

## **Chapter 4: Management and Policy Issues**

This chapter covers numerous management and policy issues a court faces as it implements electronic filing. The introduction of technology can upset the operation of an entire court system, the people, procedures, papers, equipment, space, funding, and other resources that comprise judicial branch processes. Adjacencies may be altered and the roles of court staff may change significantly. While technology may eliminate or simplify many tasks, it simultaneously introduces new ones that must be assigned and absorbed into existing processes. Many of these non-technical issues may seem insignificant, but they can be critical to the success of the electronic filing project.

It is not appropriate to force technology to fit into an existing environment. Forcing new tools on old structures will not work because technology permits different and more efficient work processes, yet includes the potential for heightened risks that can accompany computerization. Furthermore, court leaders should recognize the opportunity to break with counterproductive traditions by modernizing court processes when introducing significant technological change to the judicial branch.

The reason management and policy issues require such close attention is that electronic court filing is about more than technology. Technologists focus on technology and sometimes fail to recognize management and policy issues. Court leadership must evaluate the potential benefits from changing current processes without being blinded by electronic glitter.

The following list represents management and policy issues that should be considered by court leaders before implementing an electronic filing system. The discussion of each of these topics fills the rest of this chapter.

- Payment of filing fees.
- Network and system capacity.
- Security.
- Authentication.
- Privacy and public access.
- Records retention.
- Service providers.

## **Payment of Filing Fees**

Courts collect filing fees, copy and certification fees and certain fines and collections from their customers. These fees generally are collected pursuant to statutes and rules. The clerks of court are charged statutorily with properly managing this function, and therefore are rightfully careful and cautious about handling money.

Historically, the payment for a filing has accompanied paper brought to the filing counter. As a party delivered a document to the court, fees were assessed and collected by the clerk. When documents arrive at the court electronically, how will filing fees and other charges be paid? Dollars cannot be created and transmitted in the same manner as word processing documents.

Some courts are exploring the area of electronic payment for services. They have developed methods to collect fees for providing access to records electronically, whether on tape/diskette or through computers.

Five payment systems currently are available to courts implementing electronic filing. A court may employ combinations of these methods, as needed. They are electronic funds transfer, escrow accounts, credit and debit cards, direct billing, and digital cash.

### ***Electronic funds transfer***

One of the easiest ways to collect filing fees automatically is to set up an electronic funds transfer system. When attorneys register to file documents electronically, whether

with the court or through a private service vendor, they can provide bank account numbers from which filing fees will be drawn. Similarly, vendors can give subscribers the option to have the vendor pay the filing fee electronically, and then bill the attorneys for the fees. The court provides a list of charges to its bank, along with the attorney or vendor account numbers. The bank then transfers the filing fees to the appropriate court revenue account. Attorneys receive notification of all transactions and can correct errors by contacting their service provider or the court.

If there are insufficient funds in the attorney's account to cover a transaction, the court handles the problem the same way it does a bounced check. Of course, attorneys would be required to notify the court of changes in bank account numbers. It should be noted that frequently there are service charges associated with electronic funds transfer – charges that many filers may find prohibitive when added to each and every fee transaction with the court.

An important feature of the electronic funds transfer system is that bank account numbers need not be sent through the Internet. Account numbers can be registered at the court, which can include them with transaction information sent to the bank via a direct dial-up or private network connection.

Electronic funds transfer, once fully implemented, can be an effective method of collecting fees. If courts run their own filing service, however, then establishing and maintaining the account information and reconciliation will require greater court staff resources, and more careful attention, than processing cash or checks.

### ***Escrow accounts***

An escrow account can be established for a case. The attorney creates the account by depositing funds with the court or a disinterested third party, depending on judicial

branch procedures. As documents are filed, the court transfers sufficient funds from the escrow account to cover the filing fees. The attorney or firm is notified if the account becomes depleted.

For example, an attorney may deposit \$150 into an escrow account when a complaint is filed with the clerk. The clerk deducts the appropriate amount from the escrow account and holds the remainder to be applied to subsequent filings or copying charges. At the end of the case, any unused balance is returned to the attorney.

This approach works equally well in paper or electronic filing systems, but it has some drawbacks. While it would be practical and more efficient to establish one account for the attorney or firm and apply charges for all its cases to that single account, some practitioners require individual accounts for each case. Each attorney account then has a separate court escrow account, doubling the number of accounts attorneys must manage. Also, not all courts have the expertise to provide interest-bearing accounts with end-of-year financial reporting statements, which also may be required by ethics rules. Finally, with hundreds of thousands of attorneys and other filers, the total amount “stored away” could reach tens of millions of dollars at any given point, and may not be the most efficient use of the money.

