Washington Law Review

Volume 79
Number 1 *Symposium: Technology, Values, and the Justice System*

2-1-2004

Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information

Peter A. Winn
University of Washington School of Law

ONLINE COURT RECORDS: BALANCING JUDICIAL ACCOUNTABILITY AND PRIVACY IN AN AGE OF ELECTRONIC INFORMATION

Peter A. Winn*

I. INTRODUCTION

Francis Bacon said that knowledge is power.[1] He could just as easily have identified power with the control of information. As Bacon—the lawyer, judge, and Lord Chancellor—well knew, courts were and still are the pre-eminent information systems—institutions that process information and translate it into the exercise of power; in the case of courts, by rendering judgments. Later Enlightenment thinkers such as Cesare Beccaria well understood the connection between judicial information and power, and argued forcefully that all trials should be public.[2] Publicity was viewed as a check against the misuse of judicial power, tending to limit unfair (or at least unpopular) prosecutions by the rulers of a society, as well as increasing public respect for the legal system.[3] Of course, while the legal system has inherited from the Enlightenment a presumption of openness, that presumption has always been limited when unfair publicity, itself, threatens to become an

* Senior Fellow, University of Washington School of Law; Lecturer, Graduate Studies Department, University of Melbourne School of Law; Assistant U.S. Attorney, U.S. Department of Justice. The views expressed in this Article are the author's personal views and should not be interpreted as reflecting the position of the U.S. Department of Justice. The author wishes to express his gratitude to the following persons for their comments: Judge Donald Horowitz, Judge Dennis Michael Lynn, Dan Solove, Robert Ellis Smith, Gregory Silverman, and Katie Simon.

1. *See* JOHN BARTLETT, FAMILIAR QUOTATIONS 111 (Christopher Morley & Louella D. Everett eds., 11th ed., Little, Brown & Co. 1940) (1882) (attributing quote "Nam et ipsa scientia potestas est" (knowledge is power) to Francis Bacon in his work *Meditationes Sacrae, De Haeresibus*). The use of the term *potestas* by Bacon was no accident. *Potestas* is used to denote legal power or control, and Bacon, in his professional life, served in many different judicial capacities, including that of Lord Chancellor.

2. CESARE BECCARIA, ON CRIMES AND PUNISHMENTS 22–27, 99 (Henry Paolucci trans., Bobbs-Merrill Co. 1963) (1764).

3. "Let the verdicts and proofs of guilt be made public, so that opinion, which is, perhaps, the sole cement of society, may serve to restrain power and passions; so that the people may say, we are not slaves, and we are protected—a sentiment which inspires courage and which is the equivalent of a tribute to a sovereign who knows his own true interests." *Id.* at 22.

instrument of oppression. Experience teaches us that at times, open judicial proceedings can ensure, rather than prevent, the abuse of judicial power, can create unacceptable risks of a miscarriage of justice, and can cause unnecessary harm to the safety and privacy of individuals.

This Article examines the traditional balance courts have reached between the disclosure of information generated by the judicial process and the need at times to limit the disclosure of that information. The Article then examines how this traditional balance is upset when judicial information is placed online. The Article argues that as courts adapt to a world of electronic information, new rules and practices must be established to maintain the policies underlying the traditional balance. While there must continue to be a presumption of openness, courts must limit the disclosure of judicial information when it threatens the effective administration of justice and when necessary in order to protect the safety and privacy of individuals participating in the judicial process.

A. Access to Information in Criminal Proceedings

The presumption of openness of judicial proceedings is embodied in the Sixth Amendment to the U.S. Constitution, which guarantees the accused in every criminal case the right to a public trial.[4] In the words of Justice Hugo Black, the Sixth Amendment is "a safeguard against any attempt to employ our courts as instruments of persecution. The knowledge that every criminal trial is subject to contemporaneous review in the forum of public opinion is an effective restraint on possible abuse of judicial power."[5]

At the same time, the presumption of openness is limited when it interferes with the fair and impartial administration of justice, or threatens the safety or the reasonable expectation of privacy of the participants in the judicial process. Thus, there is no general public right of access to federal grand jury proceedings,[6] which under Federal Rule

4. U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.").

5. *In re* Oliver, 333 U.S. 257, 270 (1948).

