1-1-2004

Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records over the Internet

Gregory Silverman

RISE OF THE MACHINES: JUSTICE INFORMATION SYSTEMS AND THE QUESTION OF PUBLIC ACCESS TO COURT RECORDS OVER THE INTERNET

Gregory M. Silverman*

The machines are coming. They have been slowly taking up positions in our courthouses for more than a quarter of a century. With each passing year, they are becoming faster and more powerful. They are evolving intelligence and the ability to communicate with each other. With their assistance, the justice system is becoming more efficient—an integrated network. Soon the courts, justice agencies, law enforcement, correctional facilities, social services, and treatment providers will be able to interoperate seamlessly. Moreover, the justice machines will be able to reach out and assimilate into their network the millions of machines connected to the Internet and owned by the public, enabling the exchange of information on a scale and with an ease never before imagined. With the assistance of the machines, the myriad and diverse members of the justice and public safety communities together with the public will evolve into a single complex whole that could dedicate itself to creating a more humane and just society comprised of better informed individuals to whom they are genuinely accountable.

Some, however, are not so sanguine. They view the rise of the machines as ominous and foreboding—threatening our privacy and the erosion of human freedom and autonomy. As information flows through an integrated justice system out to the public, they worry that human actions and relationships will be subverted by these machine connections: that people will change their behavior out of fear that their frailties, misfortunes, and "unusual" preferences will be revealed and reviled, exposed and ridiculed. To avoid this travesty, they argue, privacy must supervene our traditional commitment to public access: we must tolerate some opacity in our governing institutions and limitations

* Associate Professor, Seattle University School of Law. M.A. 1984, J.D. 1987, M.Phil. 1991, Columbia University. For helpful comments on earlier drafts of this Article, the author gratefully thanks Keith Aoki, Pat Brown, Steve Burnett, Vince Chiapetta, Mark Chinen, Maggie Chon, Annette Clark, Anne Enquist, Bob Gomulkiewicz, Lilly Kahng, Jack Kirkwood, Evan Lenz, Lydia Loren, Bob Menanteaux, Joe Miller, Chris Rideout, Veronique Silverman, John Strait, Jane Winn, and Peter Winn. I would also like to thank my research assistants Yvonne Mattson and Keith McGahan for their excellent assistance on this project.

on our access to them. According to these doomsayers, inexpensive and convenient public access to court records over the Internet must be abjured if we are to preserve what remains of the collapsing catacombs of personal privacy beneath an increasingly mechanized and hostile world.

Fortunately, the dilemma between privacy and public access is a false one, nor the world as Orwellian as the first paragraph might suggest. The same technology that heralds unprecedented public access at minimum cost and maximum ease also enables an automated intelligence that is capable of understanding and processing data in sophisticated and nuanced ways yet to be generally appreciated outside the circle of technologists who currently work with it. This technology—Extensible Markup Language (XML) and its family of related browsers, parsers, processors, and standards—permits information in court records to be shared with the public at the courthouse and over the Internet while respecting the legitimate privacy interests of litigants and others who come before our courts. With it, humans really can achieve a more just and humane society—one in which they remain clearly in control.

In the first half of the present Article, I introduce the reader to this technology (Part II) and its likely role in evolving justice information systems (Parts I and III). In the second half of the Article, I enter the debate over whether the public should be permitted access to court records over the Internet. After explaining the origins, history, and principal sides of this debate (Part IV), I argue, first, that when used properly, XML permits the public to have access to court records over the Internet while promoting public safety and protecting personal security (Part V) and, second, that the presence of discrediting and embarrassing facts in a case file does not justify limiting public access to court records over the Internet while permitting unlimited public access at the courthouse (Part VI).[1]

I. CASE MANAGEMENT INFORMATION SYSTEMS: FROM INDEX CARDS TO XML

Before the development of electronic databases, tools for managing large quantities of information included paper notebooks, ledgers, and variously sized wooden cabinets and cardboard boxes filled with paper index cards. During this period, if one wanted to determine if a person or

1. See *infra* Part VII for a more detailed overview of my argument.

business were involved in litigation, one had to travel to the local courthouse of a particular jurisdiction and scan the columns in a court ledger or flip through a narrow drawer of carefully alphabetized index cards. Using paper-based information management tools such as these, court personnel developed often elaborate and ingenious systems for recording and tracking information essential to the daily operation of the court.

With the rise of modern computing and electronic databases, courts began to migrate from paper-based systems to electronic information systems. Frequently referred to as *case management information systems*, these systems are in fact database management systems (DBMSs) that court personnel use to input, store, manipulate, display, and print information relevant to such daily court tasks as case filing, calendaring, docketing, case maintenance, recording judgments and sentences, accounts receivable and collections, cashiering and creating receipts, trust accounting, checking and banking, failure to appear and warrant processing, as well as management and statistical reporting. As one can see from the preceding list, the functionality and use of these systems extend far beyond case management narrowly construed. Accordingly, such systems might better be called court record management systems or simply *judicial information systems* (JISs). Both labels are used in discussions of court automation and integration.

Of the more than 16,000 courts in the United States,[2] not all immediately migrated to electronic case management information systems. Initially, few courts had both the funding and the technical expertise to make this transition. The early case management information systems required large and expensive mainframe computers running proprietary, often custom-written, software that was hard to modify, and could only be accessed through dumb CRT (cathode-ray tube) green-screen terminals. With the development of microcomputers in the late 1970s, these early information systems running on mainframes were either replaced or supplemented with personal computers on the desktop of select court personnel. As the price of computer hardware and storage fell and an understanding of the new technologies increased, more and more courts forswore their paper-based systems and entered the information age. While these personal desktop computers ran "productivity" software that permitted the

2. BRIAN J. OSTROM & NEAL B. KAUDER, EXAMINING THE WORK OF THE STATE COURTS 12 (1996).

recording and management of information, the data entered into these computers became "trapped in the machine" and could only be shared with others through printed lists and paper reports.[3] With the introduction of modern networking technologies such as Ethernet in the mid to late 1980s, a court's isolated desktop computers could be connected together into a courthouse local area network (LAN). Using software that causes a personal computer to emulate a dumb CRT terminal, even a court's existing mainframes could be tied into this courthouse network—with some effort. By the late 1980s and early 1990s, most courts—to the extent that they could afford it and the courthouse facilities permitted it—were stringing their desktop computers together with network access cards and Ethernet wiring.

Without a doubt, connecting a court's computers into a single LAN was a real achievement and an important milestone in the history of court automation and integration. For the first time, court personnel could access, in real time and from their own desktop computers, the various electronic databases running on different computers within the courthouse. Nonetheless, network connectivity by itself could not provide a single integrated view of all the information and data relevant to a particular case or even of a particular event within a case. Courts, having automated their operations while the computer and software industries were still maturing, had different court processes and functions that were automated at different times, on different platforms, by different software programs. As a result, in many courts, the data relevant to any particular case was not found conveniently centralized in a single database management system but in several such systems and software programs distributed over the entire network. For example, to access the schedule for a particular case, one might have to consult a stand-alone calendaring program; to check whether a party had filed a document in that same case, a stand-alone docketing program; and to confirm payment of a court fee, a stand-alone accounting program. Before one could achieve a single, integrated view of all the information and data relevant to a case, one would have to not only network all of the

3. While one could transfer the data file from one desktop computer to another one using a floppy disk, this practice was not advisable as it posed significant risks to the accuracy and reliability of the information system. The transferred copy, for example, would be immediately out-of-date (since it could not be updated in real time as new information was added to the original), and created the possibility of divergent and conflicting data stores (if one added new information to the copy rather than the original).

computers storing such information but integrate the programs and information systems running on these machines as well.

While technically daunting, the benefits that result from programmatically integrating a court's information systems are clear: cost savings, error reduction, and improved performance. Simply integrating the diverse information systems in a single courthouse reduces a court's operating costs significantly. According to one study, approximately fifty percent of a court's operating expenses may be attributed to the handling and storage of paper documents.[4] While the introduction of electronic information systems reduces the volume of paper that court personnel must handle, integrating these information systems reduces this volume even more. The ability to enter data and access electronic records over a single court network obviates the need for paper forms as well as printed lists and reports that are used to "paper over" or "bridge" the information chasm that separates these islands of data.

In addition, integrating a court's information systems reduces the cost of maintaining duplicative records across multiple systems. When a court's information systems are not integrated, each system must contain information that duplicates records residing on other court systems. For example, the docketing database, electronic case index, and court accounting program—to name just three applications—will all need to contain information about parties and their attorneys. When this information changes, it must be updated separately on each system. If, however, these three systems could share data with one another, such duplicative recordkeeping would be unnecessary; each program could simply call up the information from a central database as needed. Court operating expenses would be reduced to the extent that court personnel would no longer have to repeatedly enter the same information into different information systems. Moreover, when information changes, all systems could be kept current by simply updating a single record in the central database.

Integrating court information systems in a manner that permits electronic filing also lessens personnel costs by reducing the number of court personnel needed to cover the counter in the court clerk's office. Finally, the ability to route electronic documents to judges, parties,

4. NAT'L TASK FORCE ON COURT AUTOMATION & INTEGRATION, U.S. DEP'T OF JUSTICE, REPORT OF THE NATIONAL TASK FORCE ON COURT AUTOMATION AND INTEGRATION 29 (1999), *available at* http://www.ncjrs.org/pdffiles1/177601.pdf.

attorneys, law enforcement officers, witnesses, and others reduces postage and delivery expenses.

Besides these financial savings, integrating a court's information systems also reduces data entry errors and related problems. When data must be entered more than once, there is a greater likelihood of mistakes: information may be entered inaccurately or incompletely. If such information were stored as a single record on a central database, redundant records would not be needed and the opportunity for data entry errors obviated. Integrating a court's information systems also improves the court's ability to meet the American Bar Association Standards Relating to Court Organization and adjudicate the cases before it "justly, promptly, effectively, and efficiently."[5] Judges and other court personnel can immediately access the information they need when they need it. Delays due to lost or incomplete paper files are avoided. Court scheduling conflicts are identified and prevented. Electronic reminders of required tasks are displayed. The gains in productivity and quality of service that result from a court's integrating its information systems are as varied as they are numerous.

Even more benefits accrue as courts integrate their information systems with the information systems of other courts, justice and public safety agencies, social services, and treatment providers. An especially compelling example of the benefits to be achieved by integrating court case management information systems with information systems run by a sheriff's department or department of corrections is provided by the Los Angeles Sheriff's Department: an inmate serving time on misdemeanor traffic violations was mistakenly held for nine months after he should have been released. The inmate, thirty-three year old Thao Quoc Huynh, was sentenced to serve four *concurrent* 150-day sentences for driving under the influence, hit-and-run, and two other traffic violations.[6] However, due to confusion over paperwork received from the court, the inmate ended up serving four *consecutive* sentences, keeping Huynh behind bars for 271 days beyond his correct release date.[7] Sheriff Sherman Block explained this error by noting that the paperwork that was sent to the jail from the courthouse was ambiguous,

5. Section 1.00 of the 1990 Standards of Judicial Administration promulgated by the Judicial Administration Division of the American Bar Association declared that "[t]he organization of a court system should serve the courts' basic task of determining cases justly, promptly, effectively, and efficiently." STANDARDS OF JUDICIAL ADMIN. § 1.00 (American Bar Ass'n 1990).

