submission is intended to explore whether such a framework can and should be applied to Internet access to court records. Second, in making this determination, it is necessary to balance privacy and security interests on the one hand with rights of public access on the other. The benefits of public access are clear. Therefore our submission focuses on the countervailing interests and asks whether these should limit presumptive access rights.

The Present Scope and Future Potential of Internet Access to Court Records

In considering the issues before the Commission, we believe that it is helpful to bear in mind that the present scope of Internet access to court records falls far short of its future potential.

With the technological means available today, it is feasible to implement a system of unlimited public Internet access to court records in which any person anywhere in the world who had access to the Internet could carry out a full-text (i.e., "Lexis-type" or "Westlaw-type") search throughout all the court records available on the Internet for a given search term (which could be a person's name, address, telephone number, credit card number, or date of birth, or any other search term). Such a search would locate any court records accessible anywhere on the Internet that contained the chosen search term (for example, that mentioned a chosen name), whether it was part of the caption of a case, or was just mentioned incidentally in the course of a trial transcript or in the middle of an exhibit submitted to the court. As described more fully in our response to the

Commission's Question 1 below, such a system of full-text access to all court records could raise issues of privacy and security.

Such a system of full-text Internet access to court records does not appear to be generally available to the public anywhere in the world today. In the first place, many existing systems of Internet access to court records (including the Federal system) are not open on an unrestricted basis to all Internet users, but require users to obtain and use passwords to gain access. As a matter of business policy, existing full-text Internet search engines (such as Google.com and Yahoo.com) do not index (and therefore do not offer full-text searches of) Internet sites that are available only to authorized users. For this reason alone, most existing systems of Internet access to court records are not candidates for full-text access.

There are some systems of Internet access to court records that are not limited to authorized users, but that are open to all users of the Internet.[2] A well-known example is Hamilton County, Ohio (the county in which Cincinnati is located), which initiated full Internet access to court records in late 2000. The Hamilton County web site has generated both extensive usage and significant controversy.[3] It does not, however, offer full-text search capability of the

---

[2] One such system is the New York State E.Court system, which offers Internet access to court calendars, orders, and opinions in certain cases. This system, however, does not presently offer access to all court papers filed in the cases it covers, and does not presently enable full-text searching.

[3] Our understanding is that legislation is under active consideration in Ohio to address various concerns raised by Internet access to court records.

contents of documents, but only allows users to search by case name, docket number, and names of counsel. A full-text search capability does not exist within the Hamilton County web site itself, and commercial vendors do not appear to have indexed the contents of the web site in order to provide such a capability.

Thus while Internet access to court records is still relatively new, and while this Subcommittee cannot state with certainty that it has reviewed all of the systems available to date, the capability of carrying out full-text Internet searches of court records does not appear to exist anywhere in the world today. However, if a given body of court records (for example, those in New York State) were to be opened to unrestricted Internet access, then it would automatically become technologically feasible for commercial vendors to copy and manipulate such records, thereby providing full text search capability regardless of whether or not the court system itself chose to provide such a capability as part of its web site. Alternatively, large litigants or law firms could set up proprietary systems allowing full-text searches which would not be available to other lawyers or litigants or to the public at large. This fact raises considerations of equality of access to public records that the Commission may wish to address.[4] It also suggests that the issues that would be raised by full-text searches of court records need to be considered before implementing any system of unrestricted Internet access to court records.

[4] For example, courts might provide records directly to the public or might contract out to services such as Lexis and Westlaw for that purpose. Further, courts may choose to create rules regarding permissible downloads from their own sites. Such rules could require monitoring by court personnel and sanctions for misuse.

Against the background of the foregoing facts, the Subcommittee offers the following responses to the questions posed by the Commission.

1. In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?

The Subcommittee fully concurs with the Commission that there is an extremely important public interest in having court records available for public inspection. In the case of many court records (including trial records), this public interest is of constitutional dimension. Public access to court proceedings is vital to public confidence in the fairness of the judicial process.

The Subcommittee believes, however, that there are certain countervailing interests that should be weighed against the constitutional and common law access rights in considering the implications of unrestricted Internet access to court records. The matters that come before the courts for resolution include the most intimate, private, and painful aspects of people's lives. Although many of these are already matters of public record accessible to those interested in taking a trip to the courthouse, to open all court records to full-text searching would open all of these matters to unrestricted browsing at the click of a mouse by people throughout the world.

