PLACING COURT RECORDS ONLINE: BALANCING THE PUBLIC AND PRIVATE INTERESTS*

LYNN E. SUDBECK

With identity theft on the increase and the public's safety at issue, state and federal courts are reexamining electronic access policies governing their court record information. This reexamination necessarily includes a study of the legal traditions underlying public access to court record information, balanced against the privacy interests of the public courts serve. The public's trust and confidence in the judicial system demands that such a study be undertaken before the development and adoption of any court's electronic access policy. This article examines case law governing public access and privacy interests involving court records and electronic-access-policy guidelines recently issued by federal and state court administrative organizations. This article further reviews ideas and solutions proposed in recent law reviews regarding access and privacy interests. Finally, this article recommends guidelines for electronic access to court records that balance judicial accountability and efficiency with public trust and confidence and permit public access to the activity of a court system while protecting the privacy interests of the citizens who use that court system.

One of five trial court performance standards recognized today in the field of court administration involves access to courts, including court record information (Keilitz, 2000). One way to provide better access to courts is to utilize the recent advances in technology, and specifically the Internet, for publishing information about a court system and its services online as well as for allowing access to public court record information. However, does placing court records online create new problems for court users?

Court records often contain personally identifying information, such as Social Security numbers, names and dates of birth of minor children, and financial record information, and may also contain sensitive information, such as medical records and employment histories. Such information is subject to misuse if widely disseminated. According to the Federal Trade Commission, 10 million Americans had their identities stolen in 2003, and each spent an average of 530 hours resolving the resulting problems; the Justice Department reports that identity theft costs United States businesses nearly $50 billion per year in fraudulent transactions. Identity theft is our country's fastest growing computer-related crime (Frieden, 2004; Sovern, 2003). In assuming their victim's identity, identity thieves use a variety of personally identifiable information, all of which is currently publicly available in most court records.

* This article is derived from the author's research paper for the National Center for State Courts' Court Executive Development Program, which received the Director's Award of Merit. The author would like to thank Stephen L. Wasby for his encouragement to publish this work and for his assistance in editing.

In February 2003, seven coconspirators used personal information obtained from federal court records to commit fraud and identity theft. The seven used PACER, the federal courts' online database system, to obtain information about federal inmates and open false financial accounts. In this conspiracy, thirty-four inmates and twenty financial institutions were victimized (Silvestrini, 2003). In Cincinnati, Ohio, a speeding ticket posted on a court clerk's Web site provided an identity thief with a person's Social Security number, address, height, weight, birth date, and his signature; the thief accumulated $11,000 in credit-card theft before his arrest (Lee, 2002). Apart from identity theft and credit-card fraud, public information in court records can be used to commit crimes involving blackmail, extortion, stalking, and sexual assault. Courts are reviewing their record-access policies out of concern for privacy interests and identity theft; however, the most compelling reason to protect personally identifying information in court records is public safety.

When developing an access policy for electronic court records, courts must resolve the inherent conflict between providing access to public records and protecting individual privacy interests. Some members of the court community believe that court records contain traditionally public information that should be protected and kept private when disseminating these records electronically. Others believe that the information contained in court records, whether in paper or electronic format, should receive equal treatment when courts develop their access policies so that the same record information is publicly available, regardless of the access method. This has been called the "public is public" approach (Deyling, 2003).

Rapid advances in technology have challenged courts to balance the interests between providing public access to their records and protecting the private information within those records when disseminating them electronically. A significant number of both federal and state court systems have taken advantage of the technological progress and placed their court records online. Some of these same court systems have recently removed their records from Internet access because of privacy concerns. For example, on July 1, 2003, the clerk of court in Butler County, Ohio, was ordered to remove domestic-relations-court records from Internet access because of concerns regarding personal information, including Social Security numbers and financial information, within those records (Morse, 2003a, b, c, d). On November 25, 2003, Florida's chief justice issued an eighteen-month moratorium on posting state court trial documents on the Internet; this required the Manatee County clerk of the court to disable electronic access to court records previously posted under a legislative mandate (Cunningham, 2003). The Loudon County, Virginia, clerk of court suspended electronic access to court records amid concerns of identity theft involving Social Security numbers and other personal information, just nine days after putting the county's land records online (Chase, 2003).

State and federal court systems are currently in various stages of redeveloping and amending their electronic access policies to address the issues of protecting court users' private information in public court records. An examination of relevant case

law reveals the parameters for today's electronic access policies governing court records.