In an electronic filing system, an escrow account could be maintained by the court, the electronic filing service provider or a bank or other financial institution. The advantage to the court of using a service provider or financial institution is that the funds could be guaranteed contractually by the organization providing the service. Courts receive payment quickly, with little or no costly billing activity.

While this option is convenient, there are costs to court users. Banks charge fees for establishing, accessing and maintaining accounts, and financial resources of parties or attorneys may be tied up for long periods of time.

***Credit and debit cards***

Attorneys could provide credit or debit card numbers with documents filed electronically, thus charging their filing fees. Courts would receive payment from the credit card company, though a service charge would be deducted from each transaction. These service charges typically are up to several percentage points of the total transaction amount. Many courts have allowed credit card payment of fines for years.

Courts have found that the convenience of credit cards has increased the percentage of cases for which fine payments are made immediately. With fewer accounts unpaid, the court reduces the cost of managing receivables. Courts also receive payment more quickly from the credit card companies and reduce the risk of losses due to bounced checks. Courts are not dependent upon the cardholder for payment, and rarely does the payer challenge the transaction. Most importantly, credit or debit cards offer a convenient alternative for payment; improved service for the public is an important goal of the judiciary.

Some courts are reluctant to accept credit cards because of the service charge (merchant fee) that accompanies each transaction. Credit card companies, as part of their standard contract, do not allow courts to add a separate service charge to compensate for this fee. Some courts have negotiated lower fees with credit card companies, but most accept them and believe the advantages of increased collections way far outweigh the costs.

Another problem is the security risk of providing credit card numbers over the Internet. Two standards have been developed to alleviate this concern. Many Internet browser programs, such as Netscape and Microsoft Explorer, support Secure Sockets Layer (SSL). SSL creates an encrypted or coded communications link between the person using the browser and the server. A credit card number sent over the Internet using SSL cannot be deciphered by any other machine or router between the two corresponding computers. The United States federal courts are using the SSL browser security system in their electronic filing pilot projects.

Visa and MasterCard designed a second method of securing transmissions over the Internet, called Secure Electronic Transaction (SET). It is described on the Visa Internet page as follows:<sup>138</sup>

"SET SECURE ELECTRONIC TRANSACTION™ is a specification designed to utilize technology for authenticating the parties involved in payment card purchases on any type of online network, including the Internet. SET™ was developed by Visa and MasterCard, with participation from leading technology companies...

SET focuses on maintaining confidentiality of information, ensuring message integrity, and authenticating the parties involved in a transaction.

The significance of SET, over existing Internet security protocols, is found in the use of digital certificates. Digital certificates will be used to authenticate all the parties involved in a transaction."

### ***Direct billing***

A more traditional method of collecting filing fees is to bill the attorney or party when the court receives the document. This is more difficult for courts because a billing system must be established and maintained, and it is often more difficult to collect the fees once the court has accepted a document. Parties who are unhappy with the outcome

---

<sup>138</sup> <http://www.visa.com/>

of their action might refuse to pay altogether, and the collection costs for one case could exceed the revenue collected for many cases.

### ***Digital cash***

At some point in the future, digital cash will be transferred over the Internet as easily as the documents it accompanies. In a secure environment, funds will be deducted from a smart card and moved into the court's revenue account. The communications software will perform most of the processing work, so the overhead associated with these financial transactions would be minimal.

Courts will not be required to maintain account information on attorneys and service providers, only to forward the information provided with the transaction to their bank. The electronic filing servers can complete these processes, so little human intervention will be required.

Current drawbacks are the expense to attorneys of the hardware and software and account management to experiment with digital cash. Later on, issues will arise if attorneys need several cards – one for each client.

Nonetheless, as digital cash enters the mainstream of electronic commerce, its benefits likely will be seen in the area of electronic court filing.

### **Network and System Capacity**

Another management item that at first glance appears to be a “pure” technology issue is network and system capacity. Supporting a network, and providing sufficient capacity is what allows many filers to reach a filing system at peak times. Just as courts staff-up for busy periods during the day for paper filing, electronic filing systems must have enough capacity for busy periods.