6. Tina Daunt, *Man Held for 9 Extra Months Freed from Jail*, L.A. TIMES, May 23, 1998, at B1.

7. *Id.*

indicating that Huynh was to serve both concurrent and consecutive sentences. Unfortunately, the clerk at the jail failed to contact the court for clarification regarding Huynh's sentences and simply processed the inmate as if he had been sentenced to serve the sentences consecutively.[8] Additional research by a reporter for the *L.A. Times* revealed that

> the problem of over-detaining inmates has been going on for years. In 1997, nearly 700 inmates were held in county jails for an average of 6.9 days past their ordered release dates. One inmate was held 260 days too long; two others were held for 90 days or longer. All too aware of the county's financial liability on the issue, the department's risk management unit in 1997 paid nearly $200,000 to 548 inmates who were incarcerated for a total of 3,694 days beyond their sentences—on the condition that they agree in writing not to sue.[9]

To address this problem, Sheriff Block stated that his "department is establishing a computer system that will link the Inmate Reception Center with courthouses, eliminating the need to manually process thousands of pieces of paperwork at the jails each night."[10]

In addition to reducing the number of human custodial errors by providing the relevant justice agencies with accurate information regarding court judgments and sentences, integrating court and justice agency information systems provides the courts with better and more timely information concerning parties before it, thereby enhancing the quality of the courts' decision-making. Integrating the courts' and justice agencies' information systems also facilitates court compliance with various reporting, record checking, or data collection requirements imposed by state and federal legislation. For example, on the federal level, the National Child Protection Act of 1993,[11] the Brady Handgun Violence Prevention Act,[12] the Lautenberg Amendment[13] to the 1968 Gun Control Act,[14] the Jacob Wetterling Act (including Megan's Law),[15]

---

8. *Id.*

9. *Id.*

10. *Id.*

11. 42 U.S.C. §§ 5119–5119c (2000).

12. 18 U.S.C. § 922.

13. 1997 Omnibus Consolidated Appropriations Act, *id.* § 922(g).

14. 18 U.S.C. § 922(g)(8) (1994).

15. Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, 42 U.S.C. § 14071 (2000).

the Pam Lychner Act,[16] and the 1994 Violent Crime Control and Law Enforcement Act[17] all impose reporting, record checking, or data collection requirements on state courts or justice agencies. Compliance with these requirements necessitates close coordination and data sharing between the courts and justice agencies. Similar coordination and data sharing are also required to comply with state laws imposing enhanced sentencing for repeat offenders (so-called "three strikes" legislation) as well as laws enacted pursuant to Megan's Law requiring registration of sex offenders and some form of community notification upon their release.[18] Finally, to the extent that such reporting and data sharing prevent dangerous criminals from being released due to inaccurate or incomplete information, halt the sale of guns to convicted felons, and apprise communities when known sex offenders move into their area, integrating the information systems of the courts and justice agencies also improves public safety.

Significant benefits also accrue when courts integrate their information systems with social services, such as welfare and child support services, and treatment providers. To a greater and greater degree, courts are forming an essential and central hub for the delivery of social services. With the rise of alternative sentencing, domestic violence courts, drug courts, and a variety of diversion programs, courts find themselves coordinating closely with traditional social services and treatment providers. When a court places a defendant in a drug rehabilitation or anger management program, it must periodically hold review hearings and monitor the defendant's attendance and progress. In a drug program, the results of a defendant's regular drug tests must also be collected. Alternative sentencing, such as community service, requires a court to remain in regular contact with the organization or agency overseeing the defendant's work. Assigning defendants to a residential treatment center requires the court to monitor the availability of beds at that center. The need to collect and manage new forms of information in an increasingly large number of cases places an enormous burden on court personnel and the limited resources at their disposal. These burdens may be substantially reduced and the evolving social services functions of the court greatly expedited if courts are able to

16. Pam Lychner Sexual Offender Tracking and Identification Act of 1996, *id.* § 14072.

17. National Stalker and Domestic Violence Reduction, 28 U.S.C. § 534.

18. *See, e.g.*, CAL. PENAL CODE § 11105 (West 2003); WASH. ADMIN. CODE §§ 446-20-500 to -510 (2003).

share and exchange data with the social services agencies and treatment providers that support the justice and public safety communities.

In light of the myriad and substantial benefits that accrue when isolated judicial information systems are integrated within and between courts, justice and public safety agencies, social services, and treatment providers, the justice and public safety communities should clearly be striving to achieve as complete an integration of judicial information systems as possible. Nor has this conclusion been lost on national and state policymakers. In 1999, the National Task Force on Court Automation and Integration declared that "[t]he time has come to improve the quality of the nation's justice system by improving information exchange within the system."[19]

Making a similar point, the Judicial Information System Committee (JISC) for the State of Washington has observed that the software applications composing the State's current JIS Application Portfolio "are, to a significant degree, islands of automation" with "significant levels of functionality [that] remain redundant and isolated from the rest of the court enterprise."[20] The JISC is working to replace these islands of automation with "a strategic, enterprise-wide court information system in the state of Washington"[21] that will "automate and support the daily operations of the courts" as well as "maintain a statewide network connecting the courts and partner criminal justice agencies to the JIS database."[22] In order to achieve such an integrated, statewide judicial information system, the JISC concluded that the courts and justice agencies must migrate from existing legacy systems to applications, using an object-oriented Web-based architecture.[23] The State of

19. NAT'L TASK FORCE ON COURT AUTOMATION & INTEGRATION, *supra* note 4, at 2. The National Task Force on Court Automation and Integration was assembled to guide the Court Information Systems Technical Assistance Project, a joint project of the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); SEARCH, the National Consortium for Justice Information and Statistics; the National Center for State Courts (NCSC); the National Association for Court Management (NACM); and the Conference of State Court Administrators (COSCA).

20. Judicial Information System Committee, Washington State Office of the Administrator for the Courts, *JIS Migration Plan*, *at* http://www.courts.wa.gov/jis/?fa=jis.migration (last visited Jan. 2, 2004).

21. *Id.*

22. *See* Judicial Information System Committee, Washington State Office of the Administrator for the Courts, *Judicial Information System (JIS)*, *at* http://www.courts.wa.gov/jis (last visited Sept. 7, 2003).

23. This migration is necessary because "[l]egacy applications are complex, difficult to use, inflexible, and do not adequately support changing business needs such as electronic filing and data

Washington has repeatedly won national awards for its leadership in e-government and public sector use of technology; if it is dissatisfied with the current level of JIS integration and data exchange within and between courts, justice and public safety agencies, social services, and treatment providers, then this suggests an endemic problem among courts across the nation.

Nor are the reasons for this state of affairs difficult to discern. The obstacles to successfully creating a statewide judicial information system that can share and exchange data with all the constituencies that a court serves are significant. To begin with, each state must develop its own judicial information system. A state cannot simply borrow a judicial information system developed by another state because each state's governmental structure, as well as the set of legal, political, institutional, and technical requirements that a judicial information system must satisfy, are unique.[24] Nor should one underestimate the complexity of planning for such a technology project. Justice system integration requires significant levels of coordination across legislative, executive, and judicial branch agency lines, as well as across federal, state, and local jurisdictional boundaries.[25]

Another obstacle arises from the manner in which most state courts govern themselves. Unlike the hierarchical structures found in executive branch agencies and private corporations, the governance structure of state courts is typically more fragmentary and diffuse. As a result, for a new initiative or project to succeed, individual judges must step forward and assume the mantle of leadership. With rising caseloads and the other obligations that accompany elevation to the bench, judges have scant time to take responsibility and ownership of complicated, multi-year technology projects. Moreover, even if judges and other court personnel were willing to spearhead the development of an integrated, statewide judicial information system, in a time of tight state budgets the funding for such an expensive undertaking would be at best precarious. Even in

---

exchange." JUDICIAL INFO. SYS. COMM., WASH. STATE OFFICE OF THE ADM'R FOR THE COURTS, MOVING THE JUDICIAL INFORMATION SYSTEM TO THE WEB, A JIS MIGRATION PLAN: POLICY EDITION 1 (2001), *available at* http://www.courts.wa.gov/jis/policy.pdf. As such, legacy applications "inadequately support future statewide information sharing plans." *Id.*

24. As the National Task Force on Court Automation and Integration has recognized, "[s]tates are frequently dissimilar in the structure of the judicial branches and jurisdictions assigned to their courts, which makes it difficult to develop transferable automation solutions and create national data standards that are relevant from state to state." NAT'L TASK FORCE ON COURT AUTOMATION & INTEGRATION, *supra* note 4, at 7.

25. *Id.* at 37.

states that can afford such an initiative, court funding is usually a relatively low priority, and courts are forced to compete with executive agencies and popular legislative programs for the limited discretionary spending included in a state's annual budget. It is difficult to develop the necessary institutional commitment and expertise if continued funding for the project is considered uncertain.

Beyond these more general obstacles, individual courts and justice agencies may also resist JIS integration. Courts and agencies may believe that their individual resources are too limited to participate in such a large project. Some might believe that the complexity of the justice process is so great that any attempt to automate and integrate it is doomed to end in failure. Others may be hesitant to rely on other courts' and agencies' technical staff for mission-critical computing and information. Still others may fear a reduction in their ability to serve their core constituencies. Finally, over the years, courts and agencies have invested a great deal of time, money, and other resources in developing electronic information systems that successfully address their core operational processes and requirements. Although these systems employ outmoded technologies, have limited functionality, cannot be adapted to emerging information processing needs,[26] perpetuate islands of isolated data, and store information in data formats incompatible with other systems used by that court or agency, most courts and justice agencies are still comfortable with their systems. If these systems have limitations, they have developed work-a-rounds to compensate for them. The idea of having to reengineer their core business processes, or worse, to have another court or agency dictate to them how they must perform their core mission, is not a prospect most courts and justice agencies enthusiastically embrace.

To overcome these obstacles, the most promising strategy for developing an integrated justice information system is one that forswears any attempt to impose identical hardware and software solutions on the myriad courts and agencies to be integrated and focuses instead upon achieving interoperability and data exchange among the existing electronic information systems already in use. Interoperability and data

26. Such emerging information processing needs include the ability to handle new data formats, such as those required for storing digital mugshots, digital fingerprint records, and other images, to provide email notification to the parties of a case before the court, to include email as part of the case file, to permit the electronic filing of pleadings, motions, and other documents, to engage in the remote scheduling of court proceedings with parties, attorneys, law enforcement officers, and witnesses, and to provide public access to court documents over the Internet.

exchange, however, require standards—standards governing not only the communication of one computer system with another, but the translation of data from one format to another.[27] Standards governing interoperability, data exchange, and data integrity would permit the creation of an open data-sharing network using middleware applications and data-warehousing solutions, while at the same time leaving in place the existing information systems of the courts, justice and public safety agencies, social services, and treatment providers that have been tailored to meet their unique operational requirements and the needs of their different constituencies.

Given the importance of standards to open data-sharing networks and, *a fortiori*, to the development of integrated justice information systems, it is hardly surprising that there are currently underway a number of efforts to develop various standards governing interoperability and data exchange tailored to the unique needs of the courts and the greater justice community. Two of these efforts, in particular, warrant our attention: the Global Justice XML Data Model being developed by the Office of Justice Programs in the United States Department of Justice (DOJ) and the LegalXML project of the Organization for the Advancement of Structured Information Standards (OASIS). The Global Justice XML Data Model is intended to facilitate "increased interoperability among and between justice and public safety information systems" and is "a significant milestone in the process of developing appropriate standards for expressing the baseline data needs of the justice and public safety communities and their related partners."[28] The LegalXML project produces, *inter alia*, standards for electronic court filing, court documents, legal citations, transcripts, and criminal justice intelligence systems.[29] As the names of these two development

27. Despite "the significant efforts of government and industry to develop all manner of standards, additional standards governing technology, data integrity, and interoperability are still needed to help state and local agencies integrate." NAT'L TASK FORCE ON COURT AUTOMATION & INTEGRATION, *supra* note 4, at 40. Recognizing this need, the National Task Force on Court Automation and Integration has advised that "communications protocols—such as TCP/IP (Transmission Control Protocol/Internet Protocol), frame relay, Internet/intranet standards, and universal transaction format standards like XML (Extensible Markup Language) that allow users to design the system the way they like—should be researched to determine their applicability to the development of integrated information systems." *Id.* at 50.