UNITED STATES SUPREME COURT DECISIONS

Although the Supreme Court has never ruled on a constitutional right of access to court records (*United States v. McVeigh*, 1997), it has addressed issues of access and privacy interests in court records in several opinions. In 1978, in a case involving privacy interests in President Richard M. Nixon's taped conversations regarding "Watergate," the United States Supreme Court cited cases dating back to the 1800s for the proposition that the federal and state courts of this country recognize a general common-law right to "inspect and copy public records and documents, including judicial records and documents" (*Nixon v. Warner Communications, Inc.*, 1978 at 598). The Court acknowledged that the interest in making these records publicly available is the "citizen's desire to keep a watchful eye on the workings of public agencies" (*Nixon* at 598). Today, the field of court administration recognizes that interest as judicial accountability, one of five trial court performance standards (Keilitz, 2000). The Court explained the limitations of this right of access:

> It is uncontested, however, that the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes. For example, the common-law right of inspection has bowed before the power of a court to insure that its records are not "used to gratify private spite or promote public scandal" through the publication of "the painful and sometimes disgusting details of a divorce case." Similarly, courts have refused to permit their files to serve as reservoirs of libelous statements for press consumption, or as sources of business information that might harm a litigant's competitive standing (*Nixon* at 598).

The Court further noted that access to court records is a decision left to the sound discretion of the courts, in light of the relevant facts and circumstances of the particular case. In this particular case, the Court held that Nixon's interest in privacy outweighed any public interest of the press, particularly when the only purpose articulated for the release of the tapes was their potential for commercial exploitation.

In 1989, in a case involving criminal "rap sheets" summarized in a computerized database, the Supreme Court addressed the privacy issue where records were publicly available at their source but had been compiled into computerized lists (*United States Department of Justice v. Reporters Committee for Freedom of the Press*, 1989). This case was decided under the federal Freedom of Information Act, which is not applicable to court records but is included here because it provides the Court's reasoning on the issue, relevant to court records, of whether a government record that is public as an

individual record changes character and becomes less public when combined with other public records into a computerized database of information. Had the transformation of public information into a compiled database affected the privacy interest?

The Court recognized "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the county and a computerized summary located in a single clearinghouse of information" (*U.S. Dep't of Justice* at 764). The Court noted that the privacy interest in public information is substantially affected when the information can be accumulated and stored in a computer long after the public interest in that information has been forgotten. The public's interest in release of information was described as "shedding light on the conduct of any Government agency or official" (*U.S. Dep't of Justice* at 773). The Court stated that this government accountability, which supports access to public records, "is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct" (*U.S. Dep't of Justice* at 773).

Courts have generally recognized a presumption of public access to court records and have made those records available where the purpose of access is related to public scrutiny of the judicial process. On the other hand, as noted in *Nixon* and *United States Dep't of Justice*, courts will protect personal information in the same public records where the purpose of access is related to commercial exploitation or potential misuse of the information with no public-oversight purpose. The Supreme Court held that when the request does not seek official information about a government agency but merely seeks records the government agency is storing, the invasion of privacy is unwarranted (*U.S. Dep't of Justice* at 780).

In 1977 the Supreme Court decided a case involving compiled records of the names and addresses of New York state citizens who had received prescriptions for certain scheduled drugs (*Whalen v. Roe*, 1977). Although the Court upheld the constitutionality of the statutes allowing the state to record this information in centralized computer files, the Court addressed the privacy interest in personal information in compiled government records. The justices stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and Social Security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures (*Whalen* at 605).

The Court further recognized that in some circumstances, the "statutory or regulatory duty to avoid unwarranted disclosures" of collected public data is rooted in the Constitution.

Justice Brennan, concurring, foresaw the danger of indiscriminate disclosure of public records made accessible on a grander scale by technology. He wrote that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology" (*Whalen* at 607). Today, thirty years after Justice Brennan wrote these words, court systems stand at the crossroads of making vast amounts of public-court-record information easily accessible through computerized databases and Internet use, while searching for "some curb on such technology" or other methods to protect the privacy interests of litigants and third parties named in those records.

STATE COURT DECISIONS

Very few state court decisions have addressed court records and the impact technology has on their compilation and distribution and on individual privacy rights. In 1994 a California appeals court reversed a lower court's decision that a seller of criminal-background information was entitled to periodic copies of computer tapes created for the Los Angeles municipal court information system (*Westbrook v. County of Los Angeles*, 1994). The database included the name, birth date, zip code, case number, date of offense, charges filed, pending court dates, and case disposition for every person against whom criminal charges in the municipal court system were pending. By statute, such compiled information was accessible only to certain persons in the course of their duties and to others who showed a compelling need. The statutes did not provide similar restrictions on the same information located in an individual criminal file. Despite the presence of these statutes, however, the seller had been able to collect this information monthly by computer tape from the municipal court system. He now complained that if he were denied access, he would have to travel to forty-six municipal-court locations to obtain it and that no one would be able to afford what he would have to charge for the information.