There are a few important capacity measures: concurrent users – the number of users who can be on a system or server at one time; bandwidth – the speed at which information is passed between users and the system; and processing speed – speed with which the system carries out its processes. Without sufficient capacity, users such as attorneys will get slow response or “denials of service” from the system and those users will switch back to paper filing.

## **Security**

Security is an important issue for law firms and courts attaching their computers to the Internet. Almost everyone is concerned that data may be altered or removed, viruses may be introduced, or sensitive information may be accessed illegally. Attorneys must protect attorney-client privilege and work-product confidentiality when conducting business electronically. When preparing to implement electronic filing systems, courts should plan to protect their servers from Internet-based attacks by installing electronic in-baskets and firewalls, and by developing reliable transaction logging systems.

### ***Server security***

In the May 4, 1998 edition of InfoWorld magazine,<sup>139</sup> Stuart McClure identifies four phases of an Internet attack. They are:

- Phase one: Gather information.
- Phase two: Gain access.
- Phase three: Deny service.
- Phase four: Evade detection.

For example, a hacker might see that a court’s electronic filing web site allows a new user to establish an account with the court online. The hacker may set up a routine to repeatedly establish new accounts until the disk space on the court site is completely

filled, denying potential new users the opportunity to sign up. Denial of service problems could be particularly troublesome in the early stages of implementation, since skeptics in the court may be looking for reasons to rely on traditional paper filing. Courts must acquire the necessary software and hardware, or contract for these services, to protect their electronic filing systems from Internet attacks. Fortunately, Mr. McClure points out that of the many types of Internet attacks, denial of service attacks are "the easiest types of attacks for an administrator to defend."

What kind of hardware and software are needed to defend against Internet attacks? Chapter 6 discusses the concept of an electronic in-box, a computer that is placed between the court's servers and the Internet connection, outside of the security firewall. The electronic in-box accepts documents filed electronically without allowing outside users access to the internal court computer network. Programs running on court servers have security clearance to pass through the "firewall" to retrieve documents from the in-box computer.

PCWebopaedia defines a "firewall" as:<sup>140</sup>

"A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranet. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria."

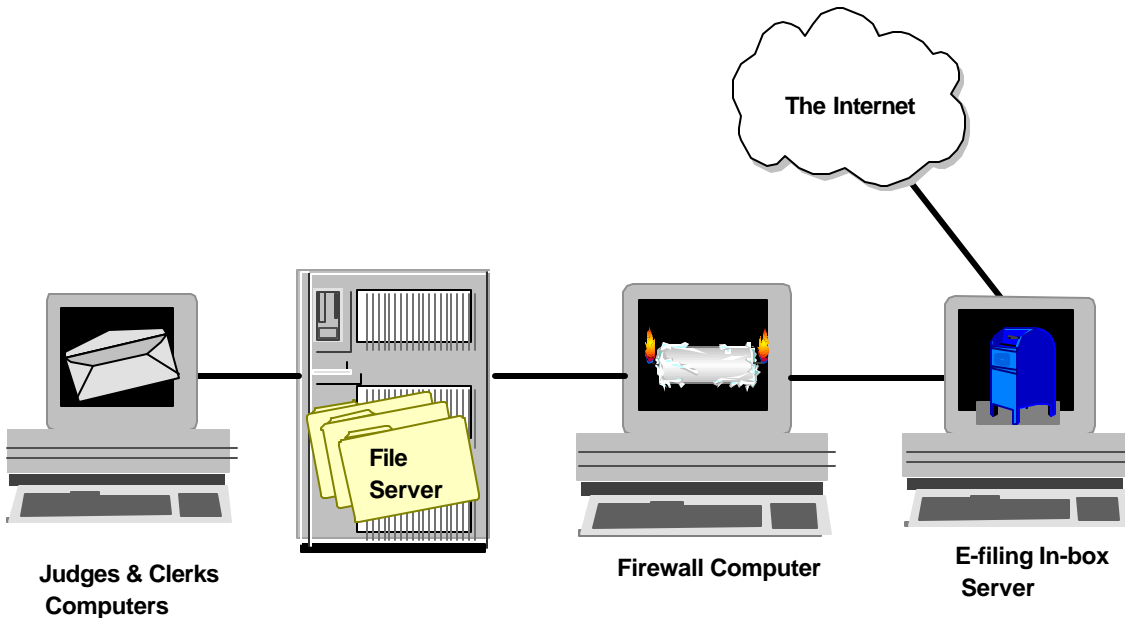
If connected to the Internet, a court should use some type of firewall to protect its internal network. The type of firewall system needed depends upon the type of computer network used and the sensitivity of cases the court hears. There is extensive help

---

<sup>139</sup> Stuart McClure, *InfoWorld Security Suite 16 Debuts*, InfoWorld, May 4, 1998, at <http://www.infoworld.com/cgi-bin/displayTC.pl?/980504sb1-iwss16.htm>

available from computer security consultants and system vendors who can work with a court or other organization to implement firewall hardware and software systems.