The countervailing interests include not only privacy interests, but security interests – the interests in physical and financial security. To the extent that unrestricted Internet access to court records included private financial data of individuals, it could be used in such a manner as to threaten their financial

security (for example, by identity theft). And there are individuals affected by court proceedings whose physical security may also be at stake if court records can be used to trace their present whereabouts, or to find out how the rooms in their dwelling place are configured.

Although a limited portion of the information at issue may already be available online, unrestricted Internet access to court records, especially with full-text searching, is qualitatively different from anything that is generally available today. Full-text Internet searching is far cheaper, and far more powerful, than manually searching records at a courthouse on a file-by-file basis. Other differences also exist. For example, while users of courthouse files typically are not required to identify themselves in order to obtain and review such files, the fact that users must appear in the courthouse in order to access court records (and therefore may later be subject to identification by courthouse personnel) may serve to deter some who would seek to use the information in court records for improper purposes.

2. Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the Internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers or other personal identifying information, should privacy concerns limit their disclosure on the Internet?

For the reasons summarized in answer to Question 1 above, the Subcommittee believes that, before unrestricted Internet access to court records is implemented, consideration should be given to whether or not such access is appropriate in the case of categories of information that may pose concerns with

respect to personal privacy or security.

The types of personal identifying information listed in Question 2 are obvious candidates for scrutiny from this point of view, but they are not the only categories of information that deserve consideration. Among the types of cases that courts and/or committees in other jurisdictions have deemed worthy of special consideration (some of which are already subject to statutory seals in this State, at least to some extent) are custody cases, juvenile cases, matrimonial cases, mental health proceedings, and probate cases. Other types of cases that would not ordinarily pose privacy or security problems may raise such problems in individual cases.

In noting that such cases may raise issues that are worthy of consideration, the Subcommittee is not prejudging or advocating that Internet access should be blocked in any or all such cases. In general, the Subcommittee believes that any restrictions on Internet access should be the minimum necessary to prevent significant harm to privacy or financial or physical security.

In weighing privacy and security concerns, it should be borne in mind that the efficiency and power of full-text search techniques will seek out and reveal even a single instance in which sensitive information has inadvertently been left open to Internet access, even if all other occurrences of the same information have been successfully blocked from access.

3. If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

For the reasons summarized in the answer to Question 2 above, the

Subcommittee does not believe that the privacy and security concerns raised by unrestricted Internet access to court records are limited to personal identifying information. For this reason, our answer to Question 3 embraces all types of personal information that might ultimately be judged worthy of protection for privacy or security reasons.

To the extent that particular categories of cases or particular cases were to be excluded from unrestricted Internet access for privacy or security reasons, it would be relatively easy to identify the cases to be excluded from Internet access and to implement the exclusion. For example, particular types of docket numbers could be used to identify such cases, and cases bearing those docket numbers could be excluded from unrestricted Internet access.

To the extent that a decision were to be made instead that particular types of information should be excluded from Internet access while the rest of the document in which such information is found remained open to Internet access, the implementation of such a decision would be more difficult. The problem is not primarily a technological one. Means will shortly exist in widely-used word processing software by which particular information in a document (such as a bank account number) can be "tagged" with an electronic indicator that could be used to exclude that information from Internet access.[5] The problem, rather, would lie in making sure that the "tag" was affixed in all cases in which it was

[5] One such means would be the use of XML (Extensible Markup Language) codes to "tag" the information in question.

supposed to be affixed. This problem is addressed in Question 4 below.

4. If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?

Again, as in the answer to Question 3, to the extent that the decision was made that particular categories of cases or particular cases should be excluded from unrestricted Internet access, it would be relatively straightforward to implement such a decision. The responsibility could be placed in the first instance on the parties (subject, if appropriate, to court review) to indicate whether or not a given case belonged to one of the categories in question. Such cases could be given distinctive docket numbers, and the system of Internet access could be established in such a manner as to exclude such cases from access. Greater ease of administration must, however, be balanced against an inherent decrease in sensitivity to both privacy and public access interests. While the exclusion of entire categories of cases is relatively easy to implement, like any categorical rule such exclusion would be both under and over inclusive with respect to private information.

To the extent that a decision was made instead to require that particular types of information be "tagged" and excluded from Internet access, it would be unrealistic and inappropriate to place the burden of identifying and "tagging" upon already overburdened courthouse personnel.

As a practical matter, it would probably be necessary to place the burden of identification and "tagging" in the first instance upon the party filing such information, perhaps with some form of required certification. Unfortunately, it

would not always be the case that the filing party had both the resources and the motivation to discharge this burden properly. In particular, there might be problems with adherence to these requirements on the part of pro se litigants.