As the seller showed no need other than his pecuniary interests in the records, the appellate court found that the statute protected the compiled information from disclosure and that the state constitutional right to privacy protected defendants from unauthorized disclosure of their criminal information. The court noted that the privacy-right amendment to the state constitution was meant to preserve a person's ability to control dissemination of personal information. In explaining this constitutional amendment to voters at the time it was adopted, the state election brochure declared: "The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them" (*Westbook* at 166).

The seller did not prevail. The court specifically noted "a qualitative difference between obtaining information from a specific docket or on a specified individual, and obtaining docket information on every person against whom criminal charges are pending in the municipal court" (*Westbook* at 165). The court further noted that the aggregate nature of the information, which made it valuable to the seller, was the same quality that made its dissemination dangerous and concluded, as has the United States Supreme Court, that the right of access to public court records is not absolute: "When that right conflicts with the right of privacy, the justification supporting the requested disclosure must be balanced against the risk of harm posed by disclosure" (*Westbrook* at 166).

In 1999 the Colorado Supreme Court also addressed a case involving an electronic database of court records, prompted by a request for bulk data from a private entity in the business of selling such information to the public (*Office of the State Court Administrator v. Background Information Services, Inc.*, 1999). The information included criminal- and civil-case-record information, such as judgment debtor and creditor information and domestic-case-filings information, as well as Social Security and driver's license numbers. Some of this data were protected by statute; the seller requested the State Court Administrator's Office (SCAO) to create an electronic database excluding the statutorily protected confidential information. Here, as in *Westbrook*, the SCAO denied the request after the seller had been receiving computerized database records for years. In refusing to deliver additional tapes, the SCAO cited two specific concerns: 1) records sealed by judges after the information was delivered to the seller made this sealed court information available to the public, and 2) release of judges' orders containing sexual-assault victims' names violated state statutes restricting release of victim information. The seller asserted that the state's public-records law created an implied duty for the SCAO to provide this information in redacted form.

The lower court ruled in the seller's favor and the SCAO appealed. Before the court of appeals ruling on the matter, the chief justice issued a directive that permitted the state court administrator to deny the request for release of bulk electronic data stored by the state judicial branch. Despite this directive, the Colorado Court of Appeals affirmed the lower court. On appeal by the SCAO, the Colorado Supreme Court held that no state statute required these otherwise public records to be made available to the public in bulk form, and absent such a requirement, the administrative policies of the supreme court governed release of these records. As in other cases previously discussed, the Colorado Supreme Court noted that courts are the official custodians of their own records, including records compiled into an electronic database. As the United States Supreme Court had noted in *Whalen*, the court recognized that access to electronic bulk data raises very different issues than access to individual case files, which are open to public inspection upon request. Compiled public records available electronically for wide dissemination are qualitatively different than individual public records available in the clerks' offices. The court held that

"[w]hether access to bulk data should be released and to whom is a matter of important policy that necessarily involves the balancing of individual privacy concerns, public safety, and the public interest in fair and just operation of the court system" (*Office of the State Court Administrator* at 429-30). The court further held the SCAO was not required to create a "sanitized," or nonconfidential, version of its computerized records solely for purposes of disclosure.

The private information within public court records, unless sealed by court order or statutory authority, is open to anyone willing to walk into the courthouse, stand in line, sort through the records in the county clerk's office, and pay copying charges. Courts have indicated that the "practical obscurity" of this information in clerks' offices, that is, the inherent difficulty in obtaining it, has helped protect its privacy. At least for paper court records, the traditional safeguards within the courts' practices have been adequate to protect individual privacy interests. With rapid advances in technology and the ease of availability and dissemination of large amounts of data found in court records, and especially compiled data, traditional protections based on "practical obscurity" are gone. The search for information can now be performed at a computer terminal by anyone anywhere; the information is available in a matter of minutes, in massive amounts, and the cost is minimal. The qualitative change in the method of access and wide dissemination over the Internet eradicates the naturally occurring privacy protections in place with paper records in clerks' offices. Such change demands reexamination of court records access policies.

FEDERAL AND STATE COURT ADMINISTRATION RESPONSE

Traditionally, access issues have been determined by judges on a case-by-case basis or by the control the clerk exercises, at the direction of the court, as custodian of these records. Technological advances have changed the information world so quickly and so recently that there has been little time for case law to develop to adjust the balance between publicly accessible electronic court records and protection of individual privacy interests. With no extensive body of case law on which to draw, court administrators, not judges, find they must develop policies for access to records that will protect private and sensitive information (Winn, 2004). Court systems today face electronic access and concomitant privacy issues, and these issues will not wait for case law to develop. Such policies are being developed following notice, public participation and comment, and careful consideration of not only the public/privacy issues but also, as with all good administrative decisions, the costs and benefits to the public and to the court system.