The following diagram shows how the electronic in-box and the firewall are configured to protect the court's information resources.



Notice that the firewall computer stands between the court's file servers and the electronic filing in-box computer. Also, note that both the file server and the firewall are between the judges and clerks using the network and the Internet. This kind of design provides the court's file server and individual computer users with two or three layers of protection, depending on network routing and protocols implemented.

For additional layers of protection, courts can use the secure file encryption software available with all major word processing software packages, and access control. If judges save their documents using a password, those files will be secure from tampering from both internal and external sources. Internal network security can ensure that only

---

<sup>140</sup> <http://www.pcwebopedia.com/firewall.htm/>

authorized users can gain access to information and documents stored on certain disk drives and subdirectories.

### ***Transaction logging***

Although transaction logging will not prevent attacks on court computer systems, it may help deter them and will help staff analyze and correct security and other technical problems that may damage information resources. Whenever any type of update is made to a database, an exact duplicate of the transaction can be made to a log file, typically kept on a separate computer disk. In the event of a system failure of any type, the backup copy of the database from the previous day can be restored to the disk, and the transactions from the log file can be reapplied, recreating the database as it existed before the problem occurred.

In addition, log files can be examined to determine who made a particular change to the database or accessed the information, if inquiries are logged. These audit trails can be extremely valuable if sensitive information is accessed inappropriately.

Electronic filing systems should log all transactions, at the electronic in-box and on the servers inside the firewall. This logging should:

- Track and store the origin and path of electronic mail coming into the system.
- Track the users attaching to the in-box and their activity, such as submitting a document to the electronic filing system.
- Log the *digital signature* (if used) of any files submitted, to eliminate any question of authenticity or completeness.
- Monitor financial transactions, such as use of credit cards or electronic funds transfer.
- Track the access, copying, and transfer of documents in any part of the electronic filing system.

Transaction log files must be maintained permanently and will be, eventually, printed on paper or transferred to Computer Output Microfilm (COM), CD-ROM, or other type of long-term storage medium.

## **Authentication**

To authenticate a document is to supply evidence to prove the identify its source and to verify the integrity of its content. Historically, signatures have been used for authentication. The court assumes that the document was submitted and its content prepared or authorized by the signer. Signatures are difficult to reproduce, and the process used for detecting impersonators is sufficiently esoteric and well established to discourage forgery. A signature, because it is unique to its owner, can be verified but not stolen. It is also infeasible to reproduce.

Of course, the signature was used for more than authentication of papers. It also expressed the approval or authorization of the signer, the intent that the transaction be legally binding. An old version of federal rule 11, adopted and still in use in some state court rules today (even though it is no longer used in the federal system), listed representations made to the court by a signature. Delaware's Court of Chancery rule is illustrative.<sup>141</sup>

### **Rule 11. Signing of pleadings, motions, and other papers; representations to the Court; sanctions.**

(b) *Representations to the Court.* By presenting to the Court (whether by signing, filing, submitting, or later advocating) a pleading, written motion, or other paper, an attorney or unrepresented party is certifying that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances:

(1) it is not being presented for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation;

---

<sup>141</sup> Delaware Court of Chancery Rule 11(b).

(2) the claims, defenses, and other legal contentions therein are warranted by existing law or by a nonfrivolous argument for the extension, modification, or reversal of existing law or the establishment of new law;

(3) the allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery; and

(4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on a lack of information or belief.

Other devices, in addition to signatures, have been used to authenticate documents. A notary public is authorized by state or federal government to administer oaths and attest to the authenticity of signatures on papers. Official seals once played an important role in verifying the authenticity of documents. Today, a date and time stamp is used by most courts to show when a pleading was submitted and that it is the same document originally submitted. In some states, staff is not allowed to remove staples from original documents out of fear that the authenticity of the submission might thereby be questioned.