6. *See* United States v. John Doe, Inc. I, 481 U.S. 102, 109 n.5 (1989); United States v. Sells Eng'g, Inc., 463 U.S. 418, 424 (1982); Douglas Oil Co. v. Petrol Stops N.W., 441 U.S. 211, 218 (1979); United States v. Procter & Gamble Co., 356 U.S. 677, 681–82 (1958).

of Criminal Procedure 6(e) are conducted in secrecy.[7] This rule protects the reputations of individuals if they are innocent, and limits their opportunities for obstruction of justice if they are guilty.[8] Applications for search warrants and for electronic surveillance nearly always take place in secret.[9] Finally, judges have the discretion to close the courtroom to public spectators when necessary to achieve a fair trial—for instance, when faced with witness intimidation[10] or other disruption to the judicial proceedings.[11] The Sixth Amendment confers no special benefits on the press,[12] and the right to a public judicial proceeding may be waived by a defendant—one who, for instance, may wish to limit the risk that he may be harmed if his counterparts learn of an agreement to cooperate with the government's investigation. Many criminal court records are prepared and maintained entirely in secret. For example, there is no right of public access to pre-sentence reports that are prepared by the federal probation office and contain extremely sensitive information about criminal defendants' health, mental condition, family history, and finances.[13]

In addition to the Sixth Amendment right of a criminal defendant to a public trial, the U.S. Supreme Court has also recognized a limited right of access to criminal judicial proceedings under the First Amendment of the Constitution.[14] In *Richmond Newspapers, Inc. v. Virginia*,[15] the Court held that "[i]n guaranteeing freedoms such as those of speech and press, the First Amendment can be read as protecting the right of everyone to attend trials so as to give meaning to those explicit guarantees."[16]

---

7. FED. R. CRIM. P. 6(e).

8. *See, e.g., Sells Eng'g, Inc.*, 463 U.S. at 424 ("Grand jury secrecy, then, is 'as important for the protection of the innocent as for the pursuit of the guilty.'" (quoting United States v. Johnson, 319 U.S. 503, 513 (1943))).

9. *See, e.g.*, 18 U.S.C. § 2518(8)(b) (2000) (providing for the sealing of applications for electronic surveillance); The Times Mirror Co. v. United States, 873 F.2d 1210, 1216–18 (9th Cir. 1989) (refusing to disclose affidavits submitted in support of a search warrant application because of reputational and privacy concerns of yet unindicted persons named in the affidavit).

10. *See, e.g.*, United States v. Sherlock, 962 F.2d 1349, 1357–59 (9th Cir. 1989); Bruno v. Herold, 408 F.2d 125, 127–28 (2d Cir. 1969); State v. Rusin, 568 A.2d 403, 405–06 (Vt. 1989).

11. *See* United States v. Akers, 542 F.2d 770, 772 (9th Cir. 1976).

12. Nixon v. Warner Communications, Inc., 435 U.S. 589, 610 (1978) (citing Estes v. Texas, 381 U.S. 532, 583 (1965)).

13. *See* United States Dep't of Justice v. Julian, 486 U.S. 1, 12 (1988); United States v. Corbitt, 879 F.2d 224, 237 (7th Cir. 1989).

14. U.S. CONST. amend. I.

15. 448 U.S. 555 (1980).

16. *Id.* at 575; *see also* Press-Enter. Co. v. Superior Court, 478 U.S. 1, 11–12 (1986).

Nevertheless, the right of access to the courts is not absolute. Courts continue to have the duty to balance the presumption in favor of public access against other interests that may justify restricting access. These include the possibility of prejudicial pretrial publicity; the danger of impairing law enforcement or judicial efficiency; and the protection of the legitimate privacy interests of litigants and other persons, such as witnesses, victims, and jurors.[17]

B. Access to Information in Civil Proceedings

In the context of civil proceedings, it has been held that the Sixth Amendment does not support a general constitutional right of access.[18] Nevertheless, for many of the same underlying reasons supporting public access to criminal proceedings, the U.S. Supreme Court has recognized a common law right "to inspect and copy public records and documents, including judicial records and documents."[19] In *Nixon v. Warner Communications, Inc.*,[20] Justice Powell, writing for the Court, articulated the limits on this common law right of access: "It is uncontested, however, that the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes."[21]

In *Nixon*, the Court considered whether the press could obtain copies of tape recordings of conversations between former President Nixon and various members of his staff that had been introduced into evidence in the trials of these staff members.[22] Although these tape recordings had been played in public during the trial, until then the press had only been able to obtain transcripts of the tapes.[23] The Court held that after the conclusion of the judicial proceedings, Nixon's interest in privacy outweighed the common law right of the press to have copies of the

17. *See* Globe Newspapers Co. v. Superior Court, 457 U.S. 596, 607–10 (1982); Ctr. for Nat'l Sec. Studies v. United States 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, 71 F.3d 1044, 1047–50 (2d Cir. 1995).

