

**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.