Federal Court Administration Organization Guidelines. In April 2003, staff of the Office of Judges Programs of the Administrative Office of the United States Courts updated its 1999 report, *Privacy and Access to Electronic Case Files: Legal Issues, Judiciary Policy and Practice, and Policy Alternatives* (Deyling, 2003). The report recognized that two different approaches to electronic court records were emerging. The first position, the "public is public" approach, assumes that the format of the record

should not alter the right of access and that current court practices, mainly orders to seal documents, are adequate to protect privacy interests. The second position relies on the "practical obscurity" of paper records to keep information private while acknowledging that there may need to be limits on information in court records that are distributed electronically. The staff report proposed the federal courts take a third approach that would allow varying levels of access to different stakeholders with electronic access to the entire file available at the clerk's office, but not available on the Internet.

In September 2001 the Judicial Conference of the United States, the principal policy-making arm of the federal court system, adopted a privacy policy for federal civil- and bankruptcy-court records, which is essentially the "public is public" approach. However, the policy restricts information in both the paper and electronic copies of the record. The policy places the burden of protecting private information in court records squarely on the litigants and their attorneys who file documents with the court, indicating they should examine documents carefully and redact certain information before filing and, where necessary, make appropriate motions to protect them from electronic access. Although Judicial Conference policy recommendations are nonbinding, they are usually followed by federal courts.

The Conference delayed for two years expanding its policy to include criminal files while the potential impact of electronic access to these records was studied in a pilot program in eleven federal courts. A report on the pilot study was published May 7, 2003 (Rauma, 2003), and on March 16, 2004, the Judicial Conference approved implementation guidance and a model local rule for electronic access to criminal files, noting that the pilot project concluded that the benefits outweigh any risk of potential harm from enhanced electronic access.[1] This process also included public hearings and receipt of over 240 comments from persons representing public, private, and government interests. The public comments noted the many benefits of electronic access to these court records. One frequently mentioned benefit is that electronic access "levels the geographic playing field" by allowing persons located great distances from the courthouse to access public information.

Like the policy for civil and bankruptcy records, the federal court policy as to criminal records places the obligation on the litigants and their attorneys for partial redaction of specific, personally identifying information before filing documents with the court. The policy advises courts to post a notice stating that court clerks will not review a party's filings for redaction. The policy states courts will need to begin routinely to check documents the court itself prepares and to redact personal information in those documents. Specifically, whether the document is filed on paper or electronically, the policy requires the filer to redact Social Security numbers to the last four digits; financial account numbers to the last four digits; names of minor children

[1] The implementation guidance for federal courts and model local rules are available at http://www.uscourts.gov/Press_Releases/implement031604.pdf and http://www.uscourts.gov/Press_Releases/ modellocalrule031604. pdf.

to their initials; dates of birth to the year; and home addresses to city and state (Guidance, 2004). The policy also permits parties to file an unredacted document under seal. This complies with the E-Government Act of 2002, Publ. L. No. 107-347, which directs the federal court system to implement access to the Internet by 2004 and directs the Judicial Conference to promulgate rules to address concerns of privacy and security of court record information in light of best practices of federal and state courts. The court may still require the party to file a redacted copy for the public record.

The Judicial Conference Policy on Privacy also expressly names additional information, such as driver's license numbers, medical records, and employment history that may give rise to personal security concerns, and court users are advised that they may wish to file a motion to seal any of their documents containing this information. No document that is the subject of a motion to seal, nor the motion itself, is accessible by the public in any form until the court has ruled on the motion. With the criminal records policy, the court further restricts some record information, such as unexecuted warrants and presentence investigation reports, from becoming public, whether in the paper file or electronically accessed file. It should be noted that the Conference also adopted a policy to make transcripts of court proceedings available electronically, delaying an effective date on this policy while its impact on court-reporter compensation is assessed.

CCJ/COSCA *Guidelines*. The National Center for State Courts and the Justice Management Institute, with support from the State Justice Institute, had a national project for developing guidelines for access to records (Steketee and Carlson, 2002). During the period of public comment, over 130 comments were received from interested persons. Draft versions were reviewed at several meetings of the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA) and at combined meetings of these two state court administrative organizations. The result was a set of guidelines and a process that states can use to develop their own policies regarding access to state court records.

The guidelines address court records in both paper and electronic form, and although they are premised on a general rule that access should be the same no matter the format, they recognize that some information in court records may be inappropriate for remote electronic access. Essentially, the guidelines advise each state court to determine the types of court record information that should be restricted from remote electronic access and suggest mechanisms for doing so. The commentary to the guidelines suggests this information includes Social Security numbers, financial identifiers, medical records, and information about minors and third-party witnesses and victims.

