THE FEDERAL COURTS LAW REVIEW

Volume 3, Issue 2 2009

Judicial Information Management in an Electronic Age: Old Standards, New Challenges

Peter A. Winn[1]

INTRODUCTION

When a court engages in the mundane business of entering a judgment or issuing an order, it is simply doing its job. If we take a step back, however, we can see that in order to engage in what ostensibly appears to be routine work, the court must process factual and legal information. From this point of view, the essence of any

1. Lecturer, University of Washington; Senior Lecturer, University of Melbourne; Assistant U.S. Attorney, United States Department of Justice. The views expressed in this article are personal to the author and should not be considered to reflect the position of the United States Department of Justice. Peter A. Winn can be contacted by mail at P.O. Box 85810, Seattle, Washington, 98145 or by email at winnp@u.washington.edu.

judicial system can be understood through how it processes information and translates it into the exercise of governmental power.[2] The point is so obvious that, usually, it hardly bears mention; and when information technology is stable, it does not need to be mentioned. When the rules of information management are settled, structural questions about the relationship between information and power recede into the background of our consciousness. When information technology changes, as it now has with the shift from paper to electronic information, so too does the relationship between information and power. Then, once again, questions about access to and control of information become charged with controversy and come to the forefront of our consciousness. This paper discusses how the recent changes in information technology have forced us once again to focus on the basic principles of information management in the context of our courts.

Under modern democratic theory, the state is considered the agent of the public, and laws are understood to be the outcome of rational debate among private individuals who, via the election of their representatives, enact laws reflecting the public interest.[3] Central to democratic theory is a citizen's right to access information about what the government is up to. Access to such information is necessary for meaningful public oversight of the government, necessary for meaningful public debate about the direction of government policy, and necessary for that debate to be well informed. Our modern legal tradition, affirming the right of a citizen to access court records, reflects this democratic theory.[4]

Of course, even without reference to democratic theory, courts have nearly always operated with the active participation of the community. Community involvement was necessary for the

---

2. The famous adage *"nam et ipsa scientia potestas est,"* translated to "for knowledge itself is power," springs to mind. FRANCIS BACON, MEDITATIONES SACRÆ, *reprinted in* 7 THE WORKS OF FRANCIS BACON, at 241, 253 (James Spedding et al. eds., 1879). Lord Bacon made the same point more articulately when he wrote that "*scientia et potentia humana in idem coincidunt,*" translated as "[k]nowledge and human power are synonymous." FRANCIS BACON, NOVUM ORGANUM 11 (Joseph Devey ed., (1902).

3. *See, e.g.*, JOHN LOCKE, TWO TREATISES OF GOVERNMENT (1824); THOMAS HOBBES, LEVIATHAN (1886). *See generally* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE (Thomas Burger trans., 1991).

4. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580 (1980); *see also* Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606-07 (1982) ("Where . . . the State attempts to deny the right of access in order to inhibit the disclosure of sensitive information, it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest.").

administration of justice when trials took place under the rule of medieval monarchs, and even in the ancient Roman and Greek legal systems. Even in so called "primitive" or pre-literate judicial systems, where magical ordeals and divination ceremonies are used to resolve disputes, the process takes place in public.[5] For whenever society uses a non-violent judicial process to resolve a dispute, the involvement of the community is necessary so that disputes *stay* resolved and the disputants do not succumb to the temptation of self-help. Publicity is simply part of what it means for a society to resolve a dispute peacefully. The alternative is a system which relies on self-help and the threat of violence.[6] By contrast, publicity not only helps resolve past disputes; it helps avoid disputes in the future by providing notice of claims to property as well as the creation or dissolution of other status relationships: marriages, adoptions, paternity, and other important legal relationships.[7]

History also teaches us that attempts to conduct trials in secret, more often than not, end badly. Whether it is the English monarch's use of secret legal proceedings in the Court of the Star Chamber,[8] the use of the *lettre de cachet*[9] by the French *ancien regime*,[10] or more

---

5. *See generally* MAX GLUCKMAN, THE JUDICIAL PROCESS AMONG THE BAROTSE OF NORTHERN RHODESIA (ZAMBIA) (1955); OSCAR CHASE, LAW, CULTURE, AND RITUAL (2005); HENRY CHARLES LEA, SUPERSTITION AND FORCE (1866); ROBERT BARTLETT, TRIAL BY FIRE AND WATER: THE MEDIEVAL JUDICIAL ORDEAL (1986); MAX GLUCKMAN, POLITICS, LAW AND RITUAL IN TRIBAL SOCIETY (2006). *See also* Peter A. Winn, *Legal Ritual*, in READINGS IN RITUAL THEORY (Ronald Grimes ed., 1995).

6. *See* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 260-62 (2007) (discussing in § 8.5 Primitive Law; Revenge; Iceland the financial aspects of primitive legal remedies). *See generally* AESCHYLUS, THE ORESTEIA TRILOGY: AGAMEMNON, THE LIBATION-BEARERS AND THE FURIES (EDA Morshead trans., 1996) (displaying the tragedies that can develop within society when self-help remedies are used).

7. Jeremy Bentham also argues that the publicity of testimony serves as an effective check against perjury. 1 JEREMY BENTHAM, RATIONALE OF JUDICIAL EVIDENCE 581-87 (1827). While this argument has some plausibility, taken to extremes, it would imply that witnesses should not be sequestered. Thus, it is not traditionally given as a reason for the requirement of publicity. Blackstone and Hale correctly note the advantages of oral testimony before the trier of fact, rather than reliance on written testimony before a judicial commissioner, but they do not suggest publicity alone constitutes an effective check against perjury. 3 WILLIAM BLACKSTONE, COMMENTARIES 373 (1769); MATTHEW HALE, THE HISTORY OF THE COMMON LAW OF ENGLAND 343-45 (Charles Runnington ed., 1820).

8. BLACK'S LAW DICTIONARY 1442 (8th ed. 2004) ("An English court having broad civil and criminal jurisdiction at the King's discretion and noted for its secretive, arbitrary, and oppressive procedures, including compulsory self-incrimination, inquisitorial investigation, and the absence of juries. The Star Chamber was abolished in 1641 because of its abuses of power.").

9. *See* Sarah Maza, *Domestic Melodrama as Political Ideology: The Case of the*

recent examples involving totalitarian regimes in our own lifetimes, the use of secret legal proceedings marks political rule which is unstable and short lived. At their core, such regimes are based not on the rule of law, but merely an institutionalized threat of violence. In conclusion, the stability of a legal system depends on its legitimacy; and for a judicial system to *be* legitimate, it must first be *perceived* as legitimate by the community, something which is impossible without an essential transparency at the core of the judicial processes.

While legal systems must be essentially public, it does not follow that any and all information used in the judicial process must be published. At times, judges must have access to highly sensitive information that is not, and should not, be made public. Some of this information may concern the parties; some may relate to non-parties such as witnesses, jurors, and victims; and some may relate to third persons in no way involved in the legal proceeding. For example, judicial decision-makers frequently must have access to the medical and mental health records of private individuals to properly resolve personal injury claims, to determine questions of competence, to decide whether someone should be civilly committed to an institution, to adjudicate a juvenile offender, or to be awarded custody of a child. They often must have access to personal financial records, intimate family letters and diaries; records relating to sexual orientation; and confidential communications between individuals and their doctors, their priests, or their spouses. In order to resolve business disputes, courts often must have access to sensitive information relating to trade secrets or other proprietary information. In other contexts, courts must review company financial information, employee personnel records, and a wide range of other sensitive information. Very little of this sensitive information pertains to the central role of publicity in maintaining the legitimacy of the judicial process, and it only rarely becomes a matter of legitimate public concern.

In addition to sensitive information concerning private individuals and businesses, a broad category of sensitive information involves the operation of government.[11] Obviously, when the

---

Comte de Sanois, 94 THE AMERICAN HISTORICAL REVIEW 1249, 1252 (1913) ("*Lettres de cachet* were secret missives emanating from the sovereign and signed by the secretary of state that, bypassing the normal judicial process, ordered the imprisonment or exile of an individual, often at the behest of members of his or her own family.").

10. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 79 (16th ed. 1976) ("The political and social system of France before the Revolution of 1789.").

11. *See* Nixon v. Warner Commc'n Inc., 435 U.S. 589, 598-99 (1978) ("The interest

government holds the types of sensitive information concerning individuals and businesses identified above—for instance, in the form of tax returns and other required filings—this information is not a matter of legitimate public concern and is entitled to be protected for the same reasons just identified. However, there are other categories of information that may involve matters of legitimate public concern but still require some degree of protection. For instance, during the pendency of a criminal investigation, some kinds of judicial information should not be made public, such as the deliberations of grand juries, information used to obtain search warrants and electronic surveillance orders, the identities of confidential informants, or information in *qui tam* complaints.[12] Likewise, sensitive information involving public health and safety, military defense, or other aspects of national security also need protection.[13] Because this information may be a matter of legitimate public concern, it usually is only temporally withheld.[14] While some information may be withheld from the public forever, as in the case of deliberations of grand juries,[15] in most cases it is disclosed after the danger to the underlying governmental interest has passed.[16] Thus, search warrant affidavits, initially filed under seal, are made public after the execution of the warrant or the indictment of the defendant, and even sensitive military secrets are eventually declassified.[17]

---

necessary to support the issuance of a writ compelling access has been found, for example, in the citizen's desire to keep a watchful eye on the workings of public agencies and in a newspaper publisher's intention to publish information concerning the operation of government.") (internal citations omitted).

12. *See Globe Newspaper*, 457 U.S. at 607-10; Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 920, 937 (D.C. Cir. 2003); United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997); United States v. Amodeo (*Amodeo II*), 71 F.3d 1044, 1047-50 (2d Cir. 1995).

13. Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring); *see* Lloyd Doggett and Michael J. Mucchetti, *Public Access to Public Courts: Discouraging Secrecy in the Public Interest*, 69 TEX. L. REV. 643, 676-77 (1991); *see also* United States v. Reynolds, 345 U.S. 1, 10 (1953) (holding that when the state exercises its privilege and there is a "reasonable danger" that confidential national security information will be exposed, "the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers").

14. Doggett and Mucchetti, *supra* note 13, at 676 ("Where disclosure of information would impede law enforcement or threaten national security, it should be withheld.").

15. United States v. Procter & Gamble Co., 356 U.S. 677, 681-82 (1958).

16. United States v. Lambert, 446 F. Supp. 890, 900 (D. Conn. 1978).

17. Oregonian Pub. Co. v. U.S. Dist. Court for Dist. of Or., 920 F.2d 1462, 1466-67 (9th Cir. 1990) (explaining that in order for disclosure of information, "[t]he court must not base its decision on conclusory assertions alone, but must make specific factual findings. . . . [T]he party seeking access [to a sealed search warrant] is entitled to a presumption of

Finally, there is an often overlooked category of information that, although public, may not be accessed by a certain class of people. Under the rules of evidence, juries are not permitted to consider public information pertaining to the result of illegal searches or improper electronic surveillance.[18] They are not permitted to hear involuntary confessions,[19] or to know immediately the prior criminal history of the accused.[20] More generally, they are not to consider *any* information pertaining to the matter at hand that has not properly been admitted into evidence, even though much of this information may be in the public court record. Thus, many evidentiary rulings by the court take place out of the presence of the jury but are still subject to the full measure of the public's right of access.