28. Office of Justice Programs, United States Department of Justice, *Global Justice XML Data Model, Promoting Justice and Public Safety Information Sharing*, *at* http://it.ojp.gov/topic.jsp?topic_id=43 (last visited Sept. 7, 2003).

29. LegalXML, Organization for the Advancement of Structured Information Standards, *About LegalXML*, *at* http://www.legalxml.org/about/index.shtml (last visited Sept. 7, 2003).

efforts suggest, both the DOJ and OASIS have chosen XML as the language in which to develop their standards.

II. XML EXPLAINED

XML stands for Extensible Markup Language. Markup is information embedded in the text of a document that is not intended for printing or display.[30] Experts generally agree that there are three kinds of markup:[31] procedural, structural, and semantic. *Procedural* or *presentational markup* involves instructions for the display or printing of a document. It indicates "how" to render the text to which it is attached. The nonprintable codes embedded in a document to control the style or font of text by a word processing program are procedural markup—though such codes are more typically regarded as part of that word processing program's proprietary file format. *Structural* or *descriptive markup* is used to indicate the type of text to which it is attached: a title, a quotation, headings, paragraphs, etc. It answers the question: what is this? Finally, *semantic* or *content markup* is used to indicate the meaning of a particular fragment of text. In a driver's license, for example, semantic markup might indicate that a string of characters is the licensee's name or that a string of numbers is the licensee's birthday or identification number. In a trial transcript, semantic markup could be used to indicate when the speaker is the judge, a witness, or one of the attorneys, as well as whether the transcribed words are spoken in open court or at a sidebar. With the Global Justice XML Data Model and LegalXML projects, the DOJ and OASIS are both developing content markup for use by courts and other members of the justice and public safety communities.

Markup is associated with content and data using a markup language. A markup language is developed using a metamarkup language. The most powerful metamarkup language is Standard Generalized Markup Language (SGML).[32] HyperText Markup Language (HTML), best known as the markup language used to create web pages on the World Wide Web, is a particular application of SGML—SGML was used to create it. Although SGML has been an international standard since 1986,

30. The World Wide Web Consortium's XML home page is at http://www.w3.org/xml (last modified Aug. 20, 2003).

31. Sany Ressler, *Markup Languages*, *in* ENCYCLOPEDIA OF COMPUTER SCIENCE 1080, 1080 (Anthony Ralston et al. eds., 4th ed. 2000).

32. *Id.*

due to its complexity it cannot be used to develop more specialized markup language for use on the Web that addresses the needs of particular industries, professions, or other common interest communities. To develop specialized custom markup languages for use on the Web, a simpler metamarkup language was needed. Extensible Markup Language (XML), a subset of SGML, was developed to fill this need.[33]

SGML and XML, as well as the particular markup languages created with them, all use tags to mark up content. Marked up or tagged content within a document is called an element. In particular markup languages such as HTML and LegalXML, each type of element is given a name. While elements can be nested, they cannot overlap, and all the elements composing a document must be contained within a single *root* or *document* element. Accordingly, an element's content comprises either text or other elements. To make this a bit more concrete, consider the following simplified example[34] of an element in a LegalXML document containing semantic markup used to tag data about a court filing stored in a court information system:

```
<courtFiling>
    <actor id="petitioner.1">
        <name>
            <personName>
                <namePrefix>Ms.</namePrefix>
                <firstName>Mary</firstName>
                <lastName>Smith</lastName>
            </personName>
        </name>
        <personDescription>
            <sex>female</sex>
            <birthDate>1972-06-15</birthDate>
            <maritalStatus>single</maritalStatus>
        </personDescription>
    </actor>
    <filingInformation id="filing.1">
        <courtInformation>
```

33. The new Web markup language known as XHTML is an application of XML. *See infra* note 46 and accompanying text.

34. A more complex example on which this example is based may be found at http://www.ncsconline.org/D_Tech/Standards/Documents/CourtDocument11-rev1/CourtDocument11/samples/petition_for_protection_filing_CDATA.xml (last visited Jan. 9, 2004).

```
            <physicalLocation>
                <postalAddress type="work">
                    <addressLine>King County Courthouse</address
                    Line>
                    <addressLine>516 - 3rd Avenue</addressLine>
                    <city>Seattle</city>
                    <state codeValue="WA">Washington</state>
                    <postalCode>98104</postalCode>
                </postalAddress>
            </physicalLocation>
            <courtType>state</courtType>
            <courtName>King County Superior Court</courtName>
        </courtInformation>
        <caseInformation newCase="true">
            <caseTitle>Smith v. Jones</caseTitle>
            <caseCategory>domestic</caseCategory>
            <caseYear>2001</caseYear>
            <filersCaseNumber>01-2-13059-5
            SEA</filersCaseNumber>
        </caseInformation>
    </filingInformation>
    <leadDocument id="doc001.01-2-13059-5-SEA/">
</courtFiling>
```

As this example shows, markup tags in markup languages created using XML begin with an opening angle bracket <, end with a closing angle bracket >, and include the name of the type of element of which they form a part. There are three kinds of markup tags in a markup language created using XML: start tags, end tags, and empty tags.[35] Start tags are formed by placing angle brackets around the name of an element: <ElementName>. They indicate the beginning of an element of the kind named. End tags are formed from start tags by inserting a backward slash / between the opening angle bracket < and the element name for that tag: </ElementName>. An end tag indicates the end of the element whose beginning is indicated with the corresponding start tag. As the foregoing suggests, start and end tags form pairs, and in markup languages created using XML, one cannot place a start tag in a document without also using its corresponding end tag. A simple

35. SIMON ST. LAURENT, XML, A PRIMER 38 (3d ed. 2001).

example of marked up text conforming to these rules is: <ElementName>ElementContent</ElementName>.

In the simplified LegalXML example, the root element is called *courtFiling*. The root element envelops all the other elements of this example and extends from the start tag <courtFiling> to the end tag </courtFiling>. More specifically, the *courtFiling* element contains three elements: *actor*, *filingInformation*, and *leadDocument*. The *actor* element has nested within it the *name* and *personDescription* elements, which in turn contain structured information—another term for marked up content—about the filer's first name, last name, sex, birth date, and marital status. The *filingInformation* element has nested within it the *courtInformation* and *caseInformation* elements, which in turn contain structured information about the physical location, type, and name of the court, as well as about the category, case number, year, and title of the case in which the document was filed. Note that although many elements are nested in others, no elements overlap: if an element's start tag occurs between a pair of tags forming another element, then its end tag also occurs between that pair.

Unlike the *name* and *filingInformation* elements, the *leadDocument* element is an empty element. An empty element is used to place markup that contains neither text nor other elements. In our example, an empty element is used to represent the document filed because the actual document filed is not included in the structured information—the marked up content—actually presented. Empty elements may be represented using start tags that have a backward slash / inserted between the closing angle bracket > and the element name: <ElementName/>.[36] In our example, the actual document filed is associated with the empty tag <leadDocument/> by assigning it a unique document ID and placing that ID number in the tag as an attribute.

Attributes permit additional information concerning elements to be included in tags. Only start and empty tags may include attributes. Among other things, attributes enable the markup author to give each element in a document a unique identifier, to associate URLs with text or images in order to create hyperlinks, as well as to insert application-specific instructions for processing the structured information and data.

36. At the option of the markup's author, a space may be inserted between the element name and the backward slash: <ElementName />.

In our example, the *leadDocument* element included the attribute: id="doc001.01-2-13059-5-SEA".[37]

As you can see, attributes are formed by concatenating an attribute's name to an equal sign followed by the attribute's value—the information that the attribute is intended to convey—within quotation marks.[38] They are inserted into markup tags between the element name and the closing angle bracket: <ElementName AttributeName="AttributeValue">.[39] In the simplified LegalXML example above, the *actor*, *postalAddress*, and *caseInformation* elements, among others, also contained attributes.

The first and current version of XML developed by the XML Working Group is referred to as XML Specification 1.0 (XML 1.0).[40] This specification comprises the syntax for creating well-formed XML documents as well as the rules for creating new markup tags.[41] Using XML 1.0 as a metamarkup language, one can create markup languages such as LegalXML that not only facilitate data exchange by specifying the meaning or significance of industry-specific data, but also specify "the structure of that data and how various elements are integrated into other elements."[42] The definition of new markup tags as well as the rules and constraints governing their use are expressed in machine-readable documents called Document Type Definitions (DTDs) and XML schemas.[43] The DOJ's Global Justice XML Data Model project, for example, employs XML schemas to define the approximately 2000 unique data elements included in its XML standard for use by the justice

37. Attributes are also used in HTML. For example, to create a hyperlink in a document using HTML, one must not only use a pair of anchor tags to surround the specific text, which when clicked will trigger the web browser to jump to another location on the Internet, but one must also include the URL of the target location. This additional information is conveyed using the Hypertext REFerence attribute, HREF: <A HREF="http://www.targetLocation.com">Hyperlink Text</A>.

38. ST. LAURENT, *supra* note 35, at 46.

39. *Id.*

40. World Wide Web Consortium (W3C), *Extensible Markup Language (XML) 1.0 (Second Edition)*, *at* http://www.w3.org/TR/REC-xml (last visited Sept. 11, 2003).

41. *Id.*

42. STEVEN HOLZNER, REAL WORLD XML 11 (2003).

43. While XML schemas can be used instead of DTDs to govern the use of customized markup tags, they are the subject of a separate W3C specification. *See* World Wide Web Consortium, *XML Schema Part 1: Structures*, *at* http://www.w3.org/TR/xmlschema-1/ (last visited Sept. 11, 2003). The central difference between a DTD and XML schema is that an XML schema is itself an XML document, while a DTD is not. Moreover, XML schemas are more powerful and precise than DTDs. For example, XML schemas allow for data typing, but DTDs do not. For these reasons, XML developers generally prefer using XML schemas to DTDs when defining new markup tags.

and public safety communities.[44] OASIS' LegalXML project, by contrast, used a DTD for its Electronic Court Filing 1.1 Proposed Standard.[45]

An XML standard, such as those being developed in the Global Justice XML Data Model and LegalXML projects, is simply an application of XML that includes various markup tags, Document Type Definitions, or XML schemas tailored to the needs of a particular industry or user community. XML 1.0 is used to develop XML standards. For example, the World Wide Web Consortium (W3C) used XML 1.0 to develop XHTML 1.0, an XML application intended to replace HTML for use on the Web. XHTML 1.0 contains all of the markup tags of HTML as well as a DTD defining the structure of a valid Web page, i.e., HTML document.[46] XML 1.0 has also been used to develop standards for use in banking, finance, telecommunications, education, and myriad kinds of businesses.[47] Documents that comply with XML standards are well-suited for use over the Internet, easily understood by humans, and machine-readable. It is hardly surprising, therefore, that the DOJ and OASIS both chose XML to develop standards for use by the courts, justice and public safety agencies, social services, and treatment providers that form the justice and public safety communities.