The only remaining alternative would be to rely upon the adverse party to check that the filing party had discharged its obligation (and, perhaps, to postpone Internet access for a few days to allow this check to be made). This would require a high degree of alertness on the part of the adverse party, and even this would not necessarily protect sensitive information of a third party which neither the filing party nor the adverse party had any incentive to protect.

Realistically, we believe that any system of identifying and "tagging" particular information for withholding from Internet access is likely to be imperfect. And, as noted at the end of our answer to Question 2, because of the power of full-text search techniques, even a single slip could result in the sensitive information becoming public.

5. Should the public be charged a fee to access court records on the Internet?

In principle, because of the importance of public access to court records, the Subcommittee believes that user fees for such access should be avoided if at all possible, and that if they are to be instituted, they should be strictly limited to an amount sufficient to cover the marginal costs of Internet access (not the costs of the electronic filing system itself, which are more properly viewed as part of the underlying costs of the court system).

Moreover, as a practical matter, if user fees were to be instituted, the likely

result would be to encourage users to subscribe to the services of commercial vendors which would download the contents of the courts' web sites, and then charge lower fees (or no fees at all) for accessing them.

6. What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

For the reasons set forth at the outset of this submission, full-text searches raise more serious privacy and security concerns than do searches limited to the captions and docket numbers of cases.

As a practical matter, however, as noted at pages 3-4 above, once unrestricted Internet access to court records was available, even if the courts themselves did not make full-text searching available, commercial vendors could index the contents of the courts' web sites and make full-text searching generally available, and large litigants and law firms could perform the same functions for themselves.

May 2003

ADDITIONAL STATEMENT BY INDIVIDUAL MEMBERS OF THE AD HOC SUBCOMMITTEE ON INTERNET ACCESS TO COURT RECORDS OF THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK

This additional statement is submitted by individual members of the Ad Hoc Subcommittee on Internet Access to Court Records (the "Subcommittee of The Association of the Bar of the City of New York (the "Association").[1] We write separately to underscore certain principles we believe should guide this Commission as it considers the application of new technology to the records maintained by the courts of this State.

INTRODUCTION

As the Subcommittee's Submission notes at the outset, clear benefits flow to society from our long history of public access to court records. We wish to stress the established legal framework for addressing access and the significant potential advantages that can be gained by Internet access to court files.

Internet access to electronically filed court documents offers an extraordinary enhancement to the public's ability to monitor and engage itself with the court system. Many individuals and groups monitor and rely upon public court files today – from the parties to litigation themselves, to the press, to watchdog and citizens' groups, to the public at large. Among the virtues of Internet access is that those who wish to review court records could do so without the limitations of court business hours, without the drain on the time of court personnel, and without the burden and expense of traveling to the courthouse and locating records. The advent of electronic filing offers very real and important opportunities.

Legitimate worries about privacy and security for information available on the Internet deserve full and focussed discussion. But, this discussion should proceed with

---

[1] The members joining in this submission include Sandra S. Baron, Richard J. J. Scarola, and David B. Smallman.

full recognition of the ground rules for resolving the tensions between access and privacy that have been established by the courts and the legislature of this State:

- Most court records are presumptively open for public inspection, a presumption that is protected by the constitution, statutes, rules, and common law of this State.[2] The courts of this State have extensive experience protecting confidentiality and security within the limits appropriately required by the public interest in access to court records.

- The Court of Appeals of this State has never recognized a tort for public disclosure of embarrassing private facts, and the legislature has never adopted a statute to protect this aspect of "privacy." It is therefore important to distinguish concerns about the release of non-public information that could be used to cause damage (*e.g.*, credit card numbers or bank account information that could facilitate identity theft), from information that would be embarrassing if widely disclosed.

The existing legal framework has developed over centuries. It reflects the hard lessons learned through long experience. That experience has taught us that the benefits of public access to information should not lightly be restricted. The application of new technology is not an occasion to reject the lessons of history.

We write separately also to underscore the fact that the same developing technology that is making possible electronic access to court documents, may itself offer innovative technological assistance to resolve many, if not all, of the legitimate privacy and security issues raised. For example, software already exists that can be used to block Internet disclosure of social security numbers or other personal identifiers in a court document. The process involves a simple coding that can be required to be included when a document is filed

---

[2] *See, e.g., Danco Laboratories, Ltd. V. Chemical Workers of Dedeon Richter, Ltd.*, 274 A.D.2d 1, 6, 711 N.Y.S. 2d 419,423 (1st Dep't 2000) (recognizing constitutional right of access to court records in civil proceedings); NY Uniform Rules of Trial Court 216.1(a)

with the court.