The relationship between the publicity of judicial information and the rules of evidence can be seen in the work of the eighteenth Century philosopher Jeremy Bentham. So strongly did Bentham believe in the power of publicity to cure all the evils of a judicial system, that he condemned the application of nearly all exclusionary rules of evidence.[21] However, while many of Bentham's reforms have been accepted, his call for a judicial Panopticon, in which juries would have unfiltered access to all information relevant to factual questions they are charged with deciding, has been largely rejected.[22]

Given the sensitivity of so much of the information in court files, it is remarkable that for the most part, parties, witnesses, jurors and others provide it to the court voluntarily—or at least without much compulsion. People are willing to disclose their sensitive information because they understand that such information is necessary for the resolution of the dispute at hand. This would seem to imply the existence of a relatively high level of trust and confidence in the judicial system—at least in its competence as an information manager. It is difficult to imagine how such a widespread public trust could have

---

entitlement to disclosure. It is the burden of the party seeking closure . . . to present facts supporting closure and to demonstrate that available alternatives will not protect his rights.").

18. Jackson v. Denno, 378 U.S. 368, 386-88 (1964); *see also* Delli Paoli v. United States, 352 U.S. 232, 248 (1957) ("The Government should not have the windfall of having the jury be influenced by evidence against a defendant which, as a matter of law, they should not consider but which they cannot put out of their minds.").

19. *Denno*, 378 U.S. at 385-86.

20. FED. R. EVID. 609.

21. *See generally* Bentham, *supra* note 7.

22. THE FORTNIGHTLY REVIEW 643 (John Morley ed., 1877) (explaining that from 1791 to 1811, Panopticon gradually lost favor and was finally suppressed in 1817).

emerged absent a tradition on the part of judicial bodies only using the disclosed information for the purposes of resolving the dispute—and not for secondary purposes unrelated to the administration of justice.

Thus, public trust and confidence in a judicial system is closely related to its ability to maintain a tradition and practice of information management, a tradition where matters of legitimate public concern are generally made public, while non-public sensitive matters are used only to resolve the dispute at hand, and not exploited for secondary purposes unrelated to the administration of justice. This tradition of information management is reflected in the common-law standards which have guaranteed public access and involvement in the judicial process while still providing a reasonable level of protection for confidential, sensitive information.

In what follows, I will first review the established standards of judicial information management in which public information was expected to be made public, and non-public sensitive information was generally protected. Second, I will place the operation of these standards in the wider context of an adversary system, as well as in the context of the information technology which these standards were developed to address—a paper-based system, in which most if not all judicial records were practically obscure. Third, I will address the changes which have come about with the introduction of electronic information systems and the death of practical obscurity. Finally, I will conclude with some suggestions to address the problems created by the change in information technology, while still preserving the culture and traditions of judicial information management which have been so critical to maintaining public trust and confidence in the judicial system.

THE TRADITIONAL STANDARDS OF JUDICIAL INFORMATION MANAGEMENT

The standards governing judicial information management are often described as striking a "balance" between transparency and privacy,[23] but this metaphor is only partly useful in understanding the standards. Clearly, in the context of any particular dispute over public

23. *See generally* Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307 (2004) (discussing the balance courts have reached between the disclosure of information generated by the judicial process and the need to limit the disclosure of that information).

access, one side argues that failure to grant access will undermine critical public oversight rights, while the other side argues about the grave, unnecessary harm which will attend the release of the sensitive information in question. Given the structure of such conflicts, it is natural to think of the process as one where courts must "balance" the interest of the public in transparency against individual interests in privacy. However, the idea of a balance implies more tension between privacy and transparency than actually exists. Direct head-to-head conflict between transparency and privacy is relatively uncommon.[24] It is rare to see a case in which insuring access to judicial information critical for public oversight threatens to cause any significant threat to an individual's privacy, to a business's ability to compete, or to the government's ability to function.[25] Likewise, protecting sensitive information, when it is not a matter of legitimate public concern, rarely limits judicial oversight or restricts public involvement in the administration of justice.[26] In cases, judges appear to be engaged not so much in *balancing* the competing interests of privacy and transparency, but in *focusing* on the nature of the underlying information itself, and ensuring that each category of information is handled appropriately. Thus, the courts can permit the parties to protect sensitive information which is not a matter of legitimate public concern—through redaction, through protective orders, and a host of other techniques—while maintaining the otherwise general open system of records. The standards have arisen not by balancing two competing interests in transparency and privacy, but out of a careful focus on how best to accomplish these two not necessarily competing goals. Thus, the standards provide reasonable protection for sensitive information without undermining the public's interest in transparency.

---

24. *See Nixon*, 435 U.S. at 597 ("[T]he existence of a common-law right of access to judicial records, . . . an infrequent subject of litigation, its contours have not been delineated with any precision. Indeed, no case directly in point-that is, addressing the applicability of the common-law right to exhibits subpoenaed from third parties-has been cited or discovered."); *Ex parte* Drawbaugh, 2 App. D.C. 404, 407 (1894) ("Such claims of right, and contests over them, are not the ordinary incidents of judicial proceeding; and any attempt to maintain secrecy, as to the records of the court, would seem to be inconsistent with the common understanding of what belongs to a public court of record, to which all persons have the right of access, and to its records, according to long established usage and practice.").

25. *Id.*; *see also In re* Cont'l Ill. Sec. Litig., 732 F.2d 1302 (7th Cir. 1984) ("[W]e fail to see its relevance to publicizing information voluntarily offered into evidence by a party whose possession of the information in no way depended on use of court process.").

26. *See Globe Newspaper*, 457 U.S. at 607-10.

Questions of privacy and publicity are heavily context-specific; as facts vary, intuitions differ. To provide courts the necessary flexibility to address the different intuitions of privacy and publicity in these different contexts, the common law has developed general principles, not narrowly drafted rules. The standards are so flexible that the case law sometimes seems to delight in the perversity of the particular. For instance, as soon as one court hazards the view that the right of public access should be stronger in criminal cases where the right of public access is protected by the First Amendment, one is confronted with an almost endless series of exceptions to this general "constitutional" rule of transparency.[27] To protect the reputation of the innocent and forestall obstruction of the law by the guilty, nearly all pre-trial judicial involvement in the criminal investigative process is secret. Grand juries meet and deliberate entirely in secret. Search and arrest warrants as well as electronic surveillance orders are automatically maintained under seal prior to their execution and often stay under seal long thereafter. The identities of cooperating witnesses are often kept anonymous in the underlying documents themselves. After charges are filed, pre-trial proceedings, such as motions to suppress or *in limine*, are often closed to protect against the danger of prejudicial pretrial publicity. During trial, information is managed even more carefully. As we have seen, juries are not permitted to hear evidence that has been suppressed due to improper searches,[28] improperly obtained confessions,[29] illegal telephone interceptions,[30] or the defendant's prior criminal record or bad acts.[31] Other information may be excluded as well, such as evidence of settlement negotiations[32] or conversations with physicians,[33] with spouses,[34] or with counsel.[35]

---

27. *Richmond Newspapers*, 448 U.S. at 580; *see also Globe Newspaper*, 457 U.S. at 606-07 ("Where . . . the State attempts to deny the right of access in order to inhibit the disclosure of sensitive information, it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest.")

28. Herring v. United States, 129 S.Ct. 695, 699 (2009) ("[O]ur decisions establish an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial.") (citing Weeks v. United States, 232 U.S. 383, 398 (1914)).

29. *See* Arizona v. Fulminante, 499 U.S. 279 (1991).

30. *See* Katz v. United States, 389 U.S. 347 (1967) ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

31. FED. R. EVID. 609.

32. FED. R. EVID. 408.

33. *See* FED. R. EVID. 501. *But cf.* Hardy v. Riser, 309 F. Supp. 1234, 1236-37 (D. Miss. 1970) ("There is no federally-created physician-patient privilege. No such privilege existed at common-law . . . . [T]he privilege is a pure creature of [state] statute.").

After the trial or plea, pre-sentence reports and a host of other critical documents in criminal cases are required to be filed under seal, accessible to the court and the parties only. All these limitations on transparency are supported by strong reasons; there is the need to prevent obstruction of justice, to protect the reputations of the innocent, or to insure a fair trial.[36] The extreme complexity of the system of judicial information flatly contradicts any attempt to formulate a simple and mechanical system of rules.

A similar perversity of the particular appears to be at play in the civil case law, where the Supreme Court has recognized the right of public access under the common law.[37] Thus, in cases that recognize a strong right of public access to information in civil cases, one finds a complimentary concern with protecting legitimate interests in privacy. Civil disputes frequently involve sensitive personal matters, proprietary business secrets, and individual medical or financial records. Various types of administrative cases, most notably involving immigration status and government benefits, involve large amounts of highly sensitive family, political, financial and health information. Information in divorce and child custody proceedings is, perhaps, the most sensitive, penetrating to the inner core of private family relationships. Thus, much of the activity in civil cases—that which involves pretrial discovery—is not filed with the court and, thereby, closed to the public. Even with respect to pleadings and other documents filed in civil cases, one finds a strong pragmatic tradition recognizing the need to protect legitimate interests in privacy.

The flexible standards of judicial information management can be seen in the leading case of *Nixon v. Warner Communications, Inc.*, where the United States Supreme Court recognized the right of the public "to inspect and copy public records and documents, including judicial records and documents."[38] In *Nixon*, the Court ruled that the press could not obtain copies of the tape recordings of conversations between former President Nixon and various members of his staff that

---

34. Wolfle v. United States, 291 U.S. 7, 15 (1934) ("Communications between the spouses, privately made, are generally assumed to have been intended to be confidential, and hence they are privileged . . . .").

35. FED. R. EVID. 502.

36. *See Globe Newspapers*, 457 U.S. at 607-10; *In re* Boston Herald, 321 F.3d 174 (1st Cir. 2003) (restricting access to pleadings containing financial information to protect defendant's privacy); *Ctr. for Nat'l Sec. Studies*, 331 F.3d at 920, 937; *McVeigh*, 119 F.3d at 811; *Amodeo II*, 71 F.3d at 1047-50.

37. *Nixon*, 435 U.S. 589.