As the framework and metalanguage within which standards are developed, XML "is the 'glue' that promotes interoperability—it allows systems already in use and those being developed to communicate with each other and paves the way for future expanded collaboration between agencies."[48] Data structured using XML markup is not tethered to particular vendors, original equipment manufacturers (OEMs), operating systems, applications, communication protocols, or storage media and "can be shared between different systems, up and down the levels of

---

44. Office of Justice Programs, United States Department of Justice, *supra* note 28. The XML schema for the prerelease version 3.0.0.1 of its Justice XML Data Dictionary is available at http://it.ojp.gov/jxdd/prerelease/3.0.0.1/jxdds.xsd (last visited Sept. 12, 2003).

45. The Electronic Court Filing Technical Committee, LegalXML Member Section, Organization for the Advancement of Structured Information Standards, *Electronic Court Filing 1.1 Proposed Standard* 1 (July 22, 2002), *at* http://www.oasis-open.org/committees/legalxml-courtfiling/documents/22072002cf1-1.pdf.

46. FRANK BOUMPHREY ET AL., BEGINNING XHTML 33–39 (2000).

47. HOLZNER, *supra* note 42, at 10.

48. Office of Justice Programs, United States Department of Justice, *Extensible Markup Language (XML) and Its Role in Supporting the Justice Data Model*, *at* http://it.ojp.gov/documents/whatisXML.doc (last visited Sept. 10, 2003).

agencies, across the nation, and around the world, with the ease of using the Internet."[49]

XML promotes interoperability by enabling the creation of XML standards tailored to the needs of different industries and user communities. In particular, XML standards tailored to the operational requirements of the courts and other members of the justice and public safety communities promote interoperability by defining elements that can express the types of data used by courts and other members of the justice and public safety communities as structured information. Using such elements, not only can data from any justice information system be re-expressed as structured information, but structured information conforming to the standard can be translated into the data format of any justice information system. As a result, XML can be used to create applications and standards that bridge the information chasm separating any justice information systems using incompatible data formats. One need only translate the data from one justice information system into a document conforming to an appropriate XML standard and then translate that document into the data format of the other justice information system. Since any type of data or information covered by an XML standard can be translated from or to structured information conforming to that standard, such structured information forms a bridge between any two justice information systems.[50] In this fashion, data and messages can be moved from one justice information system to any other with XML markup acting as a *lingua franca* or intermediate link between different and incompatible justice information systems.

By using XML to develop XML standards tailored to the operational requirements of the courts and other members of the justice and public safety communities, interoperability and data exchange among disparate and incompatible information systems can be achieved and the obstacles to an integrated justice information system surmounted. In light of the

---

49. *Id.*; *see also* Paul S. Embley & Matthew Snyder, *XML in Justice Information Sharing: An Executive Summary*, THE POLICE CHIEF, Dec. 2002, at 1, *available at* http://www.iacptechnology.org/Library/TechTalk/TechTalk1202.pdf.

50. This process is generally automated using software running on application servers connected to the communicating justice information systems. The justice information system sending data passes the data in its native data format to an application server that translates that data into XML elements defined by the appropriate XML standard. This application server then transmits the resulting XML elements to another application server that translates this structured information into the data format of the target justice information system. The reformatted data is then passed to the target information system. When required, the target information system can respond to the sending justice information system by reversing this process.

extensive benefits arising from the integration of justice information systems, it is inevitable that the courts and other members of the justice and public safety communities will migrate to case management information systems that can output XML structured data and information either directly or through a middle tier application server.

III. DOCUMENTS DISSOLVED: FROM MANILA FOLDERS TO STRUCTURED INFORMATION

At least since the construction of permanent courthouses, individuals—attorneys in particular—have generally conveyed information to the courts in the form of paper documents: petitions, bills, complaints, answers, motions, memoranda, affidavits, attachments, transcripts, requests for findings of fact and conclusions of law, informations, indictments, notices of appeal, and briefs. Courts too have typically responded with paper documents: written opinions, judgments, decrees, findings, minutes, injunctions, writs of mandamus and prohibition, as well as other kinds of orders. Indeed, some judges have created documents within documents by inscribing their rulings—granted or denied—as marginalia on motions submitted by the parties. In most courthouses, these paper documents are sorted by case, collected together in manila folders and expanding Pendaflex® or Oxford® file pockets, and stored in a filing room that provides ready access to court clerks and their assistants.

While at one time unavoidable, operating a court system in which paper documents mediate the exchange of information among judges, court personnel, litigants, attorneys, witnesses, the press, and the interested public is highly inefficient. Among the many costs incurred by parties, their attorneys, court personnel, and the quality of justice generally, we may highlight just a few. To begin with, filing a paper document with a court requires that one travel to the courthouse during court business hours, hand the document to a clerk, and receive a paper time-stamped receipt. Not only does this process increase the cost of access to the justice system, but when performed by an attorney, it prevents a more productive use of his or her time. Once filed with the court, court personnel must update the docket and physically file the document in the filing room. This not only lessens the productivity of court personnel but also creates the opportunity for data entry and filing errors. When needed again, paper documents are cumbersome, difficult to retrieve quickly, and require the user's physical presence at the courthouse. Moreover, only one person can read a paper document at a

time. This limitation leads to restricted access when judges and judicial clerks are working with case files as well as costly copying. Additionally, when paper documents and case files are moved among different users, they are not infrequently lost, disassembled, or misfiled—reducing access still more. Paper documents are also notoriously difficult to keep up-to-date. As a result, judges, court personnel, attorneys, the press, or the public may find themselves inadvertently relying on a document containing outdated information. In light of these difficulties and disadvantages, it is hardly surprising that as information and communication technologies have evolved, virtually everyone connected with the justice system has embraced the search for an electronic alternative to paper documents.

Within the federal courts, the search for an electronic alternative to paper documents may be dated from the 1991 amendment of Rule 25 of the Federal Rules of Appellate Procedure to permit electronic filing. As amended, Rule 25 provides that

> [a] court of appeals may by local rule permit papers to be filed, signed, or verified by electronic means that are consistent with technical standards, if any, that the Judicial Conference of the United States establishes. A paper filed by electronic means in compliance with a local rule constitutes a written paper for the purpose of applying these rules.[51]

Five years later, similar changes were made to the Federal Rules of Civil Procedure[52] and the Federal Rules of Bankruptcy Procedure.[53] The Federal Rules of Criminal Procedure state simply that "[a] paper must be filed in a manner provided for in a civil action"—thereby allowing electronic filing by incorporation.[54] Since 2001, the Federal Rules of Civil Procedure also permit service by electronic means.[55] The Federal Rules of Appellate Procedure followed suit in 2002.[56] Significantly, both also permit service by electronic means using the court's own transmission equipment.[57] Thus, in only twelve years, the federal judiciary has gone from permitting U.S. courts of appeals to accept

51. FED. R. APP. P. 25(a)(2)(D).

52. FED. R. CIV. P. 5(e).

53. FED. R. BANKR. P. 5005(a)(2).

54. FED. R. CRIM. P. 49(d).

55. FED. R. CIV. P. 5(b)(2)(D), 5(b)(3).

56. FED. R. APP. P. 25(c)(1)(D).

57. *See* FED. R. CIV. P. 5(b)(2)(D); FED. R. APP. P. 25(c)(2).

electronic filings to allowing U.S. district and circuit courts not only to accept service made by electronic means but to facilitate such service using its own equipment.

Just as the rules authorizing electronic filing have evolved from the early 1990s to the present, so has the technology. In its earliest implementation, electronic filing meant "filing by fax." A paper document was inserted into a fax machine at one end, an electronic signal was transmitted over the telephone lines to the courthouse fax machine, and a paper document came out at the other end. The court clerk then filed the faxed document as he or she would any other paper document. In 1995, commercial traffic was permitted onto the Internet and soon thereafter "filing by fax" was replaced by "filing by email attachment." Lawyers could now simply attach their WordPerfect, Microsoft Word, or Adobe Portable Document Format (PDF) documents to an email addressed to the court clerk and with the click of a button the filing would be at the courthouse. At first, court personnel printed the documents received via email and then processed them as they would any paper document. As courts reengineer their work flow to benefit from the lower costs of electronic storage, however, many courts are now storing all their documents in electronic form—scanning the paper documents that they receive and converting them to TIFF image or Adobe PDF files.

The benefits and savings that result from electronic filing have been recognized for a long time. In 1997, the Administrative Office of the United States Courts created a comprehensive catalog of benefits provided by electronic filing that included the following: immediate access to court documents in the courtroom; simultaneous access to the same document by many individuals; twenty-four-hour access to court documents inside and outside the courthouse; reduced file-handling and maintenance; reduced staff time for tasks such as pulling and reshelving files and making copies for the public; simplified archiving and file retrieval; easy and quick transfer of case files among courts, chambers, and other court units; elimination of misfiled papers; reduced time for dictation and retyping as portions of one document can be easily transferred to another using the cut-and-paste operation of word processing software; reduced need for physical space in the courthouse to store documents; elimination of the need for archival storage using microfilm; reduced data entry errors through automated docketing of electronically filed documents; reduced need to assist with public access to documents; reduced need for filing duplicate paper copies of

documents by attorneys as well as for the handling of such copies by court personnel; greater file integrity and security using validity checks; remote viewing of court documents over the courthouse network or Internet; enhanced ability to share, annotate, and edit documents through email; and the ability to perform full text searches within individual documents and across an entire file system.[58] In light of the substantial advantages and savings provided by electronic filing, it is hardly surprising that both federal and state courts are embracing electronic filing through pilot programs and permanent implementations.

From a systems integration perspective, electronic filing also permits a court's document management system to be integrated with its case management system. Integrating these two systems, for example, allows a user viewing an electronic docket to access and read a particular document by clicking on that document's title.[59] Moreover, just as XML can be used to integrate case management information systems across courts and other justice and public safety agencies, XML can also be used to facilitate interoperability and data exchange among integrated case management and electronic case file systems. Using an appropriate XML standard, an electronic document is merely another form of content to be marked up using tags. For example, using a pair of *documentContent* tags, one could simply insert an Adobe PDF or Microsoft Word document as an element in a LegalXML message being transmitted to another information system.

More significantly still, one may use tags defined using an appropriate XML standard to mark up different kinds of information in electronic documents filed with the courts. Tagging key pieces of information in court documents would permit court information systems to read, understand, and manipulate this information without human intervention. For example, if the plaintiffs' names, the names of their attorneys, and their attorneys' phone numbers were all tagged using LegalXML in electronic court documents containing this information, then software could be developed that could create—automatically or on

58. ADMIN. OFFICE OF THE U. S. COURTS, ELECTRONIC CASE FILES IN THE FEDERAL COURTS: A PRELIMINARY EXAMINATION OF GOALS, ISSUES, AND THE ROAD AHEAD [DISCUSSION DRAFT] 15–17 (1997), *available at* http://www.uscourts.gov/casefiles/ecfmar97.pdf.