In addressing these issues, we urge the Commission to consider the rules for public electronic access to court cases that are already being adopted by the federal courts in New York. There is a benefit for counsel to proceeding on a uniform basis, to ease the adjustment to electronic filing and access.[3]

With these initial comments, we provide the following additional responses to the specific questions posed by the Commission:

1. In light of the recognized public interest that is served by having court case records available for public inspection, are there any privacy concerns that should limit public access to those records on the Internet?

We agree with the Commission that there is an extremely important public interest in having court records available for public inspection. As the Subcommittee Submission states, public access to court proceedings is vital to public confidence in the fairness of the judicial process. As noted above, we also underscore the absence of a public policy in this State generally protecting against the disclosure of embarrassing private facts.

The implications of such a legal constraint on newsgathering, and on the legitimate public interest in a free flow of communication, have wisely constrained the courts to enter sealing orders on a case by case basis. We would thus urge the Commission not to

---

(requiring consideration of public interest before any court record is sealed).

[3] Helpful guidance is available from recommendations on civil and criminal electronic case file availability and Internet use issued by the Judicial Conference of the United States, and in the recent enactment of the E-Government Act of 2002, which require federal courts to provide greater access to judicial information over the Internet, while promulgating rules to protect legitimate privacy and security concerns.

embark on the dangerous road of determining in advance what categories of information are inherently so sensitive or embarrassing that they deserve legal protection against disclosure on the Internet. Safeguards for information on the Internet should only be imposed where required to protect financial security and safety, not to avoid embarrassment or shame.

We urge that concerns about privacy for electronic records are best dealt with in same manner as courts in this State currently mange them in connection with paper records. There might well be countervailing interests to public access that present themselves in a given case, and we have little doubt that Internet access may heighten litigants' interests in pursuing the sealing of documents to a greater degree than currently exists in a paper record world.[4] However, there exist adequate standards and procedures available to litigants and others to request the sealing of information that it confidential and warrants continuing protection. *See, e.g.*, 22 NYCRR 216.1. The courts are experienced in balancing the interests appropriately on a case by case basis, and there is no reason they can not continue to do so with electronic records.[5]

---

[4] Without downplaying such legitimate concerns, much of the information that might be most problematic is readily available from other sources already. *See* Amitai Ezioni, THE LIMITS OF PRIVACY *10* (1999) ("Consumers, employees, even patients and children have little protection from marketers, insurance companies, bankers and corporate surveillance"). Indeed, the anecdotal research by members of the Subcommittee confirmed that a great deal of information, including social security numbers, was easily obtainable from Internet research tools by others on the Subcommittee. One question that is not being asked by the Commission, but that perhaps should be looked at, is whether the courts ask for personal identifying information in instances where it is not necessary and when other, less potentially problematic, identifiers could be used. *See, e.g.*, J. Cissell, *Privacy and Court Records on the Internet,* THE JUDGES' JOURNAL 29-30 (Summer 2001).

[5] We are assuming that the court websites will make available documents on a going-forward basis. The only fact submitted to the Subcommittee with respect to past documents from closed

2. Should any information that is currently deemed public be subject to greater restrictions if made available for public access on the Internet by the Unified Court System? For example, when public court records contain an individual's Social Security identification number, credit card numbers, bank or investment account numbers or other personal identifying information, should privacy concerns limit their disclosure on the Internet?

For the reasons summarized in answer to Question 1 above, we do not believe that there should be different rules for Internet access to court records than exist for records at the courthouse. This is the policy decision that the federal courts have made and we believe it is wise.[6] That said, we recognize that the federal courts are recommending that full social security numbers, dates of birth, financial account numbers and names of minor children be excluded from electronically available records even for the bankruptcy courts which have been making such information available for some time. However, not all such identifiers in all instances require confidentiality. Hence, we again urge that case by case determinations are the best means of balancing the public's right of access to court records against specific and recognized privacy and security interests.

Any decision on Internet access should also take into account the extent to which personal information is already available over the Internet from other sources. Phone numbers, addresses, political party affiliation, mortgage indebtedness, the name of one's bank,

---

cases was that such documents would likely not be made available electronically. To the extent that the court system does plan to scan in records from cases that are closed, consideration may need to be given to a system of notifying the parties and provision for their reviewing and requesting redactions.