38. *Id.*

had been introduced into evidence in the trials of these staff members.[39] Since these tape recordings had been played in public during the trial and the press had been able to obtain transcripts of the tapes, the Court ruled that the public right of access had been adequately served. After the conclusion of the judicial proceedings, former President Nixon's interest in privacy was held to outweigh the common-law right of the press to have copies of the tapes, particularly when the only purpose which could be cited for the release of the copies was their potential for commercial exploitation.[40] The Court described the underlying purpose of the common-law right of access as furthering the "citizen's desire to keep a watchful eye on the workings of public agencies and in a newspaper publisher's intention to publish information concerning the operation of government."[41] However, as Justice Powell noted, in the majority opinion, "the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes."[42] The Court then determined that the commercial purposes offered by the media for obtaining copies of the tape recordings—ostensibly to educate the public as to a matter of great public concern—were outweighed by the privacy interests of an already thoroughly humiliated former president.[43]

In general, while upholding a general rule of openness, the courts consistently permit exceptions to be made when the parties can show a legitimate reason to keep certain types of information confidential, particularly sensitive personal and commercial information. Public access is nearly always permitted when the underlying purpose is to ensure the integrity of the judicial process.[44] On the other hand, courts are quick to protect personal information when the purpose of access is not related to facilitating public scrutiny of the judicial process and is not otherwise a matter of legitimate public concern, particularly when the purpose of the access is to exploit information in judicial records for commercial or other purposes unrelated to public

39. *Id.* at 611.
40. *Id.* at 602.
41. *Id.* at 598 (citations omitted).
42. *Nixon*, 435 U.S. 589.
43. *Id.*
44. *See, e.g.*, *Richmond Newspapers*, 448 U.S. at 575-78; *Cont'l Ill. Sec. Litig.*, 732 F.2d at 1313-1316.

oversight of the judicial system.[45]

Even in those judicial circuits which have recognized a First Amendment right of public access in civil cases,[46] the courts do not appear to apply the constitutional standard any more restrictively than in circuits which only follow the common law.[47] In all of them, the right of public access is limited to court proceedings which historically have been public.[48] The right of access is limited to "judicial documents" such as opinions, orders, and docket sheets; and ordinarily does not apply to legal documents which may be filed with the court but relate to peripheral judicial matters such as discovery disputes.[49] The right only attaches to pleadings which are "relevant to the performance of the judicial function and useful in the judicial process."[50] Such non-core documents may be sealed merely on a showing of "good cause."[51] The reasoning is that if a court relies on a document in making its decision, the right of public access should be triggered and afforded; but if a court does not refer to or use a document in its decision-making process, the parties should be permitted to protect it.

Finally, there is considerable precedent suggesting that the common-law and constitutional rights of public access do not

---

45. *See, e.g.*, *Globe Newspapers*, 457 U.S. at 607-610; *In re* Knoxville News-Sentinel Co., 723 F.2d 470 (6th Cir. 1983).

46. Publicker Indus. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1984).

47. Rushford v. New Yorker Magazine, Inc., 846 F.2d 249, 253 (4th Cir. 1988) ("[T]he denial of access must be necessitated by a compelling government interest and [be] narrowly tailored to serve that interest."); *see also* Va. Dep't of State Police v. Wash. Post, 386 F.3d 567 (4th Cir. 2004).

48. *See, e.g.*, *Publicker Indus.*, 733 F.2d at 1067-1071; *Rushford*, 846 F.2d at 253; *Cont'l Ill. Sec. Litig.*, 732 F.2d at 1308; Brown & Williamson Tobacco Corp. v. FTC, 710 F.2d 1165, 1178-79 (6th Cir. 1983); Westmoreland v. Columbia Broad. Sys., Inc., 752 F.2d 16, 22-23 (2d Cir. 1984); Anderson v. Cryovac, 805 F.2d 1, 30-31 (1st Cir. 1986) (discussing First Amendment cases in other circuits); *In re* Cendant Corp., 260 F.3d 183, 198 n.13 (3d Cir. 2001) ("[T]he parameters of the First Amendment right of access to civil proceedings are undefined. There remain significant constitutional questions about what documents are subject to its reach."); N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 200 (3d Cir. 2002) (ruling newspapers did not have right of access to civil immigration proceedings). *See generally* Wilson v. Am. Motors Corp., 759 F.2d 1568, 1569-70 (11th Cir. 1985) (explaining that the Eleventh Circuit has not explicitly joined these constitutional holdings, but has recognized a right of access to certain fundamental aspects of civil proceedings).

49. United States v. Amodeo (*Amodeo I*), 44 F.3d 141, 145 (2d Cir. 1995) ("The mere filing of a paper or document with the court is insufficient to render that paper a judicial document subject to the right of public access.").

50. *Id.*

51. Kamakana v. City and County of Honolulu, 447 F.3d 1172, 1179-80 (9th Cir. 2006).

authorize access to court records for any purpose whatsoever, but that the right only applies when the request is based on a proper purpose. Thus, in the past, courts have rejected requests where they were based solely on a desire to exploit the information for commercial purposes,[52] for sources of information to help a business rival's competitive standing,[53] or as a reservoir of libelous information.[54] The cases where courts retain the authority to review the purposes for which access was requested, and where the right of access is conditioned on the existence of a legitimate purpose, remain good precedent.[55] Unlike the statutory system of access under the Freedom of Information Act, where the underlying purposes of the requestor may not be questioned, it is difficult if not impossible to see how the context-specific standards of judicial information management can be applied without an evaluation of the proposed uses to which the information is intended to be put.[56]

OPERATION OF THE SYSTEM OF INFORMATION MANAGEMENT IN AN ADVERSARY SYSTEM

It is axiomatic that in an adversary system the standards of judicial information management are enforced only in the context of a dispute. The disputes arise between the parties to a lawsuit, when an outside party such as a newspaper intervenes in a case to gain access

---

52. *See* Damiano v. Sony Music Enter., Inc., 168 F.R.D. 485 (D.N.J. 1996) (holding that the possibility that Plaintiff would use sought after information for commercial exploitation warranted an order signifying that the materials obtained in discovery were confidential).

53. *See generally* Zenith Radio Corp. v. Matsushita Elec. Indus. Co., 529 F. Supp. 866 (E.D.Pa. 1981).

54. Park v. Detroit Free Press Co., 40 N.W. 731, 734-35 (Mich. 1888) (holding that the press has no more right than a private person to publish libelous information); *see also* Sanford v. Boston Herald-Traveler Corp., 61 N.E.2d 5, 6 (Mass. 1945) ("[W]e are not prepared to concede that the general right of inspection of public records enables one in every instance to publish such records broadcast without regard to the truth of defamatory matter contained in them.").

55. *See Nixon*, 435 U.S. at 598 (quoting *In re* Caswell, 29 A. 259 (R.I. 1893)) ("[T]he common-law right of inspection has bowed before the power of a court to insure that its records are not 'used to gratify private spite or promote public scandal' through the publication of 'the painful and sometimes disgusting details of a divorce case.'"); *see also* C. v. C., 320 A.2d 717, 723, 727 (Del. 1974); LeClair v. New England Tel. & Tel. Co., 294 A.2d 698 (N.H. 1972); *In re* J. Children, 421 N.Y.S.2d 308 (Fam. Ct. 1979).

56. The common-law and constitutional rights of public access to court records thus operate with a different standard from that employed under the Freedom of Information Act, 5 U.S.C.A. § 552 (2008), under which there is no inquiry into the underlying purpose for which a governmental record is requested.

to the information[57] or when the presiding judge *sua sponte* forces the issue. Unless someone is willing to assert the right, the principles of information management will not be enforced. The disputes often involve the practical difficulty of working with sensitive information in the context of an adversarial process.[58] Thus, when parties get into a dispute about the terms of a protective order, no general invitation goes out to the public to participate. Faced with a highly complex dispute between the parties, judges are loath to make the process more difficult by advocating for an absent public. When presented with an agreed protective order resolving the dispute, judges are usually inclined to sign it, and turn their attention to some other problem.[59] Likewise, when faced with a motion to seal a settlement (presented as a necessary condition of the deal),[60] judges may give in to the temptation to clear their busy docket of one more thorny case, even at the expense of some pesky factual and legal predicate that no party has an interest in asserting.[61]

The court system is not fundamentally designed to serve the abstract interests of the public.[62] Judges are sensitive to the fact that few people ever truly desire to be in court, and to force these people to disclose embarrassing personal information or to force the disclosure of confidential business information, is to make an already unpleasant experience that much worse.[63] Particularly with an elected

---

57. *See Nixon*, 435 U.S. 589; *Caswell* 29 A. 259 ; C. v. C., 320 A.2d 717 (Del. 1974); *Detroit Free Press*, 40 N.W. 731.

58. *See* Munzer v. Blaisdell, 48 N.Y.S.2d 355 (App. Div. 1944); *Caswell*, 29 A. 259 ; C. v. C., 320 A.2d 717 (Del. 1974).

59. David S. Sanson, *The Pervasive Problem of Court-Sanctioned Secrecy and the Exigency of National Reform*, 53 DUKE L.J. 807, 810 (2003) ("If both parties are in favor of sealing (or even if only one party is asking for secrecy), there is no reason, some argue, for the court to frustrate the aims of the litigants by unnecessarily delaying what is already likely to be a complex and costly proceeding.").

60. *See, e.g.*, *In re* Franklin Nat. Bank Sec. Litig., 92 F.R.D. 468 (E.D.N.Y. 1981), *aff'd sub nom.* FDIC v. Ernst & Ernst, 677 F.2d 230 (2d Cir. 1982) (holding that the sealed settlement, even in the face of strong public interest, will remain sealed because the agreement would never have been reached without the confidentiality clause).

61. *See* Jack B. Weinstein, *Secrecy in Civil Trials: Some Tentative Views*, 9 J.L. & POL'Y 53, 58 (2000) ("Most agreements are uncontested, and crowded calendars put great pressure on judges to move cases. As a result, judges routinely approve sealing and secrecy orders. Settlement agreements are often filed under seal as a matter of course.").

62. Although the pervasiveness of this practice is hard to measure, the *Seattle Times* revealed that the elected judges in King County, Washington "improperly" sealed hundreds of cases by the agreement of the parties. *See* Ken Armstrong, Justin Mayo & Steve Miletich, *The cases your judges are hiding from you*, SEATTLE TIMES, Mar. 5, 2006, *available at* http://seattletimes.nwsource.com/html/localnews/2002845009_seal05m.html.

63. Sanson, *supra* note 59, at 808-09.

judiciary, characteristic of the vast state court system, the courts are there to resolve disputes, and judges are far more interested in helping those unfortunate parties who are stuck in the system to get out than they are in trying to help an invisible public abstraction to get in.[64]

The tension between a set of standards dictating openness and an actual practice which appears to be more closed, follows from the simple fact that in our judicial system, rights have traditionally had meaning only as used to resolve a dispute. In this world, the right to *public* access will only exist if a party, acting on its own *private* interests, chooses to assert it. While the standards seem to imply great transparency, the structure of a dispute oriented litigation process creates a reality which often appears to work in the opposite way. Many cases recognizing a right of public access arise after the parties have obtained an improper agreed sealing order from the court, and an outsider—usually a media organization—has intervened to bring the challenge.[65] Other cases arise when an appellate court notices the violation and issues a good scolding to the parties (and implicitly the lower court).[66] Thus, underlying the very precedents articulating the standards of broad transparency, one can see a general practice of party controlled opacity un-policed by the lower courts.[67] It is a world where agreed sealing or protective orders are routinely signed by the trial judge,[68] with scant attention to the question whether the order, in fact, meets the legal standard as articulated in the case law.[69]

In the context of an abstract entity like the public, a right of public access that belongs to everyone soon becomes a matter of

---

64. *See* Lon L. Fuller, *The Forms and Limits of Adjudication*, 92 HARV. L. REV. 353 (1978) (arguing public access to trials exists but courts and judges are in place to help private parties solve private disputes through the legal system).

65. *See generally In re* Subpoena to Testify Before Grand Jury Directed to Custodian of Records, 864 F.2d 1559, 1561 (11th Cir. 1989) (allowing news organizations to appeal an order prohibiting counsel and parties from disclosing information about grand jury proceedings); *see also* United States v. Antar, 38 F.3d 1348, 1355-56 (3d Cir. 1994) (allowing news organizations to appeal a judge's order sealing voir dire transcripts); *see also* United States v. Chagra, 701 F.2d 354, 360 (5th Cir. 1983) (allowing news organizations to appeal an order closing a trial).