18. *See* Satterfield v. Edenton-Chowan Bd. of Educ., 530 F.2d 567, 573 (4th Cir. 1975).

19. Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978).

20. 435 U.S. 589 (1978).

21. *Id.* at 598.

22. *Id.* at 589.

23. *Id.*

tapes, particularly when the only purpose that could be cited for the release of the copies was their potential for commercial exploitation.[24]

As stated by the Court in *Nixon*, the underlying purpose of the common law right of access is 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."[25] In another leading case, *In re Continental Illinois Securities Litigation*,[26] the U.S. Court of Appeals for the Seventh Circuit stated that the purpose of the common law right of access is to allow the citizenry to "monitor the functioning of our courts, thereby insuring [sic] quality, honesty, and respect for our legal system."[27] This rationale, of course, comes directly from Enlightenment thinkers such as Beccaria.[28]

C. *Balancing Access and Privacy*

Understanding the rationale for public access to judicial proceedings, however, also reveals the limitations of that rationale. These limitations become evident when courts must balance the presumption of the openness of judicial proceedings against the need to keep certain types of information confidential—in particular, sensitive personal information. Courts tend to favor public access when the underlying purpose of public access is to ensure the integrity of the judicial process.[29] On the other hand, courts tend to protect personal information when the purpose of access is not related to facilitating public scrutiny of the judicial process, but to exploiting information in judicial records for commercial or other purposes unrelated to public oversight of the judicial system.[30] The balance worked out by the courts bears a close analogy to the concept of fair information practices as applied in the context of the federal Privacy Act[31] and the Freedom of Information Act (FOIA).[32] Under this body of law, an agency collecting personal

24. *Id.* at 602.

25. *Id.* at 598 (citations omitted).

26. 732 F.2d 1302 (7th Cir. 1984).

27. *Id.* at 1308.

28. *See supra* note 2 and accompanying text.

29. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 575–78 (1980); *In re* Cont'l Ill. Sec. Litig., 732 F.2d 1302, 1313–16 (7th Cir. 1984).

30. *See, e.g.*, Globe Newspapers Co. v. Superior Court, 457 U.S. 596, 607–10 (1982); *In re* The Knoxville News-Sentinel Co., 723 F.2d 470, 474–78 (6th Cir. 1983).

31. 5 U.S.C. § 552a (2000).

32. 5 U.S.C. § 552 (2000).

information for one purpose is not ordinarily permitted to use that information for a different unrelated purpose.[33] Public access to sensitive personal information about individuals is generally prohibited unless it serves the purpose of ensuring accountability in government.[34] In a very similar manner, the cases involving access to court records evidence a careful effort to balance the presumption of public access and the privacy rights of individuals.[35] In framing this balance, courts are sensitive to protect not only the personal privacy of litigants, but also the harm that can come to others, such as witnesses, victims, jurors, and other third parties, who may have no control over the information so disclosed.

The sensitivity shown by court decisions in balancing access and privacy in the context of judicial records reflects the large body of judicial experience addressing questions of privacy in other contexts. Courts are accustomed to balancing the social benefits from the disclosure of personal information against the risk of harm that such disclosure may cause the individuals who are so identified. For example, in *Nixon v. Administrator of General Services*,[36] the U.S. Supreme Court determined that President Nixon had a constitutional privacy interest in records of his private communications with his family, but not in records of his official duties.[37]

Courts have also shown particular sensitivity in protecting personal *health* information from disclosure. In *Whalen v. Roe*,[38] the U.S. Supreme Court recognized that because of its great sensitivity, personal health information is protected under a constitutional right to information privacy.[39] However, in *Whalen*, the Court permitted the collection of this personal health information for purposes of public health and safety when there were strong and effective assurances that the information so collected would be kept confidential.[40] In these cases,

33. *See id.* §§ 552–552a.

34. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 772–73 (1989); *see also* United States Dep't of State v. Wash. Post Co., 456 U.S. 595, 600–03 (1982).

35. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 775; *Wash. Post Co.*, 456 U.S. at 600–01.

36. 433 U.S. 425 (1977).

37. *Id.* at 449, 457–59.

38. 429 U.S. 589 (1977).

39. *Id.* at 598–600.

40. *Id.* at 607 (Brennan, J., concurring).

courts have excelled in demonstrating a great capacity for careful and nuanced balance.[41]

In the leading case of *Westinghouse Electric Corp. v. United States*,[42] the U.S. Court of Appeals for the Third Circuit set out five factors that must be considered in determining the appropriate constitutional balance between personal privacy and a governmental interest in disclosure of health records: (1) the type of health record requested and the type of health information it contains, (2) the potential for harm in any subsequent non-consensual disclosure of the information, (3) the injury from disclosure to the relationship in which the record was generated, (4) the adequacy of safeguards to prevent unauthorized disclosure, and (5) the degree of need for access.[43] Relying on the *Westinghouse* test, some courts have found a constitutional tort under 42 U.S.C. § 1983[44] for the improper disclosure of health information by state government officials.[45] On the other hand, in *Doe v. Southeastern Pennsylvania Transportation Authority*,[46] the same appellate court found that the disclosure of medical records to the administrator of a health benefit plan was not actionable.[47]

The pragmatic reasons supporting the need for public access (for example, the need to assure credibility and accountability of the judicial system) are typically balanced against the pragmatic reasons supporting the need to restrict public access (for example, protecting the rights of litigants to a fair trial, protecting the rights of individuals to privacy, and protecting individuals from harm caused by misuse of their personal information). While courts are vigilant in protecting the public right of access when it is consistent with ensuring the credibility of the judicial

41. *Nixon*, 433 U.S. at 456; *Whalen*, 429 U.S. at 605–06.

42. 638 F.2d 570 (3d Cir. 1980).

43. *Id.* at 578.

44. 42 U.S.C. § 1983 (2000) (providing a civil cause of action against states for the "deprivation of any rights, privileges, or immunities secured by the Constitution and laws").

45. Doe v. Borough of Barrington, 729 F. Supp. 376, 378, 382 (D.N.J. 1990) (finding a violation of the plaintiff's constitutional right to privacy when a police officer who had arrested the plaintiff disclosed to the plaintiff's neighbor the fact that the plaintiff had HIV); Woods v. White, 689 F. Supp. 874, 876 (W.D. Wis. 1988) (holding that the constitutional right of privacy extended to the fact that a prison inmate had tested positive for HIV where allegedly disclosed by prison medical personnel to non-medical staff and other inmates), *aff'd without opinion*, 899 F.2d 17 (7th Cir. 1990).

46. 72 F.3d 1133 (3d Cir. 1995).

47. *Id.* at 1143.

system,[48] they are also quick to protect individuals from the exploitation of their personal information when it bears little relationship to ensuring the integrity of the judicial process.[49] This common law and constitutional balance, carefully worked out on a case-by-case basis over the course of many years, represents the finest form of judicial lawmaking. While a system that relies on the discretion of judges sometimes runs the risk of occasional inconsistent decisions,[50] by and large, courts have shown that they are capable of exercising their discretion to carefully weigh competing interests, and their decisions show great nuance, factual subtlety, and legal imagination.

II. ELECTRONIC JUDICIAL RECORDS: HOW TO MAINTAIN BALANCE

A. The Move from Paper Records to Electronic Records

When courts move from the world of paper judicial records to the world of electronic judicial records, they must confront the same issues underlying the information revolution throughout our society. The revolution in the use of electronic information has seen the capacities of hardware, software, and communications networks continually increase and their costs continually decrease. This has permitted information to be used in ways that were previously impractical. In the law, the conversion from paper to electronic judicial records has provided courts and attorneys the opportunity to obtain substantial benefits in the operation of the legal system.[51] The conversion also offers the public the opportunity to better understand and appreciate the judicial process.

However, as our legal system undergoes the transformation to a system of electronic judicial records—with all its substantial benefits—it

48. *See supra* notes 25–29 and accompanying text.

49. *See supra* notes 21–24, 30 and accompanying text.

50. Professor Solove, for instance, takes the position that the current system does not provide enough protection for individual privacy. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1154–59 (2002).