Some state courts, such as those in Indiana, Minnesota, Nebraska, Maryland, Alaska, Ohio, New Hampshire, and South Dakota, have used the guidelines as a starting point to develop their court records rules and are in some stage of the process of adopting them. Each state makes changes to the CCJ/COSCA guidelines relevant

to its state laws and its form of court records. Many of these state court systems and others have created commissions that are currently studying the public versus privacy issues involved in electronic access to these records. In resulting court administrative documents, the relationship between two fundamental values is recognized and attempts are made to balance them: the right of the public to transparency in the administration of justice and the right of an individual to privacy. Legal commentators have also recently addressed these interests as they relate to placing court records online and making them available worldwide.

LEGAL COMMENTARY—PROPOSED SOLUTIONS

Many authors of law-review articles have not only discussed the legal issues in the public records versus private interests debate but have proposed practical solutions to the issues and to the creation of a system of rules that would protect personal information while maintaining the public court record. Daniel J. Solove (2002:1137) declared, "It is time for the public records laws of this country to mature to meet the problems of the Information Age." He wrote that a federal baseline must be established via a congressional act to govern public records in all states, with states having the ability to adopt even stricter protections of private information in public records. Solove asserted that the federal Privacy Act (5 U.S.C. §552a(b)) provides a basis for such legislation, but it would require amendment to apply to states and to provide more meaningful protection. The Privacy Act was enacted in 1974 following years of apprehension and study of computerized databases, but it only applies to the public sector and, thus, does not provide the control over use of Social Security numbers that some had hoped. The private sector may still collect, disclose, and sell Social Security number information. Moreover, the act does not extend its protection to court records. Solove advocates regulating the amount of personal information that is placed in public files in the first instance and making information accessible only for certain purposes.

Solove supports the enactment of use-restriction laws that would limit the use of information contained in public records to its original intended use, which is transparency of government actions. He explained that the principle of transparency of government actions had undergone an "ideological drift" and that "[t]ransparency today has become a tool for powerful corporate interests to collect information about individuals to further their own commercial interests, not to shed light on the government" (Solove, 2002:1199). Use-restriction laws would not permit personal information in public records to be used for commercial purposes, allowing information brokers to combine data into gigantic online databases that Solove called "digital biographies." Inaccurate information combined piecemeal by large information brokers can affect a nation beyond the problems of an individual's identity theft. One such instance is with the data that information broker ChoicePoint supplied to Florida election officials; that data prevented many persons, incorrectly identified as felons, from voting in the November 2000 presidential election. Restriction on com-

mercial use of public information would be permissible under the United States Supreme Court's decision in *Nixon* in which the right of access to public records was limited to proper use of the information in those records and where access was denied where such use was only for commercial exploitation.

Kristen M. Blankley (2004) examined several solutions that also include enacting legislation to restrict the information that initially is placed into court records. She proposed a complete ban on the following information from court records: Social Security numbers, bank-account and credit-card numbers, driver's license numbers, addresses, and the full names of persons involved in domestic-relations matters, such as divorce, child custody, and adoption. She suggested that action by state legislation, rather than individual court rules, would prevent each court's promulgating different rules that may lead to forum shopping and unequal access. However, it should be considered that court rules proposed by a state court administrator's office and adopted by a state's supreme court would alleviate these concerns and be a more appropriate way to govern court records than acts by state legislators. Other solutions Blankley discussed are increased use of protective orders to seal documents within court records, model rules to guide federal and state legislation, such as those developed by CCJ/COSCA, and amendment of federal and state constitutions to include right-to-privacy provisions where the latter do not provide for the right to privacy, as several now do.

Blankley suggested that if a particular record warrants the use of personally identifying information, this information not be made available for public viewing, either in paper or in electronic court records. She proposed that the burden for redacting sensitive information from these court records be placed squarely on the attorneys when they file documents with the court. The Judicial Conference guidelines previously discussed also place this responsibility for removing personally identifying information upon the attorneys filing the documents. This will require attorneys to become much more sensitive to the issues of privacy and communicate the risks of court record disclosures to their clients, so that an informed decision about disclosure and redaction may be made. Blankley further proposed that court clerks be responsible for redacting this information from any previously filed documents that would be accessible via the Internet.

To ensure compliance with these redaction requirements, Blankley offered two methods of enforcement. First, individuals could petition the court for removal of personally identifying information they find in their court documents. This remedy would be available to anyone, without a showing of harm as a result of the published information. Second, Blankley proposed a new cause of action against attorneys who place information into court documents without redacting personally identifying information. Blankley stated that this remedy would be available only upon a showing of actual harm, whether economic or psychological, and would be available against any attorney who placed the information in the court files, even those who did not represent the person harmed. Blankley indicated this remedy should also be

available to victims of stalking or harassment stemming from the victim's personal information being placed into court records and disseminated online.