66. *See, e.g.*, *In re* Azabu Bldgs. Co., No. 05-50011, 2007 WL 461300, at *2 (Bankr. D. Haw. Feb. 7, 2007) ("The [parties] have failed to carry their burden of showing compelling reasons to seal the Basic Agreement and its attachments. The existence of a contractual confidentiality provision, standing alone, cannot constitute a 'compelling reason.' By enforcing such a provision without additional justification, the court would abdicate to the parties its duty to preserve public access to judicial records.").

67. *See generally* Sanson, *supra* note 59.

68. *See* Weinstein, *supra* note 61.

69. *See* Armstrong, *supra* note 62.

concern to no one.[70] In 2006, the *Seattle Times* conducted a study of a typical urban country court system, finding that ninety-seven percent of the sealing orders issued failed to meet the legal standard established under state and federal constitutional law.[71] The story was presented as a scandal; a blatant and embarrassing contradiction between the ideological narrative in the case law and the actual practice of information management by the courts. However, in fact, the story represented the natural operation of an adversarial system of justice. Likewise, in a recent decision by Federal Magistrate Judge Stephen Smith in the Southern District of Texas, the court noted a large number of electronic surveillance orders still under seal long after the termination of the criminal cases with which they were originally associated—describing the manila envelopes containing the orders with the immortal words: "judicial kudzu."[72] The accumulation of such "judicial kudzu" did not reflect any intention on the part of prosecutors to flout the standards of transparency or to conceal important facts from the public. Rather, the documents were sealed appropriately when the information was sensitive, but were apparently forgotten after the information became stale.[73] Unfortunately, it appears that nothing in the adversarial system forces the judicial system to engage in any systematic weeding of such information kudzu. Unless motions are filed to lift temporary seals, the information will remain secret in perpetuity.[74]

Ordinarily in the law, someone not a party to a case cannot be

---

70. *See, e.g.*, *Brown & Williamson Tobacco*, 710 F.2d at 1178 ("The crucial prophylactic aspects of the administration of justice cannot function in the dark; no community catharsis can occur if justice is 'done in a corner [or] in any covert manner.'") (citing *Richmond Newspapers*, 448 U.S. at 571).

71. Armstrong, *supra* note 61 ("The judges have displayed an ignorance of, or indifference to, the legal requirements for sealing court records. They have routinely sealed files while 1) offering little or no explanation, 2) applying the wrong legal standard, and 3) failing to acknowledge, much less weigh, the public interest in open court proceedings. At least 97 percent of their sealing orders disregard rules set down by the Washington Supreme Court in the 1980's.").

72. *In re* Sealing & Non-Disclosure of Pen/Trap 2703(D) Orders, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008).

73. Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 210-11 (2009) ("No one questions the need for temporary sealing to avoid jeopardizing an ongoing criminal investigation, but these orders are effectively sealed in perpetuity [and] . . . court orders and warrants issued . . . will likely never see the light of day.").

74. *Id.* at 214 ("[I]t is the public record of judicial decisions that renders those decisions legitimate. . . . A court's inherent power to supervise its own records does not include the power to undermine the source of its own legitimacy.").

bound by the ruling of the court in that case, but the opposite result seems to arise in the context of judicial information management.[75] Just as decisions of the parties involving information management affect the interests of the unrepresented public, so too can these decisions affect the interests of other unrepresented private individuals. Court records contain sensitive information about crime victims,[76] about witnesses,[77] about jurors,[78] and about a host of other persons. The parties to a dispute may ignore the information privacy interests of third parties in exactly the same way they may short-change the information interests of the public.[79] The failure of an adversarial legal system to address the privacy interests of third parties was graphically illustrated when the Public Access to Court Electronic Records (hereinafter PACER)[80] system was partially audited[81] by Public.Resource.Org.[82] The audit revealed that the rule prohibiting the filing of social security numbers was not consistently enforced, with un-redacted social security numbers appearing hundreds of times in court pleadings around the country.[83] Of course, when questions of information management are placed in dispute, courts resolve the question, and the standards of information management are applied with appropriate focus. However, when no

---

75. *See Am. Motors Corp.*, 759 F.2d at 1571 ("[W]e conclude that these litigants do not have the right to agree to seal what were public records. The district court must keep in mind the rights of a third party—the public, 'if the public is to appreciate fully the often significant events at issue in public litigation and the workings of the legal system.'") (quoting Newman v. Graddick, 696 F.2d 796, 803 (11th Cir. 1983)).

76. ACLU of Miss. v. Fordice, 56 F. Supp. 2d 712, 715 (S.D. Miss. 1999).

77. *In re* Marshall, No. 500095/2006, 2006 WL 2546192, at *6 (N.Y. Sup. Ct. Aug 29, 2006).

78. Press-Enter. v. Superior Court, 464 U.S. 501, 512 (1984).

79. *Nixon*, 435 U.S. at 597-608.

80. The PACER Service Center is the Federal Judiciary's centralized registration, billing, and technical support center for electronic access to U.S. District, Bankruptcy, and Appellate court records. PACER Service Center, http://pacer.psc.uscourts.gov (last visited May 1, 2009).

81. The partial audit covered an estimated 20% of the records in the PACER system and focused on 32 of the 94 federal judicial districts. The audit covered records filed after December 1, 2007, when the new privacy rules were added to the Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure. It also covered records before that time, when most federal district courts had enacted local rules to protect privacy in court filings, as recommended by the Administrative Office of United States Courts. *See* Letter from Carl Malamud, President & CEO, Public.Resource.Org, to Lee H. Rosenthal, Chair, Comm. on Rules of Practice and Procedure (Oct. 24, 2008), http://public.resource.org/scribd/7512583.pdf.

82. *Id.* (explaining a not-for-profit advocacy group-run Web site collecting data on administrative violations by courts).

83. *Id.*

dispute is presented to the court, the judicial information management system breaks down. Because of the nature of the adversarial system, the interest of the public in the transparency of judicial records and the interest of unrepresented third parties in protecting sensitive private information are equally ignored as the parties before the court pursue their own personal interests. Thus, the standards of judicial information management, with their twin goals of publicity and privacy, cannot be enforced effectively in the context of an adversarial system.

Until recently, the limitations of the judicial system's ability to implement the twin goals of proper information management were largely concealed by the "practical obscurity" of a paper-based system of judicial records.[84] In a system where paper records are stored in clerks' offices, most records are seen only by the actual participants in the litigation at hand. In order to access a particular file, a third party has to locate the courthouse storing the records, travel to the clerk's office, wait in line, fill out necessary forms to request retrieval of the records, wait for the clerk to find the files, sign for them, read through them to find the relevant records, order the records to be copied, pay the necessary copying charges, and so forth and so on, all with no guarantee that the desired information would in fact be located in the court file, or that the court file would even be available and not in use in the judge's chambers. Thus, unless a third party has an especially strong interest in the information in a particular court file, there would be little motivation to seek access to the record. As a result, while the records in a paper-based system of court records are technically public, all information in the court file receives a considerable amount of protection virtually by the sheer difficulty of accessing it.[85] The "practical obscurity" of a paper-based system greatly reduced the dangers of third parties misusing sensitive personal information in the court file. However, for exactly the same reasons, the "practical obscurity" of a paper based record-keeping system also obscures routine violations of the public's right of access. Thus, the frequency of improper sealing orders was also concealed, and the sheer difficulty of accessing unsealed information meant that

84. The phrase "practical obscurity" was used by Justice Stevens to describe the phenomenon by which sensitive information can receive a considerable amount of protection, merely by virtue of the practical difficulty cost of retrieving paper based records. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763-64 (1989).

85. *Id.*

by and large, most information of legitimate concern to the public remained for all practical purposes entirely in the dark.

Of course, the foregoing criticism of the paper-based adversarial system of judicial information management is in large part anachronistic—it assumes the point of view of our present much more efficient system of electronic record-keeping. However, if one re-assumes the perspective of someone working within a paper-based system of records, the system of "practical obscurity" can still be seen as relatively successful in accomplishing the twin goals of providing meaningful public access—enough access for healthy judicial oversight and political feedback—while still providing enough protection for sensitive personal, business, and governmental information to maintain the trust of the litigants. The system appears to have accomplished this by making available to the parties multiple tools to manage sensitive information. As we have seen, records filed with the court enjoyed a default rule of "practical obscurity," where access was open in principle, but still required an investment of time and money—enough to ensure that, in the absence of independent interest in the proceedings, it was unlikely the information would be widely disseminated. If information were particularly sensitive, the parties, through an agreement, could usually obtain a sealing order from the court. The entry of a sealing order, however, did not indefinitely foreclose public access to the information. If there was sufficient interest in the information because of its political or social value, the news media—as a proxy for the public—could challenge a sealing order which failed to comply with the legal standard.[86] The leading cases involving the right to public access nearly all involve such interventions by the news media to challenge an improperly granted sealing order originally obtained through agreement by the parties.[87]

---

86. *See* United States v. Brooklier, 685 F.2d 1162, 1165 (9th Cir. 1982); Sacramento Bee v. U.S. Dist. Court, 656 F.2d 477, 481 (9th Cir. 1981); United States v. Sherman, 581 F.2d 1358, 1360 (9th Cir. 1978); CBS, Inc. v. Young, 522 F.2d 234, 237 (6th Cir. 1975); State *ex rel.* Gore Newspapers Co. v. Tyson, 313 So. 2d 777 (Fla. Ct. App. 1975).

87. *See, e.g.*, *In re* Express News Corp., 695 F.2d 807 (5th Cir. 1982); Central S. Car. Chapter Soc'y of Prof. Journalists v. Martin, 556 F.2d 706 (4th Cir. 1977); Phoenix Newspapers, Inc. v. Superior Court, 418 P.2d 594 (Ariz. 1966) (en banc); Commercial Printing Co. v. Lee, 553 S.W.2d 270, 272-73 (Ark. 1977) (en banc); Oxnard Publ'g Co. v. Superior Court, 68 Cal. Rptr. 83 (Ct. App. 1968); State *ex rel.* Miami Herald Publ'g Co. v. McIntosh, 340 So.2d 904 (Fla. 1976); Gannett Pac. Corp. v. Richardson, 580 P.2d 49 (Haw. 1978); Honolulu Advertiser, Inc. v. Takao, 580 P.2d 58 (Haw. 1978); Des Moines Register & Tribune Co. v. Osmundson, 248 N.W.2d 493 (Iowa 1976) (en banc); Ashland Publ'g Co. v. State, 612 S.W.2d 747, 753 (Ky. Ct. App. 1980); Northwest Publ'ns, Inc. v. Anderson, 259 N.W.2d 254, 256-57 (Minn. 1977); State v. Simants, 236 N.W.2d 794 (Neb. 1975), *rev'd on*