59. The U.S. District Court for the Southern District of New York is in the process of implementing an integrated case management/electronic case file (CM/ECF) system and has posted on the Web an online tutorial for a CM/ECF system that includes an electronic docket linked to electronic case files. *See* United States District Courts, *Electronic Case Filing: A Tutorial for Attorneys and Law Firm Staff, at* http://www.nysd.uscourts.gov/cmecf/training/ecf100/index.html (last visited Jan. 2, 2004).

request—a list of the plaintiffs' attorneys and their phone numbers for any case. Even more importantly, software could be developed that creates copies of court documents with certain tagged categories of information redacted. Sensitive personally identifying information, for example, could be removed from court documents when accessed by the public. Recognizing the need for authors to create electronic documents that include XML markup, upcoming releases of both Microsoft Word and Adobe Acrobat—the application used to create Adobe PDF documents—will include support for XML.[60]

With the development of XML standards, documents are becoming anachronistic. By tagging all the information contained in a court document, it is possible to dispense with documents altogether—through dissolving them into structured information. After all, a document is only a particular view of the information that it contains. Rather than being restricted to one particular view of that data, using structured information one could select or create a view of the data optimized for the task to which that data is relevant. Imagine, for example, being able to display simultaneously the conflicting factual claims contained in a plaintiff's complaint and a defendant's answer, or an argument and its critique culled from one side's memorandum in support of a motion and the other side's memorandum in opposition. Such tailored views of case data as well as traditional documentary views could easily be created if we filed structured information with the courts rather than documents—electronic or paper.[61] Admittedly, however, judicial information systems for filing structured information are still somewhat in the future.

IV. THE QUESTION OF PUBLIC ACCESS TO COURT RECORDS OVER THE INTERNET

Already in some jurisdictions—and soon in most—courts are integrating their case management information system with an electronic docket and document management system. Using XML standards tailored to the operational requirements of the courts and other members

60. *See* Yardena Arar, *Microsoft Unveils Office 2003 Beta 2* (Mar. 10, 2003), *at* http://www.pcworld.com/news/article/0,aid,109656,00.asp; *The Adobe XML Architecture: The Making of an Intelligent Document*, *at* http://www.adobe.com/enterprise/xml.html (last visited Jan. 2, 2004).

61. Different views of XML tagged data are created using Cascading Style Sheets (CSS) or Extensible Style Language (XSL). Using Extensible Style Language: Transformations (XSLT), one can even create and save documents in particular formats—such as Adobe PDF or Microsoft Word—out of structured information.

of the justice and public safety communities, these integrated information systems are able to interoperate and exchange data with the information systems of other courts, justice and law enforcement agencies, social services, and treatment providers. Incompatible data formats, communications protocols, and application programming interfaces are obstacles surmounted. Truly integrated justice information systems at the state, regional, and national levels are within reach. Also within reach is public access to court records on a scale and with an ease never before imagined.

Just as XML permits the myriad, incompatible information systems of the courts and other members of the justice and public safety communities to interoperate and exchange data, this same technology enables court information systems to interoperate and exchange data with personal computers connected to the Internet. As a result, it is now technically possible to permit members of the public to access court data and case files from the privacy and comfort of their own home or office, in real time, twenty-four hours a day, seven days a week. Moreover, to the extent that courts are already modifying existing information systems or designing new ones to output structured information and electronic documents as XML messages, this access can be granted to the public without any additional development costs.

Recognizing that it is now technically possible to provide public access to court records over the Internet leads inexorably to the question whether the courts ought to provide such access and, if so, to what extent. At least three answers to this question are possible. One might believe that providing public access to case files over the Internet would do too great a harm to the privacy of litigants and others discussed in court documents and, therefore, conclude that the public ought not to be permitted access to court documents over the Internet. By contrast, one might observe how public access to the courts has been an enduring and fundamental value in our society[62] and conclude that the public should be able to access court files and documents over the Internet to the same extent that they can access them in the courthouse—that courts should not discriminate with respect to methods of access. Finally, one might

62. *See* Press-Enter. Co. v. Superior Court, 478 U.S. 1 (1986) (granting access to criminal preliminary hearing); Press-Enter. Co. v. Superior Court, 464 U.S. 501 (1984) (allowing access to criminal jury voir dire); Globe Newspaper Co. v. Superior Court, 457 U.S. 596 (1982) (granting access to criminal trial); Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) (granting public access to criminal trial); Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978) (recognizing a general right to inspect and copy judicial records and documents).

balance the importance of public access to the courts against the privacy interests of individual litigants and conclude that while the public should have some access to court files and documents over the Internet, it should be more limited than the access to case files provided in the courthouse.

Of these three positions, I embrace the second: I do not believe that courts should discriminate with respect to methods of access. For the reasons explained in Parts V and VI, especially as courts migrate to XML-based justice information systems, I do not believe that limiting public access to court documents over the Internet is necessary to protect the legitimate privacy interests of litigants or others before the court. To the extent that information should be withheld from the public because of legitimate concerns about public safety or privacy, such information should be inaccessible to the public at the courthouse as well.

An alternative position has been taken by the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA). Endorsing the position that public access to court records over the Internet ought to be more limited than public access to these records in the courthouse, the CCJ and COSCA have published a set of model guidelines for granting public access to court records (CCJ/COSCA Guidelines or Guidelines).[63] The CCJ/COSCA Guidelines include definitions of both "public access" and "court record."[64] Under the Guidelines, public access "means that the public may inspect and obtain a copy of the information in a court record,"[65] while a court record is defined to include "[a]ny document, information, or other thing that is collected, received, or maintained by a court or clerk of court in connection with a judicial proceeding" as well as "[a]ny index, calendar, docket, register of actions, official record of the proceedings, order, decree, judgment, minute, and any information in a case management system created by or prepared by the court or clerk of court that is related to a judicial proceeding."[66]

---

63. MARTHA WADE STEKETEE & ALAN CARLSON, NAT'L CTR. FOR STATE COURTS & THE JUSTICE MGMT. INST., DEVELOPING CCJ/COSCA GUIDELINES FOR PUBLIC ACCESS TO COURT RECORDS: A NATIONAL PROJECT TO ASSIST STATE COURTS (2002), *available at* http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf.

64. *Id.* at 12 (CCJ/COSCA Guideline § 3.10—Definition of Court Record), 17 (CCJ/COSCA Guideline § 3.20—Definition of Public Access).

65. *Id.* at 17 (CCJ/COSCA Guideline § 3.20—Definition of Public Access).

66. *Id.* at 12 (CCJ/COSCA Guideline § 3.10—Definition of Court Record). Currently, disagreement exists within the justice community over whether administrative records of a court should be included within the definition of a court record. The Guidelines have sidestepped this

Under the Guidelines' general access rule, information in court records should be accessible to the public unless its release is prohibited by federal or state law or the court record is sealed by the court.[67] This general access rule applies to all court records—both paper and electronic.[68] The degree of access recommended by the Guidelines, however, varies with the method of access used. The Guidelines distinguish courthouse access from remote access. Remote access is defined as "the ability to electronically search, inspect, or copy information in a court record without the need to physically visit the court facility where the record is maintained" and, therefore, would include access to court records over the Internet.[69] Significantly, the Guidelines do not recommend that the degree of access provided remotely be as extensive as the degree of access provided at the courthouse. In particular, while public access to case files and documents must be provided at the courthouse, remote access to case files and documents is not recommended.[70] Remote access is presumed only for: litigant indexes filed with the court; listings of new case filings, including the names of the parties; registers of actions showing what documents have been filed in a case; calendars or dockets of court proceedings; judgments, orders, or decrees; and liens affecting real property.[71] Explaining its decision to recommend limiting the public's remote access to this type of information, the commentary to the Guidelines notes that "[t]he summary or general nature of the information is such that there is little risk of harm to an individual or unwarranted invasion of privacy or proprietary business interests."[72]

In contrast to the CCJ and the COSCA, and more closely aligned to my own view, the Judicial Conference of the United States Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files (Committee) has taken the position with regard to civil case files that with one exception, the courts should not discriminate among modes of access: "the federal courts recognize that

---

controversy by allowing but not requiring the definition of court record to include administrative records and information. *See id.* (CCJ/COSCA Guideline § 3.10(a)(3)).

67. *Id.* at 23, 45, 53 (CCJ/COSCA Guidelines §§ 4.00, 4.60, 4.70(a)).

68. *Id.* at 22 (CCJ/COSCA Guideline § 4.00—Applicability of Rule).

69. *Id.* at 19 (CCJ/COSCA Guideline § 3.30—Definition of Remote Access).

70. *See id.* at 27 (CCJ/COSCA Guideline § 4.20—Court Records in Electronic Form Presumptively Subject to Remote Access by the Public).

71. *Id.*

72. *Id.*

the public should share in the benefits of information technology, including more efficient access to court case files."[73] Accordingly, while the Committee recognizes that "[a]s a practical matter, during this time of transition when courts are implementing new practices, there may be disparity in access among courts because of varying technology," it emphasizes that with one exception, the degree of access provided over the Internet should be the same as the degree of access provided at the courthouse:

> documents in civil case files should be made available electronically to the same extent that they are available at the courthouse with one exception (Social Security cases should be excluded from electronic access) and one change in policy (the requirement that certain 'personal data identifiers' be modified or partially redacted by the litigants).[74]

Similar recommendations for electronic access are made with respect to bankruptcy and appellate case files.[75] Only with regard to criminal case files does the Committee recommend restricting public access over the Internet.[76] Even in civil cases, however, the Committee recognizes that "[c]ertain types of cases, categories of information, and specific documents may require special protection from unlimited public access."[77] Thus, its recommendation contemplates that certain personal

---

73. JUDICIAL CONFERENCE COMM. ON COURT ADMIN. & CASE MGMT., REPORT OF THE JUDICIAL CONFERENCE COMMITEE ON COURT ADMINISTRATION AND CASE MANAGEMENT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES (2001), *available at* http://www.privacy.uscourts.gov/Policy.htm. It should be noted that the Committee defines case files more narrowly than the CCJ/COSCA Guidelines. Under the Committee's definition,

> [t]he term "case file" (whether electronic or paper) means the collection of documents officially filed by the litigants or the court in the context of litigation, the docket entries that catalog such filings, and transcripts of judicial proceedings. The case file generally does not include several other types of information, including non-filed discovery material, trial exhibits that have not been admitted into evidence, drafts or notes by judges or court staff, and various documents that are sometimes known as "left-side" file material.

Id.

74. *Id.*

75. *Id.*

76. *Id.* The Committee recommended that "public remote electronic access to documents in criminal cases should not be available at this time [September 2001], with the understanding that the policy will be reexamined within two years of adoption by the Judicial Conference." *Id.* It subsequently amended this recommendation on criminal cases to allow two exceptions: one for high profile criminal cases, and the other for pilot programs granting online access to documents in criminal case files. *See* JUDICIAL CONFERENCE COMM. ON COURT ADMIN. & CASE MGMT., LIMITED EXCEPTIONS TO JUDICIAL CONFERENCE PRIVACY POLICY FOR CRIMINAL CASE FILES (2002), *available at* http://www.privacy.uscourts.gov/amend.htm.

77. JUDICIAL CONFERENCE COMM. ON COURT ADMIN. & CASE MGMT., *supra* note 73.

data identifiers—Social Security numbers, dates of birth, financial account numbers, and names of minor children—"will not be included in its full and complete form in case documents, whether electronic or hard copy."[78]

In the E-Government Act of 2002, the United States Congress also endorsed public access to court documents over the Internet.[79] Section 205(a) of the E-Government Act requires that the United States Supreme Court as well as all federal circuit, district, and bankruptcy courts establish and maintain a website that provides, *inter alia*, "access to documents filed with the courthouse in electronic form, to the extent provided under subsection (c)."[80] Subsection (c) requires all electronic documents that are publicly available at a federal courthouse to be made publicly available online as well.[81] It also requires the U.S. Supreme Court to promulgate uniform rules to protect privacy and security concerns relating to electronically filed documents and their public availability under this section.[82] "To the extent that such rules provide for the redaction of certain categories of information," subsection (c) permits a party to file an unredacted copy of the document under seal, which a court may, in its discretion, accept in lieu of or in addition to a redacted copy in the public file.[83] Although the federal courts might question Congress' constitutional authority to prescribe the manner in which the federal courts must provide public access to case files and documents, it is clear that to the extent feasible and with few exceptions, both the federal courts and Congress are committed to making electronic documents publicly available online to the same extent that they are publicly available at the courthouse.