While none of these techniques can guarantee that the purported sender submitted the document and that it has not been modified during or since transmittal to the court, our justice system has functioned effectively with this level of certainty. The introduction of photocopy and word processing technology did not raise serious questions about document authenticity, even though it is possible to attach scanned signature images to papers and make subtle yet significant changes to document contents without detection.

The development of document imaging systems first started court leaders and technologists thinking about document authenticity issues. As some courts started to rely on electronic documents as their primary source of information, holding paper versions as backups, these concerns were magnified. With electronic data interchange and electronic filing of pleadings emerging as viable additions or alternatives to paper systems, guaranteeing document authenticity has become a top priority for many.

Chapter 3 discussed passwords, electronic approval, electronic signature (both facsimile and imaging), signature dynamics, and digital signature technologies. This chapter has covered various security systems, such as access control, transaction logging, and encryption, which also can assist a court in authenticating documents.

Court leaders may argue that because authentication of documents is not a problem in the world of paper, it should not be a significant issue in an electronic environment. All documents are assumed to be authentic when the courts receive them. Because there are techniques for detecting and correcting problems with papers submitted to the court, those same techniques should be applied in the electronic world. Court leaders often are reluctant to consider large expenditures on digital signature or similar technology.

It must be understood that use of electronic commerce greatly increases the opportunities and the methods available to those who would disrupt judicial branch proceedings, while decreasing the likelihood of getting caught. While physical adjacency to paper documents was required in the past, the number of miles between a hacker and a courthouse is irrelevant. Because risk has been magnified, preparations must be strengthened. For example, in the case of some filings, courts need to know who is an attorney and who is not, and in this instance digital certification can help.

Courts must make policy decisions about which of these authentication techniques are appropriate for their environment. Higher levels of security cost more to acquire and operate. Decisions should be based primarily on two factors, strength (or effectiveness) and cost (or efficiency). The chapters that follow will provide insights into the costs of various approaches.

## **Privacy and Public Access**

Technology is changing the nature of court operations. What was once a completely manual, paper system is now becoming high-tech and electronic. Information is now available from multiple sources, paper files and computer databases. Electronic information is much easier to access than that stored on paper. This increased accessibility has raised questions about the appropriateness of traditional practices and rules. Traditional full and unfettered (albeit slow and expensive) access to court data can create significant problems for the judiciary and for those involved in court cases. Once electronic filing becomes a mainstream technology and the focus shifts from limited data about the case to the contents of all the documents in the file, the magnitude of both the benefits and concerns surrounding access issues will increase even more.

This section first will review public access and privacy issues separately, then show the need to balance the two in determining judicial branch policy with respect to information dissemination. Finally, guidelines for the development of policy will be presented. For a more detailed analysis of this subject, see Susan Jennen's work, entitled *Privacy and Public Access to Court Records*.<sup>142</sup>

### ***Public access***

Computerization of judicial processes and the general adoption of electronic commerce in many parts of our society have produced increasing pressure on courts to provide information electronically. While the right of the public to know what government is doing and hold officials accountable for their acts is a part of our custom and tradition, much of the interest in judicial branch data is motivated by different

---

<sup>142</sup> Susan M. Jennen, *Privacy and Public Access to Court Records* (Williamsburg, National Center for State Courts, 1995).

objectives. Many companies have found that providing data to the public is financially rewarding, particularly when they can shift production costs to a public organization. If a company can obtain data at no charge from a court clerk, add value to it to then sell it to the public or to other businesses, it may reap generous profits. Whether it be a lawyer publishing summaries of jury awards, a credit reporting company collecting judgment information for credit histories, a reporter doing an expose on a judge's sentencing practices, or a business compiling the names of recent divorcees for a mailing list, except where the court is paid (a common practice for tape compilations and record access) the public is bearing the expense of a private sector enterprise when the judiciary generates the data for these activities. How far should courts be required to go in providing free and open access to electronic court records?

A one-time request for information in a single case is far different than a requirement for weekly production of a computer tape containing specific data gathered from multiple computer systems. The volume and frequency of requests typically can overwhelm court technical staff, which usually has more to do for court users than it can handle.

Fortunately, data dissemination requirements placed on the courts have not been unlimited. State and federal law never have provided for completely open records. Discussions regarding how an appellate case will be decided, records of many types of juvenile proceedings, adoption case materials, and court personnel files typically have remained confidential.

Though practice varies from state to state, most courts allow full access to most non-confidential records that have been created in the normal course of business. Although some states require courts to format new records to match the specifications of the requestor, most do not.