Seen in this light, the paper-based system of information management did not "close off" information but worked to allocate costs between the parties interested in protecting the information, and the parties interested in accessing it. In the context of the adversary system, the default rule of practical obscurity may have placed what we can now see was an unfair cost on the outsider seeking access, but without major structural changes, it is difficult to see how an alternative cost allocation could have been instituted. As such, the system of practical obscurity does not appear to have been improper or irrational. There was a general presumption that information in filed pleadings would require some expenditure to obtain, but would still be relatively cheap for an outsider to access. There was then an intermediate level where information exchanged by the parties could be protected at the cost of obtaining a sealing or protective order, which would naturally increase the access cost to an outsider. However, when the information was of actual interest to large numbers of people—that is, of significant economic and/or political value—it would be in the interest of media or other outsiders to expend resources to force its disclosure. Since the adversarial system always permitted sealing orders to be subject to legal challenge by outsiders, the goals of public oversight and scrutiny were maintained, and the system could function to rationally allocate the risk of disclosure of sensitive information between the parties and the public. At the same time, however, the system also facilitated a certain level of complacency, if not hypocrisy—permitting judges to make extremely broad pronouncements about the sacred nature of the right of public access when in fact the courts never operated anything like a truly open system of public records.[88] This form of complacency

---

other grounds sub nom Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976); State *ex rel.* N.M. Press Ass'n v. Kaufman, 648 P.2d 300 (N.M. 1982); Oliver v. Postel, 282 N.E.2d 306 (N.Y. 1972); N.Y. Times v. Starkey, 380 N.Y.S.2d 239 (App. Div. 1976); State *ex rel.* Beacon Journal Publ'g Co. v. Kainrad, 348 N.E.2d 695 (Ohio 1976); E.W. Scripps Co. v. Fulton, 125 N.E.2d 896 (Ohio Ct. App. 1955); Ok. Publ'g Co. v. District Court, 555 P.2d 1286 (Okla. 1976), *rev'd on other grounds*, 430 U.S. 308 (1977); Phila Newspapers, Inc. v. Jerome, 387 A.2d 425 (Pa. 1978); Herald Ass'n v. Ellison, 419 A.2d 323, 324 (Vt. 1980); Charlottesville Newspapers v. Berry, 206 S.E.2d 267 (Va. 1974); Seattle Times v. Ishikawa, 640 P.2d 716, 719 (Wash. 1982) (en banc); Federated Publ'ns, Inc. v. Kurtz, 615 P.2d 440 (Wash. 1980) (en banc); State *ex rel.* Newspapers, Inc. v. Circuit Court, 221 N.W.2d 894 (Wis. 1974).

88. Sheppard v. Maxwell, 384 U.S. 333, 349 (1966) ("The principle that justice cannot survive behind walls of silence has long been reflected in the 'Anglo-American distrust for secret trials.'") (internal citations omitted); Estes v. Texas, 381 U.S. 532, 541-542 (1965) ("It is true that the public has the right to be informed as to what occurs in its

would come to a rude end with the introduction of electronic judicial information systems—the most prominent of which was the federal PACER system.

ELECTRONIC COURT FILING AND THE DEATH OF PRACTICAL OBSCURITY

PACER is the electronic public access service that allows users to obtain case and docket information from federal appellate, district, and bankruptcy courts via the internet. PACER, together with Case Management/Electronic Case Files ("CM/ECF"), which was implemented in the bankruptcy courts in 2001, the federal district courts in 2002, and the appellate courts in 2004, represented the largest and earliest wholesale adoption of an entirely electronic record keeping system by any court system in the United States. The attraction was obvious. For the courts, electronic filing allowed for substantial operational benefits with tremendous savings of space and storage capacity; it allowed dramatically faster processing times for the filing of documents, while permitting significant reductions in personnel at the clerk's offices. For attorneys, electronic filing permitted twenty-four hour access to the case files, the ability to file documents remotely over the internet, to receive automatic email notices for case activity, the ability for multiple parties to concurrently access a single record, and real time information about all judicial activity. It also improved search and reporting capacities, allowing for better access, and understanding of the judicial process.

At the same time, the introduction of electronic filing eliminated the phenomenon of "practical obscurity," which in the days of a paper-based information system, as we have seen, had concealed certain types of questionable judicial practices as well as protected individual privacy. Accordingly, the new electronic filing systems now made possible systematic audits of large numbers of judicial records at relatively low cost. The *Seattle Times* investigation of the extent to

---

courts . . . . Reporters of all media, including television, are always present if they wish to be and are plainly free to report whatever occurs in open court . . . ."); Maryland v. Balt. Radio Show, Inc., 338 U.S. 912, 920 (1950) (Frankfurter, J., dissenting) ("One of the demands of a democratic society is that the public should know what goes on in courts by being told by the press what happens there, to the end that the public may judge whether our system of criminal justice is fair and right."); Pennekamp v. Florida, 328 U.S. 331, 361 (1946) (Frankfurter, J., concurring) ("Of course trials must be public and the public have a deep interest in trials."); Craig v. Harney, 331 U.S. 367, 374 (1947) ("A trial is a public event. What transpires in the court room is public property.").

which sealing orders were improperly being used by state courts would have been nearly impossible to accomplish in a system of paper-based records.[89] Likewise, the identification of the extent to which court filings contained un-redacted social security numbers was also made possible by the new electronic media.[90] On the other hand, and for the same reasons, the same computerized search and compiling functions have also dramatically increased the risk of misuse of sensitive personal information in court files.[91]

The computerization of court records has also raised a new problem that did not exist in the days of paper-based records: data aggregation. When data aggregation companies such as Westlaw[92] and Lexis[93] compiled and marketed electronic versions of court records after initially obtaining the information from paper-based court systems, the cost of retrieval usually meant that data aggregation was largely restricted to judicial opinions deemed worthy of publication by the judges themselves. When the underlying court system itself went online, not only "unpublished" orders and opinions became routinely accessible, but briefs and other attachments to pleadings became accessible as well. Westlaw, Lexis, and other data aggregation companies also appear to have begun to engage in massive and indiscriminate downloads of virtually all accessible information in court files. With no oversight or audit of the various potential secondary uses to which these companies may apply this data, the homeostasis of the paper-based information ecosystem—a system where sensitive information was used only for purposes relating to the administration of justice—has now been significantly

---

89. *See* Armstrong, *supra* note 62 and accompanying text.

90. John Schwartz, *An Effort to Upgrade a Court Archive System to Free and Easy*, N.Y. TIMES, Feb. 12, 2009, http://www.nytimes.com/2009/02/13/us/13records.html?_r=1.

91. *Id.*; *see also* FEDERAL TRADE COMMISSION, CONSUMER SENTINEL NETWORK COMPLAINT DATA BOOK 4-6 (2008), http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf (noting that identity theft complaints have risen twenty-one percent from 2007, and that identity theft represents twenty-six percent of all fraud complaints).

92. Thomson Reuters, http://www.thomsonreuters.com/products_services/legal/Westlaw (last visited May 1, 2009) ("Information resources on Westlaw® include more than 30,000 databases of case law, state and federal statutes, court documents, administrative codes, newspaper and magazine articles, public records, law journals, law reviews, treatises, legal forms and other information resources.").

93. LexisNexis, http://www.lexisnexis.com/government/solutions/research/courtlink.aspx (last visited May 1, 2009) ("[Lexis] gives you instant access to current court dockets and more than 200 million federal, state and local court records. Search by litigant, attorney, law firm, jurisdiction, nature of suit and keyword to find relevant past and present business litigation activity.").

disrupted.

When criminal records were placed online, concerns were raised that providing online access to information regarding the cooperation and other activities of co-defendants might increase the risk that judicial information could be used to intimidate, harass, and possibly harm crime-victims, cooperating defendants, and their families.[94] In August of 2004, some of these apprehensions began to be realized with the appearance of Web sites such as Whosarat.com.[95] At this Web site, users around the country are provided a convenient central clearing house to post state and federal agents' and informants' related information including names, age, location, race, occupation, past illegal activity, criminal records, and, most ominous of all, photographs.[96] While the site claims merely to exist to "assist attorneys and criminal defendants with few resources,"[97] the legitimate and truthful information posted has always been made available to defense attorneys by operation of law.[98] Rather, the site appears to focus on identifying and placing in harm's way cooperating witnesses and undercover government agents.[99] Prosecutors and defense counsel, engaged in gang-related investigations, have begun to see a recent marked increase of the use of plea agreements obtained from the court system for the purposes of intimidating cooperating co-defendants.[100]

Perhaps the most significant change to the judicial information ecosystem was the elimination of a human interface in the clerk's office, ending the informal social protections which formerly existed to control access to the case file. Broad unrestricted anonymous access to the court file now meant prohibited persons—jurors—could

---

94. Adam Liptak, *Web Sites Listing Informants Concern Justice Dep't*, N.Y. TIMES, May 22, 2007, http://www.nytimes.com/2007/05/22/washington/22plea.html

95. Whosarat.com, http://www.whosarat.com/index.php (last visited May 30, 2009).

96. *Id.*

97. *Id.* at http://whosarat.com/aboutus.php ("Who's A Rat is a database driven website designed to assist attorneys and criminal defendants with few resources.").

98. Liptak, *supra* note 94.

99. *Id.*; *see also* Letter from Michael A. Battle, Dir., Exec. Office for U.S. Attorneys, U.S. Dep't of Justice, to James C. Duff, Sec'y, Judicial Conference of the U.S. at 2 (Dec. 6, 2006), *available at* http://www.floridasupremecourt.org/pub_info/summaries/briefs/06/06-2136/Filed_01-31-2007_ProsecutorsSupplementalCommentsAppendix.pdf ("The posting of sensitive witness information on websites such as "whosarat" poses a grave risk of harm to cooperating witnesses and defendants . . . .").

100. Letter from Kenneth E. Melson, Dir., Exec. Office for U.S. Attorneys, U.S. Dep't of Justice, to Abel J. Matos, Chief, Chief Admin. Policy Staff, at 2-4 (Oct. 26, 2007), *available at* http://www.privacy.uscourts.gov/attachments/65.pdf.

access defendants' criminal records,[101] review evidentiary motions *in limine*[102] to exclude evidence, and even review the underlying incriminating evidence after it had been ruled inadmissible by the trial court. Although, so far, there appears to have only been anecdotal reports of such abuses, access to the court files by jurors would be a phenomenon nearly impossible to measure. While jurors have long been known to read newspaper accounts of trials in which they were involved (in violation of their preliminary instructions), the practice did not present a serious threat to due process, since the likelihood that reading a newspaper account of a trial would significantly influence a juror's decision on the merits of a case was minimal. The ability of a juror now to access the court's electronic filing system presents a much more serious threat to the operation of the rules of evidence, and to due process itself.[103] Without having intended to, it appears that the new system of electronic court files may begin to push the judicial system in the direction of a Benthamite Panopticon, where the enforcement of exclusionary rules of evidence is abandoned as futile, and nothing stands between the defendant and justice but the power of publicity to discern the truth. It is not my intention to overdramatize this concern; but there appears no easy way to mitigate the potential harm to the defendant's right to a fair trial that a system of unmonitored electronic access permits a curious juror to inflict.

THE PRIVACY AMENDMENTS TO THE FEDERAL RULES OF PROCEDURE

In December 2007, to address general concerns about privacy and confidentiality of information in the context of the new system of electronic court records, the Judicial Conference adopted amendments to the Federal Rules of Procedure.[104] The new rules establish general prohibitions of filing certain types of sensitive information in court records, such as social security numbers, taxpayer

---

101. John Schwartz, *As Jurors Turn to Web, Mistrials Are Popping Up*, N.Y. TIMES, Mar. 17, 2009, http://www.nytimes.com/2009/03/18/us/18juries.html?_r=1.