[6] *See, e.g.*, News Release, Administrative Office of the U.S. Courts, September 19, 2001 (<http://www.uscourts.gov/Press_Releases/index.html>).

and vast amounts of other pieces of "private" information are already available on-line. Public access to court records should not be limited in the interest of privacy, if the limitation is ineffective and serves no useful purpose. Any restrictions on electronic access should be effective in protecting against the perceived harm, and should satisfy the existing legal standards for sealing court records.

While we recognize that litigants themselves may question the increased scrutiny of personal identifying information disclosed in court records that are made available on the Internet, these concerns, where well-grounded, can be met by appropriate coding to permit the "electronic redaction" of information, as we discuss in response to the next Question.

3. If such personal identifying information should not be made available on the Internet, how should that information be eliminated from electronic/Internet availability?

To the extent that personal identifying information should be excluded from unrestricted Internet access for privacy or security reasons, technological advances may make it relatively easy to identify such data and to implement the exclusion. Means may well exist now within commonly used word processing software, and more sophisticated means will shortly exist in widely used word processing software, by which particular information in a document (such as a bank account number) can be "tagged" with an electronic indicator that could be used to exclude that information from Internet access. The Commission will undoubtedly hear from those far more technologically proficient than we, and the means by which tagging can be effected should be explored.

4. If there are any limitations or restrictions to be placed on the dissemination of court records on the Internet, what role should be played by the courts, by attorneys or by others?

The means by which information is redacted from Internet access of records will, undoubtedly, largely be the responsibility of the litigants and their counsel. The court's computer system would have to be configured to read the tags that the litigants would be required to place on documents in order to identify and electronically redact information from web access.

Identification and "tagging" in the first instance would be the responsibility of the party filing such information. While it has been noted that the filing party might not always have both the resources and the motivation to discharge this burden properly, this problem also exists with records available at the courthouse. We would suggest that a means for impressing upon counsel the need to manage the tagging system appropriately would be some form of required certification to the court on the issue; inappropriate disclosures would be subject to existing laws or rules that provide sanctions for such conduct. Adherence to these requirements on the part of *pro se* litigants may pose special problems as they always do, and some form of assistance at the courthouse would likely be necessary.

Again, the federal courts noted that with respect to the burden their proposed systems would place upon counsel and litigants, the courts – and we would add, undoubtedly with the assistance of the states' bar associations and continuing legal education institutions – might well have to undertake some means to educate the bar and the public about the fact that information will be available online and the means by which it can and should be protected. This educational process could go both to the need for parties to protect their own

identifying or other information appropriate for sealing, as well as the requirements imposed for protecting such information of others.

Realistically, we believe that any system of identifying and "tagging" particular information for withholding from Internet access may initially be imperfect. However, the situation is likely to improve as lawyers become more familiar with the practice. In addition, when lapses are identified, systemwide modification can occur with little delay if an appropriate mechanism is set up for corrective action. Finally, at least with respect to lawyers, having to certify to the court that he or she has met his/her obligations to implement masking of specified data is likely to impress upon lawyers the seriousness of their responsibilities on this matter, and that sanctions could await counsel who took such obligations lightly or intentionally made such information accessible in his/her filings.

5. Should the public be charged a fee to access court records on the Internet?

We agree with the Subcommittee's response with respect to fees. While, of course, not binding on the state courts of New York, it may be worth noting that in December 2002, President Bush signed into law the E-Government Act of 2002, which now mandates that the Judicial Conference "may, only to the extent necessary, prescribe reasonable fees" for collection by the courts for access to information available through automatic data processing equipment. The Senate Report accompanying the legislation observes that: "The [Senate Committee on Governmental Affairs] intends to encourage the Judicial Conference to move from a fee structure in which electronic docketing systems are supported primarily by user

fees to a fee structure in which this information is freely available to the greatest extent possible."

6. What information should a member of the public need in order to search case records on the Internet? Should a search require the name of a litigant or index number, or some other limited method, or should full text searches be available?