I wholly endorse this policy's general commitment to the even-handed treatment of paper and electronic documents. Unlike the Committee, however, as explained in Parts V and VI, I believe that the same even-handed treatment of case files and documents can be

78. *Id.*

79. E-Government Act of 2002, Pub. L. No. 107-347, § 205, 116 Stat. 2899, 2913.

80. *Id.* § 205(a). This section also requires that the website provide access to docket information and, to the extent feasible, "to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket sheet of that case." *Id.* § 205(d).

81. *Id.* § 205(c)(1). Electronic documents include electronically filed documents as well as paper documents filed with the court of which the court has created an electronic version by scanning or other means.

82. *Id.* § 205(c)(3)(A)(i).

83. *Id.* § 205(c)(3)(A)(iv).

extended to criminal and Social Security cases while respecting the legitimate public safety and privacy interests of litigants and others involved in those cases.

At the present time, the apparent trend among state courts is to follow the recommendations of the CCJ/COSCA Guidelines rather than the policies of the United States Congress and the Committee. For example, in Massachusetts, the Supreme Judicial Court has "concluded, at least initially, that an intermediate level of access to court information is appropriate on the Web, one that provides less information than is available at a courthouse."[84] Accordingly, its policy governing public access to court records over the Internet "does not allow documents submitted to a court in connection with a case to be published on a Court Web site."[85] Moreover, while its policy does permit public access over the Internet "to docket and calendar information that is or will be maintained in computerized case management systems," the Supreme Judicial Court has emphasized that "the law does not require courts to provide electronic access to court case information" and expressly prohibits publishing any criminal case information on the Web that "would identify a specific criminal defendant by name."[86] The Supreme Judicial Court has explained that it adopted this policy of limited public access over the Internet to address "concerns about the substantial intrusions into privacy interests that could accompany publication of personal information on a Court Web site."[87]

Another state that appears to be following the CCJ/COSCA Guidelines is California. Rule 2073 of the 2003 California Rules of Court governing public access to trial court records requires that "[a] court that maintains . . . records in electronic form must provide electronic access to them at the courthouse, to the extent it is feasible to do so, but may provide remote electronic access only to the records governed by (b)(1)," where the records governed by subsection (b)(1) include *only* the "[r]egister of actions (as defined in Gov. Code, § 69845), calendars, and indexes."[88] Remote access to all other case records, including all documents filed in the case, is prohibited. Again

84. Supreme Judicial Court, *Policy Statement by the Justices of the Supreme Judicial Court Concerning Publication of Court Case Information on the Web* 1 (May 2003), *at* http://www.state.ma.us/courts/web-pubpolicy.pdf.

85. *Id.*

86. *Id.* at 1–2.

87. *Id.* at 1.

88. CAL. CT. R. 2073(b)(1), (c) (2003).

the principal motivation for restricting the court records to which the public may have remote access appears to be a concern over privacy: "[t]he rules in this chapter are intended to provide the public with reasonable access to trial court records that are maintained in electronic form, while protecting privacy interests."[89]

In contrast to many state courts, the federal courts are phasing in a new case management/electronic case files (CM/ECF) system that implements the recommendations of the Committee. This system not only permits "litigants to file and access documents electronically via the Internet, 24 hours a day and 7 days a week," but also provides public access to these electronic case files by the same means.[90] The United States District Court for the Southern District of New York, for example, has developed an extensive website to support its own implementation of this system that includes a publicly accessible online tutorial for attorneys and law firm staff.[91] These systems are already being used in twenty-five district courts, sixty bankruptcy courts, the Court of International Trade, and the Court of Federal Claims. "Under current plans, the number of CM/ECF courts will increase steadily each month into 2005" with implementation for appellate courts scheduled to begin in late 2004.[92]

The foregoing suggests that the CCJ/COSCA Guidelines and the state court policies and rules that embody them restrict public access to the court records over the Internet due to a general sense of dread and anxiety over possible harms to the privacy interests of litigants and others who come before the courts. This anxiety over privacy, however, is completely misplaced. On the one hand, courthouse access provides no greater protection to privacy than access over the Internet. Any journalist can access information in case files at the courthouse and publish it on the front page of his or her newspaper. That most litigation is dull as dishwater is no response. Credit bureaus and other information aggregators will gladly mine the most boring case files for nuggets of

89. *Id.* 2070(a).

90. United States District Court for the Southern District of New York, *Southern District To Initiate Electronic Case Filing* 1 (Dec. 2, 2002) (press release), *at* http://www.nysd.uscourts.gov/newsroom/cmecf/pressrelecf.pdf.

91. The court's ECF website is available at http://www.nysd.uscourts.gov/cmecf/cmecfindex.htm (last visited Jan. 9, 2004), while the online tutorial may be found at http://www.nysd.uscourts.gov/cmecf/training/ecf100/ index.html (last visited Jan. 9, 2004).

92. Administrative Office of the United States Courts, *Case Management/Electronic Case Files (CM/ECF)* (Dec. 2003), *available at* http://www.uscourts.gov/cmecf/cmecf_about.html.

data and pass the cost on to their information consumers. Indeed, one of the reasons that the Committee decided against limiting public access to court records over the Internet was because it would simply foster a cottage industry of court data resellers—making the resellers rich, while depriving the public of access and leaving privacy unprotected.[93] On the other hand, as explained in Part V, providing access to court records and documents over the Internet, if done properly using XML-based justice information systems, can actually protect sensitive information better than restricting public access to paper case files in a courthouse.

At the present time, the CCJ/COSCA Guidelines—and the court policies and rules that implement them—deny the public access to court documents over the Internet because some documents may include sensitive information, while those same documents are made available in full for anyone to read at the courthouse. As a result, the public is denied easily accessible information that it should have, while it is given sensitive information that it should not. The problem is that the present information systems cannot distinguish between private and public forms of information within a document. However, as justice information systems are developed around structured information rather than generic documents and files, court information systems will be able to intelligently process different forms of information, preventing potentially harmful disclosures while simultaneously permitting the same degree of public access at the courthouse and over the Internet.

V. SEALING INFORMATION TO PROMOTE PUBLIC SAFETY AND PROTECT PERSONAL SECURITY

The most compelling reason for restricting public access to court records is not privacy but public safety—protecting the physical, psychological, and economic security of individuals. The information in court records and documents is not all benign, and our commitment to open judicial proceedings and public access to court records has involved certain costs arising from the misuse of this information. Public access to information in court records can facilitate blackmail, extortion, stalking, sexual assault, subornation of perjury, identity theft, and fraud—to name only a few of the crimes that can be facilitated through the misuse of information obtained from court records. Fortunately, as court information systems come online that can accept, process, and

93. JUDICIAL CONFERENCE COMM. ON COURT ADMIN. & CASE MGMT., *supra* note 73.

output XML tagged structured information, information likely to facilitate such crimes can be withheld from the general public, and these social costs obviated without in any way diminishing the benefits of unrestricted public access to court records and documents at the courthouse and over the Internet.

The kind of information most subject to misuse is personal information: information or data linked to or identified with a particular person. While any fact can be associated with a particular individual, certain categories of personal information render a person particularly vulnerable to malfeasance and harm: these include a person's address, telephone number, Social Security number, driver's license identification number, bank accounts, debit and credit card numbers, and personal identification numbers (PINs). One of the most publicized cases of harm facilitated by information culled from public records involved the actress Rebecca Schaeffer, the star of *My Sister Sam*, a popular television series during the 1980s. As Representative James P. Moran recounted on the floor of the House of Representatives, "[a]lthough she had an unlisted home number and address, Ms. Schaeffer was shot to death by an obsessed fan who obtained her name and address through the [California Department of Motor Vehicles (DMV)]."[94] Representative Moran also described how "[i]n Iowa, a gang of thieves copied down the license plate numbers of expensive cars they saw, found out the names and addresses of the owners [from the DMV] and robbed their homes at night."[95] On the floor of the Senate, Senator Barbara Boxer described an equally disturbing account of a thirty-one-year-old man in California who "copied down the license plate numbers of five women in their early twenties, obtained their home address from the DMV and then sent them threatening letters at home."[96] Senator Boxer read two of the letters into the Congressional Record. One read: "I'm lonely and so I thought of you. I'll give you one week to respond or I will come looking for you."[97] The other read: "I looked for you though all I knew about you was your license plate. Now I know more and yet nothing. I know you're a Libra, but I don't know what it's like to smell your hair while I'm kissing your neck and holding you in my arms."[98]

---

94. 140 CONG. REC. H2522 (1994) (statement of Rep. Moran).

95. *Id.*

96. 139 CONG. REC. S15,762 (1993) (statement of Sen. Boxer).

97. *Id.*

98. *Id.*

The information that facilitated these wrongful acts came from public records at state departments of motor vehicles and led to the passage of the Driver's Privacy Protection Act of 1994,[99] but the type of information used—an individual's name and address—might just as well have come from court records accessed at a local courthouse.

Identity theft is another example of wrongdoing that can be facilitated by information culled from court records. "An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft."[100] An identity thief may call a person's credit card issuer, change the billing address by impersonating that person and then run up charges on that account, or the identity thief may simply open a new credit card account in that person's name. In either case, when the charges remain unpaid, the delinquent account is reported on the victim's credit report. An identity thief may also open bank accounts in a victim's name and proceed to write bad checks. Telephone and wireless accounts as well have been established in victims' names. Identity thieves have also been known to purchase automobiles by taking out auto loans in the name of a victim. Some identity thieves have even filed for bankruptcy in the name of a victim to avoid eviction or to discharge debts that they incurred in a victim's name. Perhaps the most egregious form of identity theft occurs when an identity thief is arrested and gives a victim's name as his or her own: when the thief fails to appear on a scheduled court date, the arrest warrant is issued in the name of the victim. The Federal Trade Commission (FTC) estimates that in the United States over the last year alone losses from identity theft have approached fifty billion dollars.[101] The FTC also estimates that over the last year approximately ten million people in the United States discovered that they were victims of identity theft and that each victim spent on average five hundred dollars and thirty hours resolving the resulting problems.[102]

Personal information that facilitates these kinds of wrongs should not be accessible to the public either at the courthouse or over the Internet. It places an individual in jeopardy of physical, psychological, and economic harm without furthering any of the benefits of public access to

99. 18 U.S.C. §§ 2721–2725 (2000).

100. FED. TRADE COMM'N, ID THEFT, WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME 1 (2003), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf.

101. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 6 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

102. *Id.* at 7.

court records. The principal benefits promoted by public access to court records may be grouped into two categories: accountability and citizen education. With respect to the former, public access to court records makes the courts themselves directly accountable to the people. As Justice Oliver Wendell Holmes noted over one hundred years ago:

> [i]t is desirable that the trial of causes should take place under the public eye, not because the controversies of one citizen with another are of public concern, but because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed.[103]

Reviewing court records not only achieves this end and promotes public trust and confidence in the judiciary, but it also demonstrates to the public that the rule of law is being upheld and the law enforced. Moreover, insofar as government agencies, corporations, businesses, charities, politicians, and other individuals in whom a public trust has been invested come before our courts, public access to court records also keeps them accountable to the people. With respect to citizen education, public access to court records teaches the general public how the courts operate and informs them of the results of cases as well as the evidence that supports those results. By educating the public in this fashion, public access to court records promotes a set of stable and predictable rules by which we can govern ourselves and instructs members of the public with respect to people, circumstances, and business practices that might cause them harm.