102. BLACK'S LAW DICTIONARY 1038-39 (8th ed. 2008) ("A pretrial request that certain inadmissible evidence not be referred to or offered at trial.").

103. *Whalen*, 429 U.S. at 607 (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

104. *See* H. COMM. ON THE JUDICIARY, 110TH CONG., FED. R. CRIM. P. 56-57 (2008).

identification numbers, birth dates, names of minor children, and financial account numbers.[105] New Civil Rule 5.2 provides that online public access is available only for the docket and for judicial decisions, while general access to the entire case file is available only to the parties and their counsel. If members of the public want to access the entire case file, access remains available upon request at the courthouse.[106] Finally, the rules broaden the availability of protective orders for "good cause" to permit "redaction of additional information" and the "limit[ing] or prohibit[ing] [of] a nonparty's remote electronic access to a document filed with the court."[107]

To understand these rules properly, it is necessary to understand the architecture of the CM/ECF system. There is a spectrum to the different levels of privileges. At one end of the spectrum, the default level, access is allowed to all members of the general public—to any person who obtains a user ID and a password—who agrees to pay the set fees from running reports and accessing documents. At the other end of the spectrum are the court records filed "under seal." When a document is filed under seal, computer privileges for online access are limited to the court, its staff, and those specifically identified persons who are given privileges to access the document.[108] Between these two ends of the spectrum are many different possible levels of access. The levels of access are determined by the hardware and software in the computer system, and by general legal rules. For instance, in some cases, a person who wishes to obtain online access to a court record merely has to enter an appearance in the case to obtain privileges to access the document remotely or request a copy of the document in the clerk's office. Social security and immigration cases are typically

---

105. *See, e.g.*, FED. R. APP. P. 25; FED. R. CRIM. P. 49.1; FED. R. BANKR. P. 9037; FED. R. CIV. P. 5.2.

106. FED. R. CIV. P. 5.2(c)(1)-(2) ("Unless the court orders otherwise . . . access to an electronic file is authorized as follows: the parties and their attorneys may have remote electronic access to any part of the case file, including the administrative record; any other person may have electronic access to the full record at the courthouse . . . but not any other part of the case file or the administrative record.").

107. FED. R. CRIM. P. 49.1(e); FED. R. BANKR. P. 9037(d); FED. R. CIV. P. 5.2(e); *see also* FED. R. APP. P. 25(a)(5) (stating that while on appeal, privacy will continue to be governed by the civil, criminal, and bankruptcy rules).

108. In some districts, in the context of a criminal case, when a defendant's pre-sentence report is filed under seal, computer privileges to access the document online are limited to the court, the prosecutors and the defense counsel—exactly the same persons who have the legal right to access the document were it filed in paper form. The public has neither the legal right nor computer privileges to obtain access to the document. Those who do have the right to access the document are under a legally binding duty to maintain the secrecy of the document's contents.

filed under this system. This level of privileges does not preclude access by a member of the public, but eliminates some of the conveniences of unrestricted online access, as well as entirely prohibiting *anonymous* access by non-parties.

To some extent, this intermediate level of access recreates some of the informal social restraints that provided an intermediate level of protection for sensitive information in the days of practical obscurity. In effect, it allows parties to opt into the same system that is presently used solely in the context of social security and immigration cases, where the cost of redacting large immigration files with sensitive financial information, or large social security files with medical records, would be prohibitively expensive for the people in these cases who typically were of lesser means. By expanding the availability of these intermediate forms of access to parties in all cases, the Conference appears to have decided that an intermediate solution should be available for sensitive information in any case.[109] If a document were limited by such a protective order, access would be available only after an explicit request for the document and after an automatically generated electronic notice was sent to the parties by email. This permits them to review the request for information, coordinate with the requesting party, and if necessary, object to the access, or substitute a redacted document in the public court file.[110]

The intermediate system of access, reflected in the new privacy rules, appears to comply with the constitutional and common-law right to public access. For all practical purposes it merely recreates certain aspects of the system of practical obscurity of the former paper based system—which, perforce, met constitutional muster. Under the case law, the right of public access is only implicated where there has been a denial of access to a judicial record *in toto,*[111] as when the underlying information is filed under seal.[112] So long as the public has some means of access to the underlying information, the constitutional right of public access is protected.

The rules represent an important step to addressing the

---

109. *See* Judiciary Privacy Policy, http://www.privacy.uscourts.gov/crimimpl.htm (last visited May 1, 2009) ("This Guidance explains the policy permitting remote public access to electronic criminal case file documents and sets forth redaction and sealing requirements for documents that are filed. The Guidance also lists documents for which public access should not be provided.").

110. *Id.*

111. BLACK'S LAW DICTIONARY 841 (8th ed. 2004) ("In whole; completely; as a whole.").

112. *See generally Nixon*, 435 U.S. 589; *Press-Enter*, 464 U.S. 501.

transformation that the introduction of the PACER CM/ECF system has brought to the ecosystem of judicial information management. However, many concerns remain unaddressed by the new rules. The rules place on the attorneys the primary burden of monitoring the system of online access.[113] They make it clear that it is counsel's responsibility to keep sensitive information out of court records, and to move for protective orders or sealing orders when it becomes necessary to file sensitive information in a case.[114] Requiring counsel to become more familiar with the technology and adopt better information management practices is an important step, but many lawyers formed their habits around the system of paper filings when "practical obscurity" protected their clients from disaster. Many attorneys and judges—particularly those of an older generation—rely on clerical staff for the actual interaction with the technology of the PACER CM/ECF system. As the audit by Public.Resource.Org revealed, the bad habits of a generation raised under "practical obscurity" has led to a rash of pleadings which violate the new rules; and as we have seen, the adversarial system has no natural tendency to impose negative consequences on the offending parties when the rights of non-represented third parties are affected.[115] Clearly, there is a need for more training of both the bench and the bar in the operation of these new rules.

It is also worth noting that the existing electronic filing system does not facilitate public access to core judicial records to the fullest extent possible, given available technology. Although there are no charges to access judicial opinions, one must still pay to conduct computerized searches to find them, reducing the effectiveness of the "free opinions" policy.[116] Accessing briefs in the context of dispositive motions also involves charges per page, although these pleadings represent "core" judicial records under the standards

---

113. Judiciary Privacy Policy, *supra* note 109 ("If a redacted document is filed, it is the sole responsibility of counsel and the parties to be sure that all documents and pleadings comply with the rules of this court requiring redaction of personal data identifiers. The clerk will not review filings for redaction.").

114. Lynn E. Sudbeck, *Placing Court Records Online*, S.D. L. REV 81, 90-92 (2006).

115. Public.Resource.Org, *supra* note 81.

116. PACER User Manual for ECF Courts 5, *available at* http://pacer.psc.uscourts.gov/documents/pacermanual.pdf. Written opinions are free if accessed through the hyperlink, which is located in both the reports and query areas of CM/ECF. One can search for specific reports by case number, party name, date range, case type, and nature of suit.

establishing the right to public access.[117] While a system of user IDs and passwords may be necessary to ensure the financial integrity of a self-financed system in the absence of a specific congressional appropriation, such a requirement also prevents access by powerful public search engines, such as Google. Of course, in some ways, this limitation may well be defensible, since it limits to some extent the danger, referenced above, of jurors "googling" the court file and gaining access to materials the juror is prohibited from seeing. However, there is no reason that most judicial opinions and briefs should not be searchable by Internet search engines, particularly after the conclusion of the underlying litigation. At the same time, the electronic filing system contains few if any privacy enhancing technologies—software programs that can automatically identify and flag sensitive information, such as social security numbers or other forms of sensitive information. Nor does it contain software programs that permit the easy and effective redaction of sensitive information in pleadings.[118] In sum, the existing federal electronic filing system does not appear to have been designed with the competing goals of facilitating access and protecting privacy in mind, and there remains considerable room for improvement in both of these two respects.

Another concern relates to the current terms and conditions of the PACER site license. The current site license places no conditions on what users who access court files do with the information; the only requirement is a willingness on the part of the user to pay the appropriate fees.[119] As we have seen, the existing common-law system of standards permits courts to limit access to court records for underlying purposes that are legitimate,[120] but the PACER system contains no such restrictions. The existing PACER technology places tremendous potential power in the hands of the administrative office of the courts. For instance, if a user were to abuse his or her privileges through repeated violation of the privacy rules, a simple and effective means to correct the problem would be to revoke the user's PACER ID and password. Likewise, potentially abusive secondary uses of

---

117. *Id.*

118. John Schwartz, *An Effort to Upgrade a Court Archive System to Free and Easy*, *supra* note 90 ("[One individual downloaded] thousands of documents in which the lawyers and courts had not properly redacted personal information like Social Security numbers, a violation of the courts' own rules. There was data on children in Washington, names of Secret Service agents, members of pension funds and more.").

119. PACER User Manual, *supra* note 116, at 4.

120. *Nixon*, 435 U.S. 589.

personal information, such as that involved in the operation of Web sites such as Whosarat.com, might also appear appropriately to result in similar administrative action.[121] However, nothing in the PACER site license currently addresses these scenarios or suggests a legal remedy for such misconduct.

Finally, there is one more potential area of concern with respect to the operation of the PACER system. The current system is funded by fees generated by users' accessing records.[122] At present, it appears likely that a substantial amount of the fees generated by the PACER system come from data aggregation companies.[123] These companies download massive amounts of information from the court system, process it, and sell it for a profit.[124] While companies such as Westlaw and Lexis have traditionally focused on the collection and distribution of core judicial information, such as court orders and opinions, it is unclear whether these companies limit themselves to this function. It appears that other bulk users of the PACER system include companies conducting background searches on individuals—with a particular focus on their criminal records or bankruptcy files. If all information is downloaded without restriction and processed for data mining purposes, it would appear that the court system should engage in some audit and oversight of such secondary uses of information, but none presently appears to take place. Of course, there is nothing per se improper about data mining public records, but the absence of any effort to date to study exactly what such companies do with the information they mine from court files is a source of some concern. As the PACER system has become increasingly dependent on fees generated by sales of data to these large aggregation companies, there arises a concern about potential conflicts of interest.

Over the last few years, it appears that PACER access fees have

---

121. PACER User Manual, *supra* note 116, at 2-4.

122. PACER User Manual, *supra* note 116, at 4.

123. The 2006 Judiciary Information Technology Fund Annual Report, *infra* note 125, lists fees collected from electronic public access as $62.3 million. Of course, Westlaw and LexisNexis have always been the courts' largest information customers. *See generally* GEORGE S. GROSSMAN, LEGAL RESEARCH: HISTORICAL FOUNDATIONS OF THE ELECTRONIC AGE (1994).

124. Thomson Reuters, the parent company to Westlaw, reported 2008 revenues of $3.5 billion and operating profits of $1.1 billion within their legal segment. THOMSON REUTERS, 2008 ANNUAL REVIEW 34 (2009). Reed Elsevier, the parent company to LexisNexis, reported that LexisNexis's revenues were $2.2 billion and operating profits were $809 million. REED ELSEVIER, 2008 ANNUAL REPORT AND FINANCIAL STATEMENTS 16 (2009).

generated a substantial surplus over the cost of operations.[125] I would respectfully suggest that some of these funds be allocated to addressing the various shortcomings of the system which so far have been identified in this paper. First, funds could be used to dramatically improve general public access to core judicial records, by making legal opinions and briefs searchable via the Internet. Second, funds could be used to purchase more "privacy friendly" technology in the system interface (for instance, software could be made available to flag and automatically redact sensitive material in pleadings before they are filed with the court). Finally, funds could be used to commission audits and other empirical investigations to determine more accurately the general level of compliance with existing privacy requirements, or examine more carefully the practices of data aggregation companies to confirm that secondary commercial uses of data are consistent with the core mission of the administration of justice. Such empirical studies would provide invaluable information for the Judicial Conference to use as it seeks to engage in a more informed rulemaking with respect to all these difficult issues.