Unless the court system is going to establish limits on the degree to which a user can download records from the system it establishes, it is our understanding from the information presented to the Subcommittee that a user could, theoretically, download the entirety of the records (or any significant and/or identifiable body of them) and render them full text searchable either for the user's own benefit or as a commercial venture. The Subcommittee received information that suggested that the cost of managing this was not so substantial that it would deter a user such as a large law firm from doing just that for its own benefit. [7] Whether due to cost in setting up the system, or concerns about security of the

[7] As the Subcommittee Submission states, if the courts themselves do not provide full text searchability, but allow private concerns to do so, there will likely arise issues of equity in terms of public access. One manner of addressing the issues of equality of access is for the court system itself simply to provide court records in a technologically sophisticated manner to all to whom it authorizes access, whether that ultimately is the public or authorized users. A related alternative would have courts contracting out to services such as Lexis and Westlaw to accomplish the same end, but providing for reasonable rates that would presumably make access reasonably and broadly affordable. While theoretically access could be conditioned on the user's agreement not to download the entire contents for this purpose, the fact is that rules would then also have to be developed that somehow determined what amount of downloading was too much (*e.g.*, one case, ten cases, twenty cases) which in turn would require monitoring by court personnel backed up by sanctions for misuse. One reality that the research of the Subcommittee has revealed is that increasingly greater quantity and quality of access or access capability is inevitable, and the only material question is on what terms.

system,[8] or concerns about securing the confidential data in the systems, no court system to our knowledge has, as yet, offered a full text searchable system open, without password or other limitation, to the public.

Full text searchability would allow for research into the number and disposition of categories of cases, of great use to press, scholars and those who monitor courts and their management more generally. It is among the great benefits of electronic record keeping.

It would require those who have information they believe should be confidential to take steps to insure that is managed. But to deny the public overall the benefits that could accrue as a result of full text search capacity because of fear of litigant error or misdeed would be short sighted and, in light of the exponential developments in computer technology, likely short lived.

May 2003

---

[8] The Subcommittee spoke by teleconference with Judge James Cissell, who as Clerk of the Court of Hamilton County, arranged for that court's electronically stored documents to be placed on a website, accessible by the public on the Internet. He told the Subcommittee that the reason Hamilton County had not adopted a full text searchable system was that at the time they felt the costs were too great and had been advised that it would allow the system to be more easily sabotaged.

Statement of Bob Port, Staff Writer, *New York Daily News*
New York Commission on Public Access to Court Records
May 30, 2003
New York, N.Y.

I have been a newspaper reporter and editor for more than 20 years, working first at the *St. Petersburg Times* in Florida, then at the headquarters of The Associated Press in New York and since July 2000 at the *Daily News*. I am also an adjunct professor at Columbia University Graduate School of Journalism, where I teach a popular elective course called "Investigative Techniques."

Since the early 1990s, I have specialized in investigative reporting that uses large databases of public records to build a foundation for accurate, probative journalism. I process electronic records, sometimes by the billions, to ferret out and document otherwise hidden connections and trends. This has yielded, for example, stories about: abusive nursing home aides employed after concealing their prior convictions for abusing the elderly; federal employees stealing horses from federal lands to sell for horsemeat; anti-smoking physicians with huge personal investments in tobacco farm land; and the involvement of all major clothing retailers in widespread illegal labor practices in New York City's garment sweatshops.

I rely on the courts, more than on any other branch of government, to be an impartial source of balanced, truthful information.

With the growth of the Internet as a digital communications medium in recent years, a cacophony of voices are expressing worry about the danger this poses to individual privacy rights. By publishing all court records on the Internet, for instance, the fearful warn, the World Wide Web could become a 'Big Brother' library. Each intimate detail of our past embarrassments will be logged for eternity. Facts once anonymous by their obscurity will join an instantly searchable database available to any faceless enemy to unjustly use against us with a mouse click on a screen.

In reality, this idea is foolishness rooted in ignorance - a modern version of killing the messenger, or in this case, a whole medium. The Internet does one thing and does it utterly democratically: It makes the transmission of information exponentially more efficient. All else that results would, or could, have occurred nevertheless. For court records, it merely saves trips to the courthouse.

I would also maintain that to attempt to make private on the Internet that which is already public on paper - like material archived by court clerks - is futile. Worse, such policies harm the public in a manner that outweighs the protection afforded any individual. Suppression of access hinders our progress, leaves our state's commerce less competitive and conceals threats to our safety that we rely on our courts to expose.

There is one and only one policy that makes sense for electronic access to court records: Information that's public at the courthouse should be available on the Internet to all for no more than its cost of publication.

To do less is to bar the common man from the real clerk's office of the future. To overcharge for access would be like selling tickets to a trial.