***Privacy***

Federal and state laws have established the right of privacy, or the “right to be left alone.”<sup>143</sup> While computerization revolutionizes our ability to access information, it creates opportunities for abuse of individual privacy. Electronic searches can extract personal information from databases that would be impractical to assemble in a paper environment. These searches also can produce inaccurate results, such as listing court cases for people with similar names, with no way to distinguish between correct and incorrect information. Without privacy protections, individuals could be denied employment, insurance, scholarships, and other benefits and opportunities without knowing that the reason for denial was incorrect information obtained from a court database. It is ironic that increased demand for access to information has accompanied similar demands for greater privacy protections.

Our legal system allows court records to be sealed, purged, expunged, or to have access limited to specific purposes. As electronic filing systems proliferate, documents will be accessed and may be stored in many locations. Just as they are today when paper records are viewed and/or copied, when the court issues orders to remove or limit access to electronic materials, the orders will be impossible to enforce. Court leaders and legislatures should consider modifying these policies to apply them at the beginning of cases, rather than at the end, or traditional privacy protections may be lost.

***Balancing privacy and public access interests***

Rights of privacy and access overlap, often conflicting with one another. Federal and state policy provides boundaries, but most state courts have a great deal of discretion within those boundaries. Courts must adopt and follow policies that respect both the

right to know what government is doing and the right to be left alone. Of course, there are other issues that will be a part of this determination, such as the need for confidentiality in certain parts of the judicial process, security needs of the courts and the cost of various solutions.

A California case captures the essence of this balancing act.<sup>144</sup>

“While there is no question that court proceedings should not be conducted in secrecy, the public’s right to information of record is not absolute. Where 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.”

Laws and practice vary widely from state to state. It is impossible to provide precise guidance as to what the policy of any particular jurisdiction ought to be. The following guidelines were developed by the National Center for State Courts to assist with the process of developing policy that considers both rights of access and privacy.<sup>145</sup>

**Guidelines for Policy Development**

1. Understand federal and state legal requirements regarding public access and privacy rights. Review the following bodies of law:

<i>U. S. &amp; state constitutions</i>	<i>State common law</i>
<i>Federal statutes</i>	<i>State court rules</i>
<i>State statutes</i>	

2. Identify the degree of discretion that the court or state judiciary can exercise in defining record access rules, policies, and procedures.
3. Consider court operational issues that may affect discretionary decisions.
4. Analyze electronic court information to facilitate decision-making.
5. Actively share resources and ideas with other state and local courts.

---

<sup>143</sup> *Griswold v. Connecticut*, 281 U. S. 479 (1965).

<sup>144</sup> *Westbrook v. Los Angeles County*, 32 Cal. Rptr. 2d 382 (Cal. App. 1994).

<sup>145</sup> Susan M. Jennen, *Privacy and Public Access to Court Records* (Williamsburg, National Center for State Courts, 1995), p. 39.

6. Develop public access policy and practices by balancing the relevant factors within the state and state court system; create a "working" document to record and update findings and conclusions.

Courts want to provide information to the public. They also must protect the privacy of individuals. Yet, they desire to promote the use of technology to increase access to the courts for all citizens. Unfortunately, all these objectives cannot be achieved without compromise. This may be one of the most important areas of policy determination for court leaders.

## **Records Retention**

Management of paper files consumes a great deal of court and law office resources. The introduction of computer systems lowered the cost of collecting and storing it, but not the cost of categorizing it. The introduction of electronic filing and document management systems will introduce new records retention issues that must be addressed. If policy is created with the design of the system, it will be much more effective and cost less to administer.

### ***Retention of paper records***

Most courts have faced problems with record storage at one time or another. For many large courts, this is an acute problem that must be managed continually. Overflowing records rooms and inefficient procedures developed to deal with the problem are symptoms of inadequate records management.

Some courts instituted microfilming programs to ensure that older files could always be retrieved. This microfilming originally was done at the conclusion of a case, just before a paper file was sent to an archive or destroyed. Later, as paper management problems produced more and more lost files, some courts began microfilming documents

upon receipt. This resulted in delays in acting on a pleading for as long as a week. Because all the materials in the case file were not on the same roll of microfilm, it was still necessary to film the cases again at the end of processing. Although this may seem like a ridiculous solution, it has been practiced by hundreds of courts throughout the United States.

For a variety of reasons, some courts have created multiple files for the same case. Sometimes this is for purposes of protecting confidentiality—sensitive material is excluded from a file used for public access. Some courts create a separate file for the judge’s area. Lawyers representing litigants also maintain files of materials and must deal with storage issues.