51. The federal electronic case filing system offers the following benefits: 24-hour access to case files over the Internet, ability to file pleadings electronically with the court, automatic e-mail notice of case activity, ability to download and print up-to-date documents directly from the court system, no waiting in line, expanded search and reporting capacities, the elimination of the cost of expensive courier services, and an overall reduction in the physical storage space needs of the courts. *See* Federal Public Access to Court Electronic Records ("PACER") system website, *at* http://pacer.psc.uscourts.gov/cmecf (last visited Jan. 5, 2004).

is critical to ask how the advantages of public access are to be balanced against the other competing policies that have served to limit access in the past, such as maintaining the integrity of the judicial system and protecting individuals from invasion of their privacy and misuse of their personal information. It is temptingly easy to assume that if one applies the same set of rules to electronic judicial records that was applied in the past to paper records, it will result in the same balance between the various competing policies. Unfortunately, this is not the case. The assumption of parity represents a serious misunderstanding of the differences between paper records and electronic records. When the same rules that have been worked out for the world of paper records are applied to electronic records, the result does not preserve the balance worked out between the competing policies in the world of paper records, but dramatically alters that balance. It shifts the balance away from individual privacy, producing little if any benefit on the side of judicial accountability.

In this context, to assert that electronic judicial records should be placed under the same rules as paper records is nothing more than to advocate for the free flow of information at the expense of the many other competing values. This position appears to be driven more by an abstract philosophy about the importance of the free flow of information than a study of the actual historical experience of courts. That experience forces us to recognize that the flow of information can have very serious and concrete consequences—not all of them beneficial to the effective administration of justice or the protection of the dignity and security of individuals. For instance, the unrestricted shift to electronic court records permits the type of commercial exploitation of judicial records that courts have traditionally eschewed. Such commercial exploitation of judicial records harms the privacy of litigants with virtually no corresponding benefit to the administration or the accountability of the justice system. Furthermore, if the shift from paper to electronic court records takes place without appropriate safeguards, we will celebrate the abstract value of the free flow of judicial information at the cost of the privacy and security of litigants and other participants in the judicial system. They will lose not only their interest in privacy—their identities will be subject to potential misuse by thieves, and their children may be exposed to sexual predators. Instead of increasing social respect for the judicial system, unrestricted access to court records will undermine the respect and confidence the courts in this country have traditionally enjoyed.

B. The "Practical Obscurity" of Paper Records also Protects Privacy

In the past, paper-based records, while technically public, continued to retain a high degree of "practical obscurity."[52] This was true because the retrieval of paper records involved costs that do not attend the retrieval of electronic records. In the world of paper judicial records, personal information could be open to the "public" in the sense that it could be accessed by any member of the general public, but the costs of retrieval limited access as a practical matter. Only those with a relatively strong interest in the information would take time out of their day, wait in line at the clerk's office, fill out the necessary forms, and pay the necessary copy charges. Once judicial records go online, however, computerized compilers can search, aggregate, and combine the information with information from many other public filings to create a profile of a specific individual in a matter of minutes, at minimal cost. Information in many different locations can be combined and aggregated in ways that previously were impossible, permitting entirely new uses of the information that could never have been intended before. These search, aggregation, and bulk dissemination capabilities can handle major magnitudes of information, take little time, and have minimal cost. While there may be social benefits from this increased access to personal information, electronic access will also mean that court records can be commercialized in ways they have never been before.[53]

Paper records also exist in time and space differently from electronic records. Paper records—like human beings—are organic. As such, they experience a natural progression of decay and change. Over time, paper-based information accumulates and grows old and must be cleared away to make room for the new. The "practical obscurity" of old records generates an expectation of privacy that has been recognized as legitimate by common law courts.[54] The concept of practical obscurity developed by federal courts in the context of FOIA cases also recognizes that the passage of time may actually increase the privacy interest at stake when disclosure would revive information that was once public

52. *See* United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762, 780 (1989).

53. *See* Solove, *supra* note 50, at 1149–52.