The status quo

Currently, I would describe New York State's online access to court records as poor. The federal courts, usually a bastion of conservatism where technology is concerned, are years ahead. The federal judiciary now has nationwide online access to dockets and other basic information available to anyone through its Public Access to Court Electronic Records (PACER) system. Fees are a modest seven cents per page collected quarterly by credit card and discounted for large downloads. Most federal districts have web access. Soon all will. A national case party name search is available and it includes all criminal indictments. Almost a third of federal courts have converted or will soon convert to a fully digital document system, where pleadings are filed electronically in Adobe's Portable Document Format (PDF), a format recognized by the Library of Congress and the National Archives and Records Administration.

The federal civil court in New York's Eastern District, home to much significant litigation, went digital two years ago. In New York's Southern District, bankruptcy court has been digital for five years. The record of the Enron bankruptcy case, including reports and many transcripts, for example, can be downloaded from the Internet on a Saturday afternoon. *The New York Times* did just that when it published a breaking Sunday report on the company's early internal investigation of what went wrong - news that rightly stunned readers everywhere and promptly intensified public debate.

By comparison, New York State courts make available only calendar entries online and only for open cases - what appears to me to be a convenience designed to aid lawyers and law firms in checking their schedules.

There are states where electronic access to court records is far worse. Mississippi is one. Alabama is another. Maine, a place where some court records still exist only on paper index cards, has a historic hostility toward computerization of government records. Had Maine's archival criminal files been automated, we might well have known earlier than a week before Election Day of the well-kept secret of candidate George W. Bush's youthful arrest for drunken driving. That we eventually learned of this case anyway is an illustration that nothing once public in court can be expected to remain hidden forever.

New York State should become a model for public access to court records on the Internet - for the health of its economy and to better inform its citizenry.

Florida, a less populous state with a shakier revenue base for its judiciary and a constitution that outlaws income taxes, manages to make electronic access widely available at cost, county-by-county, online or on CD-ROMs containing whole data sets. One can download a statewide Florida

rap sheet check (covering arrests of more than two million living persons dating back to the 1940s) through the Internet for $15 with a credit card.

In New York, a complete check of the "CRIMS" database is not available on the Internet or through any private vendor. It covers only populous counties, costs $25 and requires a visit or call to a clerk's office. This is inefficient, costly and it reduces the productivity of businesses that rely on this basic due diligence in hiring, lending or other business. It complicates the legitimate work of a free press, too. We can do better.

The privacy myth

As a journalist, what I fear most is that when New York begins to seriously publish court records on the Internet - and it will - names, dates of birth and addresses will be censored for "privacy" reasons.

Many Americans seem to assume that, by some birthright, they can expect their name, date of birth and home address to remain secret from whomever they choose, even when it was recorded because of their conviction for a crime.

This has always been a silly idea in a nation that requires citizens to serve as jurors in court. It became sillier as America industrialized and embraced inventions like the telephone, which requires telephone books. In an age of digital recordkeeping, it becomes downright stupid.

Get a clue. Names, birth dates and addresses for nearly all adult Americans are already widely available to the public through the Internet. Finance, commerce and politics depend on this.

While personal identifying information in its most accurate and detailed form is not *freely* available, that is, it is not published on free web sites, it is absolutely available at a low cost. I teach journalism students how to locate the birth date and home address of anyone in the United States in five minutes or less at a cost of about $5 per name. The only requirement is that the person has possessed a bank account or credit card (the details of which are *not* public); has received mail; has owned a car; or has registered to vote.

Information is like water. It flows to the sea via the path of least resistance. In our nation of free speech and capitalism, we reward investors who get people information they need and want. So it is with identifying facts on individuals. They will always be everywhere.

For more than 10 years, Aristotle Industries, a data vendor that mostly caters to political campaigns, has collected nationwide voter registration records. With an Aristotle internet account, and at a cost of less than $20 per search, one can call up any voter's home address or addresses; his or her date and place of birth; past and present party affiliations; and election attendance. I can see the same information for other voters who shared the same household, such as spouses and children. The information

is meshed with neighborhood demographic and religious data culled from a range of sources. This is how the Michael Bloomberg campaign, for instance, can conduct a phone survey of older white Jewish Democratic voters in Washington Heights whenever it wishes.

If Aristotle goes out of business, I assure you there will be a new capitalist venture emerge to take its place and elected politicians who will assure its right to compile records. Unless we make voter registration confidential, an un-American concept that would invite corruption, we can expect our names, birth dates and addresses to remain available through the Internet forever. It is the price of citizenship. A small price, I'd say.

There are many more examples. The federal Fair Credit Practices Act gave Americans unprecedented rights to demand the equitable availability of credit from banks. It gave creditors rights, too, such as the right to share identifying information on borrowers. The intent was a good one: to facilitate bill collection. What evolved were numerous businesses that legally sell access to databases of name, age and address histories. The data are accurately interconnected by confidential Social Security Numbers that are withheld from customers not authorized to obtain an SSN.

