

**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 manage 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.