Some courts, prosecutors and law firms have procedures for purging files for long-term storage. This procedure consists of reviewing every page in a case file, retaining a few specific documents and discarding the rest. This reduces the size of the case file so it consumes less space in the records room, but the amount of time required to purge each file far exceeds the cost of storage space.

When records rooms become full, many courts use off-site archive facilities for older cases. It requires a great deal of effort to keep track of the location of individual cases to ensure they can be retrieved, if necessary.

At some point, most court case files are no longer needed. Some courts are not allowed ever to destroy these public records, but most eventually purge older materials. Traffic tickets, for example, often are destroyed as soon as the conviction disappears from a person’s driving record, roughly three to five years after the case disposition. Felony convictions may be retained permanently.

A final issue with paper files is retrieval. Although very few historical records are ever needed again, occasionally one is required. Courts may spend hours trying to locate these old files.

### ***Records retention and computerization***

If there is any universal truth in court automation, it is that judicial branch employees want to have all case information available forever. Were it not for the expense and limitations of technology, electronic archiving never would have been developed for case management systems. As the cost and capabilities of computer hardware have improved, technologists have discovered another problem. While it has become possible and affordable to retain case information for decades, it is still not desirable to do so. The reason is performance. Even though a file of docket records can hold millions of entries, the length of time needed to retrieve an individual record increases with the file size. The index records that track individual entries must be read to locate specific information. If a docket entry can be found with a few reads of the index file, then response time is rapid. As the size of the index file increases, the number of reads on the file will grow, and response time deteriorates to an unacceptable level. It is still wise to manage electronic records just as carefully as paper, to avoid these problems.

The second generation of court computerization moved away from large, centralized computer systems to distributed environments. Smaller minicomputers were placed in individual courts and networked together. This reduced the size of the electronic files and provided better performance on cheaper equipment. These systems were more efficient at their most important work, supporting trial court activities. Generation of statewide statistics became more cumbersome, but the tradeoff was more than worthwhile for everyone at that time.

Even with distributed systems, courts found it necessary to keep file sizes as small as possible by purging older records. Because state criminal history repositories maintain files of convictions and sentences, courts found it easy to remove criminal cases shortly after work was completed. But new legislative initiatives, like *three strikes* and the Brady law, created a greater need to be able to review details of older convictions.

An emerging technology relevant to court case information management is data warehousing. A warehouse is a server that stores information. It is still accessible to court users, but is not stored with active case data. Though it takes a little longer to retrieve, it is still on-line information. Using a data warehouse, courts can maintain *legacy data* indefinitely without hampering day-to-day operations. The warehouse also can be used to consolidate cases from multiple servers for inquiry purposes in a distributed environment.

### ***Electronic filing and records retention***

The use of document management systems actually will increase the need for active management of court records for two reasons. First, the electronic case file will be the primary source of information about the case and paper documents will be a backup source. With today's computer systems, the roles of these record types are reversed. Second, as courts implement electronic filing fully, the paper case file will cease to exist. Without tight integration to management systems, documents conceivably could be filed with other papers submitted on the same date, not with pleadings for the same case. It still will be possible to reconstruct a file with paper in case of a catastrophic system failure, but this will require considerably more time and effort.

Because electronic documents require much more space than docket entries describing them in a case management system, the storage needs of courts and law firms

will grow significantly. As with data entries, very large document files will at some point begin to impair retrieval time, degrading system performance. Courts always will be required to manage their information storage resources, regardless of whether they are found in the basement of a building or on an optical disk platter.

Retention policies should be adopted as the system is designed, rather than waiting for performance problems to create a crisis. If a court decided, for example, to flag certain document types for deletion two years after case disposition, it would be a simple matter to begin removing these records when storage space became a problem. If a court waited to make this decision until there was a problem, it would have no way to identify these pleadings without individual review of tens of thousands of pages. The development of electronic records retention policies must be an integral part of system design.

### **Service Providers**

When a court owns and operates its own technology system and chooses to incorporate electronic filing into that overall system, it also takes on the burden and responsibility of a service provider. While, in a sense, courts have always provided services to attorneys, those services have been the traditional ones of a clerk's office, most of which commence only after a pleading has crossed the counter on paper. With electronic filing, there is now a technology service component to be delivered as well.