THE NEW ECONOMICS OF ELECTRONIC INFORMATION

So far, we have been evaluating the system of electronic access against the background of the traditional measure which applied to the system of paper based records: how well it addresses the twin goals of facilitating public access while still protecting sensitive information in the court files. We have focused on the three traditional tools for regulating the creation and distribution of judicial information: better rules, better technology, and better training for those who use the system. However, technology and behavior must also be understood in the context of the economies of electronic information—for when judicial information becomes an aggregate system of data, it also becomes a commodity with a well-defined commercial value.

Economists Carl Shapiro and Hal R. Varian have conducted extensive studies of the economics of information management, and in particular the management of aggregate electronic information.[126] In

125. ADMIN. OFFICE OF THE U.S. COURTS: JUDICIARY INFO. TECH. FUND ANN. REP. 11 (2006) (showing revenues of the fund that oversees the PACER system, which over the years of 1996 to 2006, has operated with a surplus of over $735 million dollars.)

126. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1999).

their work, they have described how, when electronic information is aggregated in large computer systems, it takes on new and different properties from when it was first created.[127] Aggregate information operates under very different economic rules from individualized information. For instance, once aggregated in large databases, electronic information can be systematically crossed with other data to create an even more valuable economic resource.[128] Once it has been so processed, the cost to copy and disseminate the information has a marginal cost of zero.[129]

When compared to the familiar rules that apply to individualized communicative information, the rules that apply to aggregate data often operate in a counter-intuitive fashion—particularly with respect to competition. Thus, where increasing acquisition costs might raise costs for an individual user seeking information for ordinary communicative purposes, increasing acquisition costs for an established data aggregator, works as a barrier to entry for any potential competitor. The established data aggregator, operating with a zero marginal cost for subsequent distribution of information, can quickly recover any increase in acquisition costs. Competition is also diminished because of the phenomenon of "switching costs," where users of aggregate data are subject to a lock-in (both as a matter of training and technology) that restricts them from exploring other channels of access to the information.[130] In general, under the new economic rules governing the information economy, established aggregators often become immune to competition.

More importantly for our purposes, aggregation of information generates network effects or externalities. A network effect is the effect that one use of a good or a service has on the value of the product to other people. A telephone, for instance, has a positive network effect, because the more people who own telephones, the more valuable the telephone becomes to each owner. Aggregate bodies of public data have both positive as well as negative network effects. In facilitating greater public access to the system of judicial records, aggregate bodies of court data improve the public's understanding of and involvement in the system of justice, facilitating

---

127. *Id.*

128. *Id.* at 13.

129. *Id.* at 21 ("Information delivered over a network in digital form exhibits the first-copy problem in an extreme way: once the first copy of the information has been produced, additional copies cost essentially nothing.").

130. *Id.* at 11-12.

the critical public-private feedback loop which is critical to a healthy democratic society. At the same time, aggregate bodies of court data also increase the danger that sensitive information—information which is not a matter of legitimate public concern—will be found and used to the detriment of the data subjects—through identity theft or other dignitary privacy violations.

Given the importance of public access to information in court records for the health of a democracy, the standards of judicial information management have been traditionally hostile to any formal access restrictions on information in court files. This position made sense in the context of a paper-based judicial ecosystem, operating against a default of "practical obscurity." However, this ecosystem appears to have been dramatically altered by the introduction of electronic information. As judicial information has become aggregated in electronic form, the information in court files is no longer merely public information—it has become a public resource. As we have become aware of both the positive and negative network effects of the exploitation of this public resource, it is increasingly evident that this is a public resource which increasingly demands to be managed.

The different economic reality in operation of managing large bodies of public information has forced courts to treat aggregate information with different rules from those that apply to purely communicative information. In particular, courts have been willing to permit governments to place far greater limitations on commercial access to aggregate governmental records than when the underlying purposes of the access relate to the traditional individualized communicative purposes. Under *Los Angeles Police Department v. United Reporting Publishing Corp.*, the Supreme Court reviewed a state law, under which persons wishing access to police arrest records were required to:

> 'declare[ ] under penalty of perjury that the request is made for a scholarly, journalistic, political, or governmental purpose, or that the request is made for investigation purposes by a licensed private investigator . . . except that the address of the victim of certain crimes shall remain confidential. Address information obtained pursuant to this paragraph shall not be used directly or indirectly to sell a product or service to any individual or group of individuals, and the requester shall execute a declaration to that effect under

penalty of perjury.'[131]

The Court upheld these access restrictions. The Court's decision appears to recognize a broad governmental power to regulate acquisition of bodies of information when, in the aggregate, the information acquires commercial value—a commodity with a recognized value as property. Under the Court's analysis, government is not restricting access to information, it is only managing public property.[132] Therefore, as long as it does not attempt to limit the public's access to information—requested for proper use—the government has broad discretion to manage proprietary data belonging to the public as a public resource.[133]

Under the developing case law, it is unclear the extent to which the First Amendment will be held to protect the collection of and access to aggregated computer data for commercial purposes.[134] However, the line of reasoning in *United Reporting Publishing Corp.* appears to be correct.[135] Proprietary information, information that is protectable by law, is clearly different from individualized communicative information employed in public discourse. The right of public access may protect the public's right of access to public information, but it has never been held to give a private commercial entity a right to profit from a public resource.[136] As we have seen, courts have always retained the power to condition access to court records on the establishment of a legitimate purpose for such access.[137] In addition, under First Amendment jurisprudence, commercial speech[138] typically receives a lesser degree of protection

---

131. L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 35 (1999) (quoting CAL. GOV'T CODE ANN. § 6254(f)(3) (West Supp. 1999)).

132. *Id.* at 40.

133. *Id.*

134. Jennifer Bresnahan, *Personalization, Privacy, and the First Amendment: A Look at the Law and Policy Behind Electronic Databases*, 5 VA. J.L. & TECH. 8, ¶ 14 (2000), http://www.vjolt.net/vol5/issue3/v5i3a08-Bresnahan.html. (arguing that "the Court's early definitions [of commercial speech] leave no room for databases. Data by itself is not intuitively speech. The act of collecting data is not expressive, and it does not propose a commercial transaction.") (citing Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1799 (1995)).

135. *See United Reporting Publ'g Corp.*, 528 U.S. 32.

136. *Nixon*, 435 U.S. 589.

137. *Id.*

138. The conventional definition of commercial speech is "speech which does no more than propose a commercial transaction." Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976) (internal citations omitted). Later, the Supreme Court employed a broader sense of the term and defined commercial speech as

than speech relating to political, cultural, and other civic-minded activities.[139] With a better understanding of the economic and legal parameters applicable to the problem, we can now turn to examine a new model to address the special problems surrounding aggregate electronic court records.

A NEW MODEL TO ENFORCE OLD STANDARDS

We must begin with the clear goal that the standards for managing judicial information, which developed in the days of paper-based information, should continue to apply to the new world of electronic judicial information. Access to judicial information should be facilitated where it furthers the goals of oversight and civic involvement in the democratic process. Restrictions on such access may be upheld only when the underlying information is not a matter of legitimate public concern, or where there are compelling reasons to protect the information. However, while these general standards should continue to be enforced, the introduction of electronic aggregate information has exposed weaknesses in the enforcement model used in the past.

We have seen that when the standards of judicial information management were only enforced in the context of an adversarial system, information that was a matter of legitimate public concern could often be sealed by the agreement of the parties.[140] While a third party could always challenge the sealing order, the process could inappropriately shift substantial litigation costs to those seeking to access otherwise public information. We also saw that, for exactly the same reasons, private information that should have been filed under seal or otherwise protected, was often filed openly, either because it pertained to third parties who were not represented in the litigation, or because concerns of privacy were not the focus of the dispute between the parties.[141] While the paper-based system of "practical

---

an "expression related solely to economic interests of the speaker and its audience." Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 561 (1980).

139. *Cent. Hudson*, 447 U.S. at 566 ("For commercial speech to come within [the First Amendment], it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.").

140. *See* Sanson, *supra* note 59.

141. *See* Armstrong, *supra* note 62.

obscurity" shielded many of these dysfunctional information management practices from public scrutiny, it also benefitted those whose privacy interests might otherwise have been harmed.

While the new system of electronic information may provide less protection for privacy than in the past, it also provides new opportunities for the implementation of audit and oversight of its records—so that information management can take place far more efficiently than ever before. In a case on point, after courts were made aware of Public.Resource.Org's partial audit of the PACER system, many courts identified and removed offending pleadings. The courts then directed respective council to take steps in correcting their mistakes by resubmitting the documents with the private information redacted.[142]

The introduction of electronic judicial information has caused both positive as well as negative externalities associated with the medium of electronic information itself. On the positive side is the new-found ability to make core judicial records—legal opinions and briefs—available to a far larger audience than ever before, at a far lower cost. Increased access to court records offers the prospect of dramatically enhancing the understanding and involvement of ordinary citizens in the judicial process, considerably improving the political feedback loop. Unfortunately, to date, the PACER system has only partially utilized the full potential of this new electronic medium—core judicial records are still not available to be searched by Internet search engines. On the negative side, PACER has eliminated the natural system of privacy protection that existed in the days of "practical obscurity." Here, many problems might have been mitigated if the bad habits of a generation of attorneys trained in a paper-based system had not made the problem worse. The other potential negative externalities of aggregate electronic court information relates to the many possible secondary uses of electronic judicial information that has nothing to do with traditional oversight functions. Some secondary uses of aggregate court data may have legitimate social benefits, such as preparing credit and criminal background checks. However, other secondary uses—Whosarat.com most prominently among them—raise much more problematic questions.

---

142. *See, e.g.*, *Out of Sight, But Not Gone*, THE THIRD BRANCH: NEWSLETTER OF THE FEDERAL COURTS, Aug. 2008, http://www.uscourts.gov/ttb/2008-08/article06.cfm (reminding courts and attorneys to properly redact information).

As we have seen, even under a paper-based system, the adversary system was of limited effectiveness in enforcing the twin goals of judicial information management. While it arguably provided adequate protection for sensitive non-public information, it failed to facilitate true public access. Now that judicial information has become aggregate electronic data and operates under a new and unfamiliar set of economic rules, relying solely on an adversary system is no longer adequate. First, such a process provides no effective controls over the secondary uses of information by commercial data aggregators. Many commercial aggregators, such as those running background checks, adhere to principles of fair information practices set forth in such statutes as the Fair Credit Reporting Act.[143] However, a small group of aggregate data users, such as Whosarat.com, appear to act in utter disregard of any of these well established social standards. Furthermore, after privacy violations occur in the primary body of judicial information, and are identified and corrected, there is nothing requiring aggregate secondary users of data to enter similar corrections to their now private databases. In sum, the adversary system seems ill equipped to address a series of new problems associated with the enforcement of traditional standards of judicial information management in the context of electronic judicial information.