Congress has recently given citizens the right to request that creditors not share their identifying information, but large brokers of credit bureau data, such as Equifax, already possess so much data from so many credit accounts, and have so much other data available to them - for example, from magazine subscriptions and professional associations - that all our horses are way out of their barn. The U.S. Postal Service makes its change-of-address database available to businesses. This also assists data brokers in tracking us. What else is the post office supposed to do? If our identities are secret, how is the postman to deliver us our mail?

With computers, today's mosaic of sources, each one legally public, makes it possible to compile directory-type information on anyone, but this is not exactly top secret stuff, is it? Data brokers are civilly liable for misuse of their material. Identity theft can be vigorously prosecuted. The press cannot barge into someone's home to get a story.

This is the reality of personal identification data in the United States today. Americans who live normal lives enjoy great benefits, but must expect that their names, ages and addresses be knowable. Courts should recognize this reality and leave it to politicians to debate privacy. It is not the job of the courts to suppress public information as a prophylactic measure based on hypothetical concerns about privacy. Law enforcement authorities already have the power to pursue criminal acts violating privacy. Civil law already acts as a check on irresponsible acts by the news media or businesses.

Personally identifying information in court records should be as public on the Internet as it is in court records - no more and no less.

The court's digital divide

I suspect many judges would be surprised to learn how much of the court's business is already published on the Internet. However, what principally characterizes this material is that it is very, very expensive. As a result, a digital divide has evolved. The rich can use computers to automate their work with court records. The poor cannot afford it.

Currently, Meade Data, through its Lexis-Nexis service, is the biggest vendor of New York State court records. Every filing and every final judgment in civil court triggers a synopsis published in the Lexis-Nexis public records library. All major news organizations and any sizable business typically subscribes to this data at an annual cost ranging from tens of thousands to hundreds of thousands of dollars. Some public libraries subscribe, too, and their Nexis terminals stay busy.

New York civil docket information is available through at least two vendors, the bigger being CourtLink, which was recently acquired by Lexis-Nexis. CourtLink can supply a current docket report for any civil case at a cost of roughly $10 per search. Some corporate customers spend thousands of dollars per week for live, e-mail-based tracking of selected cases or selected categories of litigation - a kind of automated due diligence.

Competitors who might offer more affordable alternatives face a daunting obstacle: The Unified Court System's fee is $20,000 to acquire the raw historic civil data accumulated since the 1980s needed to seed a new database. Daily data transmission of updates incurs a weekly fee of $545.

I question the propriety of these fees. The *Daily News* recently acquired this data. It can be recorded on two blank CD-ROMs at a duplication cost of less than $2. Why does the judiciary charge the public $20,000?

The picture is worse for the public when it comes to criminal records. There are no legitimate private vendors of criminal data. Record checks are offered by the Office of Court Administration at $25 per name - an exorbitant fee for public records from a system paid for by the public.

One can negotiate the purchase of a copy of the "CRIMS" database from the OCA at a cost of $750 per update, but only in exchange for an agreement not to share or publish the database - so that the courts retain their ability to raise revenue by selling criminal records checks.

This is not fair. Electronic criminal records checks should be available for free or for the pennies that they actually cost. The executive branch freely publishes Department of Corrections inmate records on the Internet.

In short, New York State's courts have developed a taste for selling electronic records to generate a profit on an investment of public money in technology. The rich enjoy the benefits of automated court records while others, including many worthy non-profit public interest groups, are deprived of information they equally deserve.

While this may have its roots in the failure of the Legislature to properly finance technology for the third branch of government, the court system ought to know better. Fees based on the cost of duplication or publication would be more appropriate.

Open records on the Internet promote accuracy and truth

In the competitive news environment of New York, there is great demand to know as much as possible as quickly as possible. When it comes to old fashioned paper court records, this is a challenge.

By making basic data, and eventually court documents themselves available on the Internet, the judicial system would become a force for greater good by promoting the free flow of knowledge. People unjustly accused can have the disposition of their cases known more quickly. Questions about how many citations the city is issuing can be answered impartially, quickly and authoritatively. A corporate citizen's record on product safety can be sized up within a week or two, rather than with an impractical lengthy investigation.

Rather than representing a threat to personal privacy, open electronic records, in my experience, promote public good, public safety and healthy political debate.

New York's judiciary should get to work and go totally digital - immediately.