Withholding sensitive personal information from the public when they access court records will neither undermine nor subvert any of these benefits. The adjudicatory facts upon which a court relies to dispose of a case or controversy according to the rule of law need never include the specific, arbitrarily assigned street address of a person's home, the precise series of numerals composing his or her telephone number, or the exact digits of his or her Social Security number. That a person has a Social Security number may be relevant to the just and rational disposition of a case, but the specific number will not be. That a person resides along a particular street or next to one of the parties may be relevant, but the exact house number will not be. Similarly, the general education that an individual might be expected to acquire from the

103. Cowley v. Pulsifer, 137 Mass. 392, 394 (1884).

perusal of court records does not include committing to memory the street addresses of fellow citizens, their Social Security numbers, or their bank accounts. Accordingly, such information should be omitted from publicly accessible court records and documents, irrespective of their form or the public's method of accessing them.

One must be careful, however, not to throw the baby out with the bath water. While personal information that renders an individual vulnerable to physical, psychological, and economic harm should not be released to the public, the information that surrounds personal information should be publicly accessible. Too often, information that would further accountability and citizen education is kept from the public because it cannot be effectively disentangled from personal information in documents or files that courts order sealed. While redacting the personal information contained in these documents and files is possible, it is quite costly, and many courts lack sufficient resources to do so on a regular basis.[104] As a result, the public is denied access to information that it should have. Thus, courts are caught between the horns of a dilemma: either they deny the public access to information it should have or grant it access to information that it should not.

To pass between the horns of this dilemma, some jurisdictions have adopted court rules that permit parties to omit sensitive personal information from publicly accessible documents filed with the court. When exercising this option, parties submit their personal information on confidential court forms that are not publicly accessible. General Rule 22(g) of the Washington State Court Rules, governing access to family court records, provides a good example. Subsection 22(g)(1) states, in relevant part, that "[i]nformation filed by a party in any file or record . . . shall be available to the public unless . . . access is restricted under section (c)(2)."[105] Subsection (c)(2) provides a list of forms for collecting personal information—such as a party's residence address, Social Security number, driver's license number, telephone number, Social Security number of a child or date of birth of a child—that the public is restricted from accessing.[106] An official comment to the rule

104. STEKETEE & CARLSON, *supra* note 63, at 18.

105. WASH. CT. GEN. R. 22(g)(1).

106. *Id.* 22(c)(2). Pursuant to General Rule 22(g)(3), "[a]ny person may file a motion, supported by an affidavit showing good cause, for access to any document otherwise restricted under section (c)(2)." *Id.* 22(g)(3). Moreover, pursuant to General Rule 22(g)(2), "[t]he parties may stipulate in writing to allow access to the public to any files or records otherwise restricted under section (c)(2)." *Id.* 22(g)(2).

notes that if a party files a document containing sensitive personal information normally collected on the confidential forms listed in subsection (c)(2), "such documents shall be publicly available in the case record."[107]

Although paper and electronic forms are reasonable short-term measures for resolving this dilemma, once courts implement information systems that can accept, process, and output XML markup, a more efficient and versatile approach would use XML tags to mark up sensitive personal information and control access to it programmatically. For example, when a party or attorney authors a document for filing with a court, he or she could include markup for recognized categories of personal information that the public should be restricted from viewing. Once filed, this document would be stored on a justice information system capable of processing XML markup. Then, when a member of the public accesses this document at a courthouse computer terminal or over the Internet, generic text such as a series of Xs—possibly hyperlinked to a message that explains that personal information has been omitted—would be substituted for the tagged personal information. Moreover, when the same document was accessed by the judge or an attorney of record, the justice information system would be programmed to display the entire document, including the sensitive personal information. As this example makes clear, the justice information system would be programmed to respond to a hierarchy of user access privileges, providing to each user the information that he or she is authorized to view. Significantly, such a system would discriminate among users and not the methods by which they accessed the system. A particular user would be granted access to the same information, whether that user was accessing the system at the courthouse or over the Internet.

In this fashion, the next generation of justice information systems will be able to prevent potentially harmful disclosures of personal information, while simultaneously permitting the same degree of public access at the courthouse and over the Internet.

VI. PRIVACY AND PUBLIC ACCESS TO COURT RECORDS OVER THE INTERNET

In reaching its decision in a case, a court will embrace a particular factual narrative of how the dispute being litigated developed. This

107. *Id.* 22(g)(1) cmt.

narrative is formed from facts found in the case file—the adjudicatory facts viewed by the court as material to its disposition of the case.[108] Unlike the specific details of sensitive personal information, such as one's exact street address or the specific numerals forming one's Social Security number, having access to the adjudicatory facts of a case is essential to achieving the benefits of accountability and citizen education that are promoted by public access to court records. Accordingly, *ceteris paribus*, the public should not be restricted from viewing court documents and files containing adjudicatory facts. In general, courts have accepted this conclusion.[109]

Recently, however, the argument has been put forward that when adjudicatory facts could prove embarrassing or damaging to one's reputation, then public access to these facts should only be available at the courthouse. The idea appears to be that making such discrediting or embarrassing adjudicatory facts available to the public over the Internet will result in more members of the public learning of these facts and that this result is not socially desirable—that is, leads to a net loss of social utility. To evaluate this argument, we need to distinguish between discrediting facts and embarrassing facts, and consider in turn the effects of making each kind of information publicly accessible over the Internet.

Discrediting facts are "the sort that impair[] reputation and by doing so reduce[] one's opportunities for favorable transactions."[110] Discrediting facts often concern "past or present criminal activity or moral conduct at variance with a person's professed moral standards."[111] We might also include within this category, information that "would if revealed correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fiancée."[112] If

---

108. Adjudicatory facts are "unique to individuals—the who, what, where, and when issues typically resolved by juries in judicial trials." 1 KENNETH C. DAVIS & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 293 (1994); *see also* Kenneth C. Davis, *An Approach to Problems of Evidence in the Administrative Process*, 55 HARV. L. REV. 364, 402 (1942). Professor Davis developed the distinction between adjudicatory facts and legislative facts in the context of administrative agency factfinding.

109. Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978) (recognizing a general right to inspect and copy judicial records and documents).

110. RICHARD A. POSNER, OVERCOMING LAW 539 (1995). They reduce opportunities for favorable transactions because people who will not deal either socially or in business with discreditable people will not deal with a person if they learn discrediting facts about him or her.

111. Richard A. Posner, *The Right to Privacy*, 12 GA. L. REV. 393, 399 (1978).

112. *Id.*

discrediting facts about an individual are concealed, inefficient social and economic transactions will often result because the decision to transact with that individual will have been made "either with second-rate information or with information obtained at a higher cost."[113] Concealing discrediting facts about individuals will also lead to an undesirable redistribution of income:

> When it becomes more difficult to measure differences among individuals, their treatment becomes more uniform. Lower and higher risk credit are treated as average risk credit, and similarly with the traits of workers, students, and others. It has become a little easier to default on consumer credit, to embezzle funds, and to shirk duties. A redistribution of income takes place within the enlarged class.[114]

Accordingly, as Richard Murphy has concluded, "if accurate information flow is inhibited, there will be an efficiency loss, whether that loss takes the form of increased transaction costs, a cross-subsidization of 'undesirable' activity, or simply a decrease in the number of mutually beneficial transactions."[115] For these reasons, to the extent that public access to court records and documents over the Internet promotes the disclosure of discrediting facts, it is efficient, and, *a fortiori*, restricting such access is inefficient and, therefore, a questionable public policy.[116]

---

113. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Property*, 84 GEO. L.J. 2381, 2385 (1996).

114. George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 630 (1980).

115. Murphy, *supra* note 113, at 2385.

116. Of course, if one believed that informational privacy and the concealment of discrediting facts were required by our commitment to values that trumped efficiency, one might very well embrace a different judgment about the merits of such a policy. Today, many privacy advocates of a theoretical bent attempt to justify and ground normative views regarding privacy by appealing to autonomy as such a value. An autonomy-based defense of privacy is generally instrumental, arguing that privacy in one form or another is necessary to protect and further individual autonomy. I find such arguments unconvincing for several reasons that I intend to explore more fully in a separate article. For present purposes, however, three areas of concern may be highlighted. First, whether individual humans are in fact autonomous is deeply problematic and contested. Most autonomy-based privacy theorists simply adopt uncritically an Enlightenment era, modernist conception of the self as autonomous. This conception of the self, however, has been challenged and problematized since the mid-twentieth century by many structuralist, post-structuralist, and postmodern theorists. Accordingly, anchoring one's defense of privacy in an uncritical and dogmatic notion of human autonomy is to beg an essential question and commit the fallacy of *petitio principii*. In this regard it is worth noting that even Immanuel Kant did not claim that human beings were autonomous, but merely that an autonomous will is an *a priori* condition on the possibility of moral action—in his sense of "moral action." *See, e.g.*, Otfried Höffe, IMMANUEL KANT 156–57 (1994). Second, given the instrumental character of an autonomy-based defense of privacy, such theorists are promoting a

The preceding argument focuses on static efficiency, that is, the efficient utilization of information that has already been produced. Static efficiency contrasts with dynamic efficiency—the efficiency of the incentives to create new information. While we have just shown that static efficiency favors public access to court records over the Internet, it is also worth noting that dynamic efficiency does not dictate a contrary result. Indeed, assuming that the public has access to court records at the courthouse, the impact of public access to court records over the Internet on dynamic efficiency is likely to be minimal. As a result, the adverse consequences of this enhanced disclosure on the incentives to create new information are likely to be small. Where there is a market for information in court records, data aggregators will compile databases of this information at the courthouse and make them available online for a fee. While this will increase the search costs for obtaining the

---

particular conception of human flourishing and the good life as a socially desirable *telos*. In a liberal democracy, however, law and social policy should not be grounded in any individual's or group's particular conception of human happiness. In the present context, for example, communitarians might very well regard the equation of human happiness with autonomous action as highly problematic and contestable. Finally, insofar as rights to informational privacy appear to require granting an individual some form of control over facts and information, they look suspiciously similar to property rights. In the realm of intellectual property, however, we have a long tradition of viewing facts as part of the public domain. Before we erode this commitment and the public domain that it supports, we should be very sure that there is a sound basis for doing so. The debate over creating a new set of property rights in facts and information should take place within the framework of intellectual property law where if we recognize a property right in facts, we do so directly and expressly after balancing all of the relevant interests and considering all of the relevant policies. We should not do so indirectly through the law of privacy where contested metaphysical appeals to autonomous human selves are likely to be mistaken for an adequate normative and descriptive basis to support such a change.

Unfortunately, a fuller discussion of autonomy and other values that might trump the efficiency analysis presented in the text is beyond the scope of the present Article but such a discussion would clearly have to consider the insightful work of scholars such as Fred H. Cate and Richard J. Varn, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS, A NEW FRAMEWORK FOR FINDING THE BALANCE (1999); Fred H. Cate and Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35 (2002); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 552 (1995); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001); and Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

information, those who value the information more than the access fee will still acquire it. Creditors might be thought a natural example of a group who might pay such an access fee, but they already have access to an inexpensive source for relevant discrediting information: credit bureaus. A more likely example is a passionate gossip, but such a person would probably be just as willing to visit the courthouse. In other words, so long as the information is available at the courthouse for individuals and data aggregators, there will be no shortage of discrediting information available to the interested public. Thus, like considerations of static efficiency, considerations of dynamic efficiency provide no reason for restricting public access to court documents over the Internet.