Beth Givens (2002), director of the Privacy Rights Clearinghouse, proposed several solutions to reduce the negative consequences of making court records available electronically. She suggested that courts limit what is posted online to indexes, registers, and calendars. Givens also suggested that courts use only automation systems capable of redacting sensitive information so that the records can be viewed by court personnel but blocked from public view. This suggestion, also discussed by Silverman (2004), is an excellent one in allowing the work process to drive the use of technology rather than the other way around. Third, Givens implored courts to adopt rules that protect such information and examine their policy objectives in making their records available online. She also recommended that the information-broker industry itself needs regulating and accountability, something that does not currently exist except for the credit industry under the Fair Credit Reporting Act (15 U.S.C. 1681), which is governed by principles, including openness, access to data, correction of data, purpose specification, collection limitation, use limitation, security, and accountability.

Karen Gottlieb (2004) addressed another possible solution to the public-private issue in court records similar to the use restrictions Solove discussed. Gottlieb suggested that courts define permissible uses of the court records and state those uses in a data-dissemination contract between the court and the end user of the information. Kilpatrick (1995) also advocated the use of access contracts between courts and users of electronic court records and provided sample contracts courts could revise and adopt. Gottlieb suggested that such a contract be modeled on the Fair Credit Reporting Act's compliance procedures to ensure that information would only be used to promote and enhance the justice system. Downstream users of the data would also be required to certify the purpose for which they seek the information and that they will use the information for no other purpose. The original end user would be liable for civil penalties for improper use of information they directly obtained from the court as well as any improper downstream use of information that they share. Gottlieb's proposal also accommodated access of records that were sold by courts to bulk data distributors.

Gottlieb spoke of the erosion of public trust and confidence that can occur when courts do not take steps to protect their record information. She stated that most people do not realize that the majority of information in court records is public information and would never think their local court is giving away or selling their court record information. When fashioning a policy for electronic access to court records, most courts are unwilling to adopt rules that would expose confidential or protected information, thus jeopardizing the public trust and confidence of court users. Close examination of the proposals offered by these legal commentators provides some workable suggestions for a court's policy to improve public access to court records and better serve its users while protecting private information.

CONCLUSIONS

No government organization collects information about its citizenry that is as broad or as personally identifying and as sensitive in nature as that collected by court systems. Moreover, citizens are generally not in a position to refuse providing this information to the court. It is imperative that the courts themselves, not the legislative or executive branches of government, control this information and develop the rules that will provide public access while protecting private information in its supervision and control. It is a violation of the public's trust and confidence in the judicial system when courts knowingly allow private information to be accessed for purposes other than that for which the information was originally provided and for reasons other than shedding light on the workings of the judicial system. The United States Supreme Court has held that where a third-party request for information in a public record "seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted'" (*U.S. Dep't of Justice* at 780). The "practical obscurity" that has protected this information for years in paper records no longer exists when records are accessible and widely disseminated by electronic means. The balance of public access and privacy interests has shifted with the recent advances in technology.

Although courts as organizations are traditionally slow to act, the issue of electronic access to court records and the processes that govern this issue in a particular court system will not wait. John Martin, of the Court Executive Development Program of the National Center for State Courts' Institute of Court Management, teaches that the work itself should drive the processes used within any court system. With that in mind, the rationale underlying public access, that is, judicial accountability, should govern the process of electronic access to court records. However, many courts have allowed advances in technology, rather than the work itself, to drive their electronic access processes. Because the Internet exists, some clerks scanned documents in the court records and placed them online for easy access. In those relatively early days of electronic access, little or no thought was placed on the public's privacy interests, only that these were public documents and the technology was available for expanding public access. As previously discussed, these same clerks were required to remove court documents from Internet access while their state court administrative offices and state supreme court committees studied the issues and developed policies that protect citizens' privacy interests.

Technology is not the enemy, of course. The recent advances in technology have been put to good use in many justice systems across the country in ways that greatly benefit the public and reduce operating costs. Court systems have been able to integrate their vast amounts of information through case-management-information systems, providing statewide information to the public that was before only available by circuit or by county. Court systems have also been able to share information databases with other state government entities, such as those involved in law enforcement, corrections, social services, driver licensing, and provision of treatment, thus

improving the levels of service that all these governmental organizations provide to the public. Electronic searches of court systems' criminal-record databases by employers at hospitals, schools, and day-care centers have provided greater protection to the public. In many rural court systems, technology is used to move work processes to those less busy offices, allowing rural courthouses to remain open and clerk-of-court services to remain available to the residents in rural areas.