Looking back in time, there appears to be an interesting and potentially useful analogy with the history of environmental law. Prior to the twentieth century, most questions involving pollution were addressed in the context of disputes between private parties, largely under the common-law doctrine of nuisance.[144] In the twentieth century, widespread industrialization began to harm far more people than could be adequately addressed through the nuisance doctrine.[145] Thus, the legal system was forced to supplement the common-law nuisance doctrine with a legal approach that involved the use of specialized government agencies and experts. The agencies could conduct scientific testing and propose rules, reflecting a more systematic cost-benefit analysis of the overall effect of certain environmentally sensitive actions on the overall social welfare.[146]

---

143. 15 U.S.C. § 1681 (2006).

144. *See* Andrew Jackson Heimert, *Keeping Pigs Out of Parlors: Using Nuisance Law to affect the Location of Pollution*, 27 ENVTL. L. 403, 406-08 (1997).

145. *Id.*; *see also* Richard O. Faulk & John S. Gray, *Alchemy in the Courtroom? The Transmutation of Public Nuisance Litigation*, 2007 MICH. ST. L. REV. 941, 953 (2007).

146. Faulk & Gray, *supra* note 145, at 954.

While the rights-based nuisance law continued to operate, it was supplemented by a complementary system where government agencies could also address the problem from a more comprehensive point of view.[147] For the first time, the management of access to resources could be addressed, not merely from the narrow point of view of the two individuals engaged in a dispute over the resource, but from the point of view of the entire ecosystem. In a similar way, the problems that have been identified with the system of electronic judicial information suggest that we look to the earlier model of environmental protection law. Some form of audit and oversight capacity now seems to be needed to address the problems of the management of electronic information from the point of view of the judicial "ecosystem" rather than merely from the individual litigant.

Large aggregate electronic databases benefit society through traditional communicative and informative functions, but they have also taken on the characteristic of commodities and become an important proprietary resource. However, if the work product of an agent belongs to the principal and the courts are agents of the public, then the aggregate data generated by the courts clearly belongs to the public, not to those with an interest in commercial exploitation of the resource.[148] The basic question is how the public can maximize the positive effects of disclosure of the public information while limiting the negative effects to individual privacy. It appears the answer to this question may necessarily involve placing certain conditions on those who wish to exploit the public information resource if that resource is to be managed truly in the public interest.

Again, there is a useful analogy in the context of government owned environmental resources—minerals located in public lands. Governmental agencies grant permits or patents to extract such minerals after a cost-benefit analysis shows that the value to the public of extracting these minerals outweighs the negative externalities—typically pollution of land and groundwater—that the mining activity

---

147. *Id.* at 954-55.

148. *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matter connected with the agency relationship"); RESTATEMENT (THIRD) OF AGENCY § 8.02 ("An agent has a duty not to acquire a material benefit from a third party in connection with transactions conducted or other actions taken on behalf of the principal or otherwise through the agent's use of the agent's position"). *But see* INS v. Associated Press, 248 U.S. 215, 237 (1918) ("The question, whether one who has gathered general information or [data] at pains and expense for the purpose of subsequent publication . . . has such an interest in its publication as may be protected . . . has been raised many times . . . .").

may generate. In the context of environmental reviews, federal and state agencies are to consider all the potential costs and benefits of any significant environmentally disruptive activity. Surely some similar systematic cost-benefit analysis should productively take place with respect to the information practices and policies within the judicial system. While the Judicial Conference has attempted to pass privacy rules to address perceived threats, such rulemaking activities now appear to take place largely in the dark—without the benefit of any empirical analysis on how the current system actually achieves the twin goals of privacy and publicity. Likewise, empirical work would allow for a better understanding of the ramifications of secondary uses of aggregate judicial information by data mining companies.

In this context, much can be done to enhance the twin goals of privacy and publicity that was not technically feasible under a paper-based system. With proper management, the greater accessibility of a system of electronic access appears to be able to provide for more effective protections for privacy, not less. For instance, in the recent audit conducted by Public.Resource.Org, free open-source software programs were used to identify privacy violations in court filings and the identities of the violators were provided to the respective clerks in each district. Clerks responded by removing the documents from public access and then ordered counsel to file corrected versions of the pleadings and other documents.[149] In this case, paradoxically, by making court records more accessible to the *public*, a positive feedback loop was created that strengthened the ability of the judicial system to enforce the laws protecting *privacy*.[150]

As we have seen, the enhanced ability to conduct audits and oversights of electronic information is evident in the identification of "judicial kudzu"[151] and the exposure of the widespread violations of sealing of settlements.[152] Obviously, to maximize the benefits of the public information and minimize the privacy problems, regular audit and oversight activities should take place. The most natural public body to be tasked with conducting such audit and oversight functions as well as empirical analysis, would appear to be the Administrative

149. Letter from Carl Malamud, President & CEO, Public.Resource.Org, to Lee H. Rosenthal, Chair, Comm. on Rules of Practice and Procedure (Oct. 3, 2008), http://public.resource.org/scribd/7512580.pdf.

150. *Id.*

151. *In re* Sealing & Non-Disclosure of Pen/Trap 2703(D) Orders, 562 F. Supp. 2d 876.

152. Armstrong, *supra* note 62.

Office of U.S. Courts, presently charged with running the PACER system. Given the increased eagerness on the part of public interest organizations, like Public.Resource.Org, to point out the failures of the court system—and the Administrative Office in particular—in the context of judicial information management, there presently appears to be little doubt that the Administrative Office will increasingly need to undertake these information management responsibilities. Some of the tactics of such non-profit organizations—including an apparent hack[153] of large portions of the PACER system and the subjecting of the alleged shortcomings of the Administrative Office to a so-called Internet "wall of shame" are certainly distasteful. However, these organizations do appear to have managed to create an interesting political feedback loop and this can only benefit the judicial information management so essential to a healthy democracy. Whatever system of regulation is ultimately adopted—an organized one managed by the Administrative Office or a chaotic one controlled by Internet vigilantes—it appears to be essential for the courts to have some mechanism to "weed the kudzu" on what is both metaphorically and literally a public common. There is no reason to abandon the traditional adversary system, but that traditional system needs to be supplemented by some non-adversarial administrative system which can perform a more systematic audit and oversight function of the aggregate data.

A public body such as the Administrative Office could also address the question whether private extraction activities by large data users result in greater social benefits than in negative externalities. This should be relatively easy for companies such as Westlaw and Lexis to establish—since they serve a well understood and traditional role of facilitating better understanding and appreciation of the legal system—consistent with the core values of public access. However, in framing the policies which apply to such aggregate commercial users of this judicial database, the Judicial Conference should also keep in mind the importance of facilitating

153. By "hack," I mean only a non-consensual access to and downloading of data from a computer system belonging to another. I express no opinion on the question whether such a "hack" constitutes an unauthorized access in violation of the Computer Fraud and Abuse Act. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (1988)). For a detailed analysis of the circumstances when non-consensual access to a public computer should constitute an actionable computer trespass, see Peter A.Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1495 (2007).

broad public access, and frame its rules to assist the many non-profit bodies who are now attempting to provide core judicial information free of charge. Given the tremendous commercial advantages the economic laws of aggregate electronic information provide established commercial data uses, facilitating access to aggregate court data by other competitive data aggregators will only benefit the public.

All companies providing data aggregation services, however, should be required to adhere to the same principles of information management as apply to the courts. Thus, they should be required by contract to "scrub" their data to identify and remove social security numbers before they republish the information for public distribution. Likewise, upon the identification of any such rule violations, such companies should be required to report them back to the local clerks' offices so that the responsible attorneys can be contacted and the privacy problem corrected. The Administrative Office could also place other requirements on data aggregate companies when they contract for access to the PACER system data. To the extent that such data mining companies engage in purely secondary disclosures of information unrelated to the administration of justice, they should probably be required to adhere to well established principles of fair information practices which presently apply to credit reporting companies and many other large aggregate commercial data compilers. Contracts with such data aggregators should provide for adequate audit and oversight capacity so that actions inconsistent with the principles of information management can be addressed swiftly, either by framing new rules and policies through policy established by the Judicial Conference, by contract negotiated by the Administrative Office, or by enforcement action—revoking the contractual license of the company to engage in data mining activities.

CONCLUSION

There are some obvious conclusions that can be drawn from this new administrative model. The aggregate data in court files should be used to promote better management of the judicial system and to promote greater understanding and opportunity for civic involvement in the judicial process. It should be managed to reduce the cost of access to core judicial records, to facilitate empirical research into operation of the judicial system, and to enhance positive network effects of the information. In general, information management policy should focus on encouraging public participation in the judicial

process and discouraging practices which undermine the administration of justice. To that end, restrictions on individual access to core judicial records should continue to be narrow with a strong presumption for transparency. Likewise, aggregate commercial data users and non-commercial data users should both be encouraged, to the extent their use is in the public interest. At the same time, as a public resource, electronic data in court files should be managed to minimize negative externalities. These negative externalities include the loss of individual privacy, loss of confidential business information, and unauthorized secondary uses.

Nixon affirmed the principle that courts have broad power to manage judicial information.[154] In an age when information has become electronic, this principle needs to be invigorated. General requirements for responsible information use should be explicitly incorporated into the PACER site license, which at the moment only requires that one agree to be financially responsible for the access charges.[155] The most difficult challenge facing the system of information management today is addressing intentional misconduct of using ostensibly collected public information from the court system—the Whosarat.com type problem. It appears that such intentional misconduct, whether committed by aggregators or individuals, should result at a minimum in the loss of access privileges—the cancellation of their user ID and password—after a clear warning prohibiting such misconduct is included in the terms and conditions of the PACER site license.

The process of administering judicial records should focus on better utilization of the traditional tools of rulemaking, technology, and training. In framing new rules, in designing new technology, and in promoting better training, the courts need to understand the new economic rules which apply to electronic data. Rulemaking is blind without empirical information; technology cannot be designed without a clear understanding of the problem that needs to be solved, and training is of limited value if it does not incorporate the best practices learned from experience.

Finally, as we have seen, none of these potential solutions—the framing of better rules, the design of better technology, and the

---

154. *Nixon,* 435 U.S. at 598.

155. PACER Service Center, Acknowledgment Of Policies And Procedures (06/24/2008), https://pacer.psc.uscourts.gov/psco/cgi-bin/regform.pl (last visited May 1, 2009) ("By registering for a PACER account, I assume responsibility for all fees incurred through the usage of this account.").

promotion of better training—arise in the context of the ordinary course of litigation. They are the types of developments that typically arise in the context of an administrative agency. Such agencies presently exist. The Administrative Office has the power to engage in audit and empirical analysis; the Judicial Conference has the power to formulate rules; and the Judicial Center has the responsibility to fashion better training programs. The solutions are multifaceted and interrelated; however, they all require new and creative ways both to expand opportunities to enhance the public benefit from the rich resource of electronic judicial information as well as to limit the many potential detriments of improper secondary use of such information. The solution is a coordinated program that uses all the tools available—rules, training, and technology—to further the twin goals of public access and privacy within judicial information management. Such a program would not change the traditional standards set out in the common law, but would merely better enforce those standards in an age of electronic information, always cognizant that courts are, and have always been, managers of a rich and important public resource.