Embarrassing facts are "the sort that cause[] embarrassment by revealing aspects of a person that while not necessarily or even typically discreditable are not part of one's constructed public self."[117] While different people will find different things embarrassing, most people desire to keep embarrassing facts about themselves concealed. Accordingly, we may assume that for most people, disclosing an embarrassing fact about themselves is personally undesirable. Whether, however, such a disclosure is also socially undesirable will depend on whether we desire to encourage, discourage, or are indifferent to the embarrassing conduct.

To demonstrate how the socially desirable policy varies with our attitude toward the embarrassing conduct, imagine an individual named Bob who has engaged in some form of embarrassing conduct that resulted in an injury caused by Mary. Imagine further that the circumstances surrounding this injury are such that if Bob brought a lawsuit against Mary, Bob would be awarded compensatory damages. Finally, assume that Bob is rational and has a strong preference for concealing embarrassing facts about himself. Although injured, Bob will not bring a lawsuit against Mary if the expected disutility of disclosing his embarrassing conduct is greater than the expected utility of

117. POSNER, *supra* note 110, at 539.

compensation for his injury.[118] Now consider the following three cases.[119]

Case 1. Bob's embarrassing conduct is the kind of conduct that we want to discourage. In this case, the socially desirable policy is to make court records publicly accessible at the courthouse and over the Internet. To see why, consider the effect of this policy both before and after Bob's decision to engage in the embarrassing conduct. Ex ante, Bob's knowledge that the court records in any litigation arising from the embarrassing conduct will be publicly accessible will reduce the expected utility of this conduct and (at the margin) will lead to a different, more socially desirable course of action. Ex post, a policy of disclosing embarrassing conduct will punish Bob for engaging in such socially undesirable conduct, possibly deterring Bob and others from doing so in the future. If Bob sues, the punishment will be the disclosure of the embarrassing conduct. If Bob does not sue, the punishment will be the loss of compensation for his injury.

Case 2. Bob's embarrassing conduct is the kind of conduct to which we are indifferent. In this case, the socially desirable policy is also to make court records publicly accessible at the courthouse and over the Internet. To see why, recall that public access to court records promotes the twin benefits of accountability and citizen education. Because we are indifferent to Bob's embarrassing conduct, whether Bob engages in this embarrassing conduct will neither increase nor decrease the social utility derived from these twin benefits. Moreover, since Bob is rational, he will act to maximize his personal expected utility. Thus, the policy of making court records publicly accessible enhances social utility to the extent that it includes both Bob's personal happiness and the benefits of accountability and citizen education.

Case 3. Bob's embarrassing conduct is the kind of conduct that we want to encourage. In this case, the socially desirable policy is to limit public access to court records at the courthouse and over the Internet to the extent necessary—and only to the extent necessary—to avoid the

---

118. The *expected disutility of disclosure* is equal to the probability of disclosure times the disutility of disclosure. The *expected utility of compensation* equals the probability of winning the lawsuit times the utility of the damages. Under a legal regime in which court records are private or sealed, the probability of disclosure approaches 0. Under a legal regime in which court records are public and easily accessible, the probability of disclosure approaches 1.

119. The three cases set out below assume that Bob is the agent of the embarrassing conduct. Cases could also be developed in which Bob is the recipient or victim of conduct that he finds embarrassing to report. The same policy recommendations would result.

embarrassment of disclosure. Under this policy, Bob does not need to fear the disclosure of his embarrassing conduct. As a result, he will bring the lawsuit against Mary and receive compensation of his injury. This policy encourages the embarrassing conduct both ex ante and ex post. Ex ante, it encourages the conduct because its expected utility is not reduced by the prospect of disclosure. Ex post, it encourages it because he is not punished.

Under this third scenario, limiting public access to court records at the courthouse and over the Internet to the extent necessary to avoid the embarrassment of disclosure can be achieved in two ways. First, for embarrassing conduct that is of a type that recurs frequently, an exception to the public access rule can be established for cases that often involve this kind of conduct. This approach is already used to encourage victims of conduct that they might find embarrassing to report to seek the protection of the courts. Exceptions would presumably be made for cases involving juvenile dependency (abuse and neglect), termination of parental rights, petitions for waiver of parental consent for minor abortions, adoption, guardianships, conservatorships, mental health, and sterilization. Second, for embarrassing conduct of a type that is unlikely to recur, courts can be permitted to limit public access to court records and case files on a case-by-case basis. Courts already exercise this power when they entertain motions to seal documents and entire case files.

Whether one limits access by a general exception to the public access rule or on a case-by-case basis, it should only be limited to the extent required to prevent embarrassment to the potential plaintiff. In most cases, this would require only that all personally identifiable information pertaining to the potential plaintiff be removed from the public records. As already noted, this could be done easily if the information in court records is marked up with XML tags.[120]

Finally, we need to consider the impact of making court records containing facts that are both discrediting *and* embarrassing publicly accessible over the Internet. As before, whether the disclosure of such facts is socially desirable will depend on whether we desire to encourage, discourage, or are indifferent to the underlying conduct. If we want to discourage or are indifferent to the embarrassing and discrediting conduct, then insofar as revealing discrediting information is efficient,[121] the fact that it is discrediting in addition to embarrassing

120. *See supra* Part V.

121. *See supra* notes 110–15 and accompanying text.

simply strengthens the case for public access over the Internet and at the courthouse that was made above for merely embarrassing conduct.[122]

Since presumably we would never want to encourage any kind of discrediting conduct, the only interesting case remaining is one in which we want to encourage the victim of discrediting and embarrassing conduct to seek the protection of the courts. Consider, for example, a woman who while having an abortion is injured through the doctor's negligence. As noted in our earlier discussion of merely embarrassing conduct, to encourage such victims to seek recourse in the courts, we should restrict public access both at the courthouse and over the Internet to the extent necessary to avoid embarrassment to the victim. In the present example, however, there is a public interest in disclosing the doctor's malpractice. While the same information cannot both be revealed and concealed, we can nonetheless develop a process that respects both the needs of the victim and the interests of the public. As with cases of merely embarrassing conduct discussed above, if such a case recurs frequently, it should be subject to a categorial exception from the public access rule, and public access to the case file should be restricted both at the courthouse and over the Internet to the extent necessary to avoid embarrassment to the victim. If, however, such a case occurs only rarely, then the victim should be able to petition the courts to restrict public access to the case file at the courthouse and over the Internet to the extent necessary to avoid embarrassment to the victim. Under either approach to restricting public access to the discrediting and embarrassing facts, a court record indicating the defendant's (e.g., the doctor's) involvement in a lawsuit should be made publicly accessible both at the courthouse and over the Internet, and a process should be created that permits individuals with a legitimate interest in acquiring the discrediting information to petition the court for access to the restricted information.[123] Thus, like facts that are either discrediting or embarrassing, facts that are both discrediting and embarrassing do not justify treating public access to court records over the Internet differently from public access at the courthouse.

The foregoing discussion suggests that notwithstanding the presence of discrediting and embarrassing adjudicatory facts in court records, documents, and files, the public should be able to access these records

122. *See supra* Cases 1 & 2.

123. For an example of such a procedure, see STEKETEE & CARLSON, *supra* note 63, at 53 (CCJ/COSCA Guideline § 4.70(b)).

over the Internet to the same extent that it can access them at the courthouse. If court records and case files should be sealed, then public access to them should be prohibited both at the courthouse and over the Internet. If they are accessible at the courthouse, then they should be accessible over the Internet as well: the courts should not discriminate between methods of access.

VII. CONCLUSION

The machines are coming—a new generation. XML-enabled, these new machines are able to connect to existing legacy systems and with each other to form local, state, and national networks. From the myriad connections being established among the local machines and information systems of courts, justice agencies, law enforcement, correctional facilities, social services and treatment providers, and other members of the justice and public safety communities, integrated justice systems are emerging. These integrated justice information systems provide significant efficiencies, among them diverse kinds of cost savings, error reduction, and improvements in productivity. They permit members of the justice and public safety communities to seamlessly interoperate and exchange records, files, and messages, bridging the information chasm that once separated islands of isolated data. In light of these advantages, the continuing integration of justice information systems into ever larger systems appears inevitable. The Office of Justice Programs at the United States Department of Justice and the Organization for the Advancement of Structured Information Standards are developing XML standards to further facilitate this integration. Court administrators and policymakers mindful of the benefits within their reach are implementing XML solutions.

XML solutions enable individual courts to integrate their case management information systems with an electronic docket and their document management system. They permit the courts to migrate from an increasingly anachronistic paper-based conception of a case file as a collection of documents and records to an understanding of it as structured information. With structured information, one is no longer limited to manipulating two-dimensional containers of information, such as a sheet of paper or the surface of an LCD, but can process and manipulate the information itself. This capability by itself promises to revolutionize court work flow.

These same XML technologies enable integrated justice information systems to interoperate and exchange data over the Internet with personal computers owned by members of the public. With this new ability arises a new question of policy: whether public access to court records over the Internet ought to be permitted and, if so, to what extent? There are at least three answers to this question: public access to court records over the Internet should be denied; public access to court records over the Internet ought to be more limited than the access available at the courthouse; and public access to court files and documents over the Internet should be permitted to the same extent that the public has access to them in the courthouse—that is, courts should not discriminate with respect to methods of access. As the readers who have perused the preceding pages know, I believe that the last is the better answer.

To defend this position, I have parsed the information in a case file into two general categories: sensitive personal information and narrative adjudicatory facts. With regard to the former, I argue that for reasons of public safety and personal security, the public should not have access to it either at the courthouse or over the Internet. Accordingly, the presence of such information in the case file does not provide any grounds for treating public access to court records over the Internet differently from public access at the courthouse. Along the way, I discuss two different ways of removing sensitive personal information from the public case file, one using paper or electronic forms, and the other using XML. Unsurprisingly, I believe that courts will ultimately adopt the latter solution—even if they are forced to use forms in the short term as a transitional measure.

With regard to narrative adjudicatory facts, I further subdivide this category into discrediting facts and embarrassing facts, implicitly recognizing a third subcategory containing all others. Among narrative adjudicatory facts, discrediting and embarrassing facts are foregrounded because they provide the most compelling case for restricting public access to court records over the Internet while allowing unrestricted public access at the courthouse. Clearly, such facts would be more easily and more widely known if the public was permitted to access them in court records over the Internet. Nonetheless, I argue that neither discrediting facts nor embarrassing facts, nor indeed facts that are both discrediting and embarrassing, provide sufficient grounds for limiting public access to court records over the Internet while permitting unlimited access to them at the courthouse. As to discrediting facts, I make my argument by appealing to considerations of static and dynamic

efficiency. As to embarrassing facts, both benign and discrediting, my argument proceeds inductively: considering the effects of disclosing embarrassing facts under several different scenarios. While I conclude that embarrassing facts do not justify discriminating between methods of public access, I do note that under some circumstances, the public should be barred from accessing embarrassing facts both at the courthouse and over the Internet. I note as well that when appropriate, XML permits us to easily remove embarrassing facts from the public files.

The machines are coming. XML-enabled, they promise a justice system that is more efficient, accessible, and humane.