Technology can also provide a true cost savings for court systems in storing electronic records rather than paper records. A 1999 national study by the United States Department of Justice indicated that approximately 50 percent of a court's operating expenses could be attributed to the handling and storage of paper documents (Silverman, 2004). James E. McMillan, principal court management consultant at the National Center for State Courts, recently estimated it would cost just $25,000 for computer storage space for all of the court records for the state of Arizona (McMillan, 2004). With physical courthouse space at a premium and increasing costs for offsite storage for paper records, electronic storage presents a real advantage to court systems. As good stewards of taxpayers' dollars, courts would be remiss not to explore this use of technology with their court records. As technology continues to advance, courts will find more uses that will ultimately benefit the public they serve.

One particular advance in technology, the development of Extensible Markup Language (XML), has been touted as a solution that permits information in court records to be shared with the public at the courthouse and over the Internet while protecting certain data from access by some users and at the same time allowing other users, such as judges and court personnel, to view the entire record (Silverman, 2004). Using XML, tagged categories of sensitive and personally identifying information in a court record can be automatically and electronically redacted when accessed by the public without requiring the court system to maintain two separate systems of electronic court records—one public and one for use by court personnel. Instead of differentiating access to court records by method of access, electronic or paper file, access will be differentiated by the user. New versions of both Microsoft Word and Adobe Acrobat, used to create Adobe PDF documents, include support for XML. XML is the computer language chosen by the United States Department of Justice, Office of Justice Programs, in its development of the Global Justice XML Data Model, a program to increase sharing of data between the Justice Department and public-safety-information systems. It is also the language selected by the Organization for the Advancement of Structured Information Standards (OASIS) in developing its LegalXML project. This project produces standards for electronic court filing, court documents, legal citations, transcripts, and criminal-justice-intelligence systems. Both of these programs are customized to address the unique needs of court systems and the noncourt justice community. Even with this "new and improved" technology, it is important to remember to examine the work processes and allow them to be the driving force in decisions made regarding electronic access and information sharing rather than the mere existence of advanced technology.

RECOMMENDATIONS

For the past several years, Congress has been studying legislation that would protect Social Security numbers in public records, including court records. Proposed legislation requires redaction of Social Security numbers from court records within two years of enactment but remains under discussion pending legislative resolution of other problems with our Social Security system. Michael L. Buenger, Missouri state court administrator and former COSCA president, testified before Congress on June 15, 2004 regarding the impact such legislation would have on state courts and offered COSCA's willingness to work with Congress toward a viable solution. State court administrators realize it is not a question of whether this legislation will be enacted, but when it will be enacted, and are taking proactive steps to protect personally identifiable information in their court records.

On the basis of what has been described herein, the best way for courts to respond is to develop an electronic-court-records policy that satisfies several goals. Such a policy would:

Limit information in the case record. The type of information that is placed in the court's public record, paper or otherwise, should be limited, thus protecting sensitive and private information that could be used to gain identifying information that can facilitate criminal activity but does not shed light on court functions. Methods of collection should be developed that allow the court to continue to collect and use such information to the benefit of the public but that protect the data from public access.

Vary levels of access for different users. Differing levels of access should be permitted to different users of that information, thus allowing parties, attorneys, and noncourt government entities greater access than the public, which will ultimately benefit the public. The use of XML or other technology, which restricts access electronically to the entire court record for various users while allowing access by court personnel and judges, should be explored to avoid duplicative automation systems, thus reducing costs and the potential for entry errors.

Limit Internet access to court-generated documents. Public electronic access via the Internet should be limited to court-generated documents such as written opinions, judgments, docket sheets, indexes to the court record, and calendars. This is in keeping with the traditional rationale for public access to court records of shedding light on the activities of the judicial system. These documents rarely include personally identifying information that can be misused by identity thieves, and courts would be sensitive as to the nature of the information included in these documents. Consider Internet access, by judicial discretion, to the entire public file in high-profile cases.

Provide access to case records at public terminals in the clerks' offices. Access to all public documents in the case records should be permitted through electronic access at public terminals located at the clerks' offices. These could be accessed by court users in the courthouse, thus benefiting the public with greater access and the clerks by reducing their need to assist with public access.

Provide electronic storage of case records. Electronic storage of all case records should be provided. This saves space and money, benefiting the courts and the public. Technology that can serve dual-duty, that is, permitting electronic access to records while also achieving archival storage quality, should be explored.