Some courts will decide to avoid the costs, complexities and potential headaches of the service provider role by allowing third-party, commercial firms to handle the electronic filing component. For courts that already are using a commercially developed case processing system and receiving system support from the vendor, this decision is

almost a foregone conclusion. These courts will be concerned mainly with whether their case management system is tightly integrated to the system capabilities. In addition, many courts that have developed and will continue to maintain their own case management systems may elect not to own the front-end technology needed for electronic filing. Just as some judicial technology departments have let third parties connect electronic public access systems to the court's databases, many courts will turn to outside service providers for electronic filing. When a court decides, for whatever reason, not to take over the traditional private function of courier and messenger, then the choice of a service provider, cost factors and the need to ensure the quality of the service that is delivered become critical issues.

### ***Role of service providers***

Service providers may have a varying role in the overall technology and operation of a court, depending upon the characteristics of each court. In some courts, the vendor will assume the maximum role of providing the entire technology infrastructure to support the court. A maximum role would involve providing several components:

- Case management system.

- Electronic public access system.

- Electronic filing interface, consisting of:

  - Interface with court database and case management functions.

  - User interface (client software resident on the attorney's PC).

  - Electronic filing functions, including:

    - Electronic packaging of attorney's documents.

    - Authentication and security.

    - Transmission to court.

    - Time stamp and acknowledgement.

    - Fee processing.

    - Workflow routing for review and approval.

    - Updating of case management system database.

    - Noticing (electronic or hybrid).

- Customer service.

- Installation support.

- Training on-site.

- Marketing/promotion.
- Upgrades and ongoing enhancements.
- Integrated benefits to other systems.
- Support for new operating systems, browsers and other filer technology.

A minimal role, on the other hand, could involve providing only a single component, such as a secure dial-up connection for the attorney. In fact, during the early stages of an electronic filing implementation, it may be necessary to provide conversion services to law firms that do not meet the requisite level of computerization to file directly. The Republic of Singapore, for example, which initiated an electronic filing project for civil litigation in 1997, addressed this problem through the use of private “law bureaus.” These service firms operate as an intermediary, accepting paper pleadings from law firms and submitting them electronically to the courts.

Just as courier services now exist in most U.S. cities to handle the transportation and physical submission of paper pleadings, there may be an interim role for an “electronic courier” service as courts begin to convert to electronic documents. Such services could be furnished by the vendor that provides the electronic filing system or by independent businesses that are themselves end users of the electronic filing system.

For a given court and legal community, the range of potential functions and services would be delivered through some combination of shared responsibilities among court staff, one or more vendors and law firm staff.

### ***Major issues***

When considering the role and responsibilities of an electronic filing service provider, courts must address a number of sensitive issues that have not been of concern in a paper environment. Although there is much overlap, these can be grouped into three categories: policy issues, management and procedural issues and technical issues.

**Policy issues:**

Allowing a filer to update court database without court supervision.  
“Partnership” roles and responsibilities (court—service provider—attorney).  
Exclusive *versus* open service provider agreements.  
Fee structure and revenue sharing.  
Authentication and security standards.  
Liability for system “down-time” and transmission failures.

**Management and procedural issues:**

Financial accounting and billing.  
Training of users.  
Time stamp (e.g., if an attorney files at 4:59 or 11:59 p.m., how to ensure that the court receives it at the same effective time).  
Assurance of noticing.  
Future modifications to case management system and database (how to ensure that electronic filing interface will be kept compatible without delays).

**Technical issues:**

Ease of use.  
Method of transmission (e.g., direct dial-up or Internet).  
Uptime approaching 24 hours a day.  
Sufficient capacity to handle peak volumes.  
Speed of total transaction.  
Providing secure transactions (attorney to provider, provider to court).

***Ensuring satisfactory service providers***

Courts have much at stake when they take the significant step forward into electronic filing. While electronic public access systems raise important policy issues as we have discussed, they serve primarily an inquiry function with minimal danger of adversely affecting court records. On the other hand, electronic filing, by design, most definitely affects the content of court records, just as pleadings filed on paper do. Clerks of court should expect to review filing submissions in electronic forms much as they do paper submissions today delivered by lawyers, couriers, messengers and the public. In addition to facing a variety of legal, procedural and technical hurdles, courts must overcome the inertia of tradition and address the doubts and concerns among both court officials and the bar. Consequently, they must exercise great care in selecting the service providers

they rely on for this critical function and ensure that proper safeguards are in place to protect the judicial processes.