A policy that includes these proposals would not only achieve judicial accountability and public trust and confidence, but also benefit court users with more efficient and effective access to court record information; court clerks would be able to make better use of their time and work efforts, and citizens would obtain more cost-effective use of taxpayer dollars. Wider dissemination of court record information through electronic means necessarily includes a responsibility for ensuring that courts do not inadvertently provide information that is subject to misuse, but does nothing to shed light on the operations of the judicial branch of government. Improved access to court record information and the courts themselves are laudable goals; we must be cognizant of all of the ramifications accompanying electronic dissemination of court record information as we work to attain those goals. **jsj**

REFERENCES

Blankley, K. M. (2004). "Are Public Records Too Public? Why Personally Identifying Information Should Be Removed from Both Online and Print Versions of Court Documents," 65 *Ohio State Law Journal* 413.

Chase, D. (2003). "Loudon Halts Online Land Records Access," *Virginia Lawyers Weekly*, August 11.

Cunningham, L. (2003). "Florida Freezes Posting of Online Court Records," *Miami Daily Business Review*, December 2.

Deyling, R. (2003). *Privacy and Public Access to Federal Court Case Files*. Washington, DC: Office of the Judges Programs, Administrative Office of the United States Courts.

Electronic Privacy Information Center (2003). *Privacy and Public Records*, last updated April 29, 2003. http://www.epic.org/privacy/public records/ (accessed July 13, 2004)

Frieden, T. (2004). "U.S. Wraps up Net Crime Sweep," August 26, 2004. http://money.cnn.com/2004/08/26/technology/cybercrime/index.htm

Givens, B. (2002). *Public Records on the Internet: The Privacy Dilemma.* San Diego, CA: Privacy Rights Clearinghouse.

Gottlieb, K. (2004). "Using Court Record Information for Marketing in the United States: It's Public Information, What's the Problem?" Paper presented at an International Workshop on WHOLES—A Multiple View of Individual Privacy in a Networked World, Swedish Institute of Computer Science, Sigtuna, Sweden. http://www.privacyrights.org/ar/courtmarketing.htm (accessed July 13, 2004)

Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files, Agenda E-6 (Appendix A), March 2004.

Judicial Management Council of Florida (2001). "Privacy and Electronic Access to Court Records, Report and Recommendations." Supreme Court of Florida, Office of State Courts Administrator, Tallahassee, November 15.

Keilitz, I. (2000). "Standards and Measures of Court Performance," 4 *Criminal Justice* 559.

Kilpatrick, K. P. (1995). *The Electronic Handshake: Public Access to Court Databases*. Williamsburg, VA: National Center for State Courts.

Lee, J. (2002). "Dirty Laundry, Online for All to See," *New York Times*, September 5.

McMillan, J. E. (2004). *Planning, Acquiring and Implementing Court Technology*. Williamsburg, VA: National Center for State Courts, Institute for Court Management.

Morgan, L. (2001). "Strengthening the Lock on the Bedroom Door: The Case Against Access to Divorce Court Records On Line," 17 *Journal of the American Academy of Matrimonial Lawyers* 45.

Morse, J. (2003a). "Web Cutoff Causes Butler Backlash," *Cincinnati Enquirer,* July 8, 2003.

—— (2003b). "Should Records Go On 'Net?" *Cincinnati Enquirer,* July 13.

—— (2003c). "Separating Court Records for Net Access May Be Costly," *Cincinnati Enquirer,* July 24.

—— (2003d). "Clerk Asks For Web Site Ruling," *Cincinnati Enquirer,* October 1.

Rauma, D. (2003). "Remote Public Access to Electronic Criminal Case Records: A Report on a Pilot Project in Eleven Federal Courts." Court Administration and Case Management Committee of the Judicial Conference of the United States.

Silverman, G. M. (2004). "Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records Over the Internet," 79 *Washington Law Review* 175.

Silvestrini, E. (2003). "Federal Prisoners' Personal Information Used in Credit Fraud," *Tampa Tribune,* February 8.

Solove, D. J. (2002). "Access and Aggregation: Public Records, Privacy and the Constitution," 86 *Minnesota Law Review* 1137.

Sovern, J. (2003). "The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules," 64 *University of Pittsburg Law Review* 343.

Steketee, M. W., and A. Carlson (2002). *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts*. Williamsburg, VA: National Center for State Courts and the Justice Management Institute.

Winn, P. A. (2004). "Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information," 79 *Washington Law Review* 307.

CASES CITED

McVeigh, United States v., 119 F.3d 806 (10th Cir. 1997).

Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978).

Office of the State Court Administrator v. Background Information Services, Inc., 994 P.2d 420 (Colo. 1999).

Westbrook v. County of Los Angeles, 27 Cal.App. 4th 157 (Cal.Ct.App. 1994).

Whalen v. Roe, 429 U.S. 589 (1977).

United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).