54. *See, e.g.*, Briscoe v. Reader's Digest Ass'n, Inc., 483 P.2d 34, 36, 44 (Cal. 1971) (holding that a truthful publication of an eleven-year old criminal conviction constitutes a valid cause of action for invasion of privacy); Melvin v. Reid, 297 P. 91, 91, 93 (Cal. Ct. App. 1931) (holding that a movie truthfully depicting plaintiff's previous life as a prostitute many years earlier constitutes a valid cause of action for invasion of right to pursue happiness).

knowledge but has long since faded from memory.[55] On the other hand, electronic records are inorganic; they do not grow old, get moved to warehouses, or eventually get destroyed. They continue to exist, potentially forever. In an age of electronic information, a serious question arises as to whether a rehabilitated criminal will be allowed to put his past behind him,[56] whether a former prostitute who was acquitted of a murder charge will ever be allowed to forget it,[57] or whether a victim of a sexual assault will be allowed to heal her wounds and not be victimized once again by reminder and new public disclosure many years later.[58]

C. *The Dark Side of Online Access*

In this context, it may be helpful to examine other examples of online information. Putting consumer credit information online has permitted credit-reporting agencies to aggregate huge amounts of personal financial information. While this has created unprecedented access to consumer credit in the United States, it also has spawned a new type of crime—identity theft. Identity theft is now reaching epidemic proportions and has left millions of innocent victims little, if any, means of redress.[59] In health care, the electronic revolution has created new opportunities for advances in medicine, but it also has begun to

---

55. *See, e.g.*, *Reporters Comm. for Freedom of the Press*, 489 U.S. at 767 ("[O]ur cases have also recognized the privacy interest inherent in the non-disclosure of certain information even when the information may have been at one time public."); Rose v. Dep't of the Air Force, 495 F.2d 261, 267 (2d Cir. 1974) ("[A] person's privacy may be as effectively infringed by reviving dormant memories as by imparting new information."), *aff'd*, 425 U.S. 352 (1976).

56. *See Briscoe*, 483 P.2d at 36.

57. *See Melvin*, 297 P. at 91.

58. *See* Midland Publ'g Co., Inc. v. Dist. Court Judge (*In re* Midland Publ'g Co., Inc.), 317 N.W.2d 284, 285, 288 (Mich. Ct. App. 1982).

59. *See* SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 5 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (noting that 12.7% of national survey participants reported being victims of identity theft in the past five years); *see also* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION OVERVIEW OF THE IDENTITY THEFT PROGRAM OCTOBER 1998–SEPTEMBER 2003 7 (2003), *available at* http://www.ftc.gov/os/2003/09/timelinereport.pdf (noting an increase in reported cases of identity theft from 1380 in 1999, to a projected 210,000 in 2003); FED. TRADE COMM'N, ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME 1–2 (Nov. 2003) [hereinafter ID THEFT], *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf; U.S. GEN. ACCOUNTING OFFICE, IDENTITY FRAUD: INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED 40–45 (1998), GAO/GGD-98-100BR, *available at* http://www.gao.gov/archive/1998/gg98100b.pdf.

undermine the relationship of trust between physician and patient.[60] Congress has attempted to address some of the social problems created by electronic financial and health care records through the enactment of privacy legislation.[61]

In Section 205 of the E-Government Act of 2002, Congress directed the federal court system to implement public access to the Internet by 2004 and also directed the Judicial Conference to promulgate rules to address concerns about the privacy and security of personal information in light of the best practices of the federal and state courts.[62] The E-Government Act places considerable discretion in the hands of the courts, and indicates a congressional deference to the courts to be responsible for the management and oversight of their own records.[63] However, the language in the E-Government Act clearly shows that Congress believed that, as always, courts continue to have a responsibility to balance the benefits of public access against the concern for the security and privacy of individuals.

It is also important to remember in this context that courts have a responsibility not only to protect the litigants—most of whom at least are represented by counsel (although an increasing number of litigants are acting pro se)—but also a responsibility to witnesses, victims, jurors, and other third parties who enter the legal system without the due process protections of the Fourteenth Amendment.[64] Courts must ensure that those who encounter the legal system—voluntarily as well as involuntarily—do not face exploitation of their personal information by commercial information brokers or become the victims of cyber-criminals or electronic peeping toms.

D. Legal Protections for the Privacy Value in Practical Obscurity

The information age has transformed the world so quickly that there has been little time to develop case law that adjusts the balance between public access and the protection of personal information with the

60. *See* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 634–39 (2002).

61. Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2000); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681v (2000); Gramm-Leach-Bliley Financial Modernization Act, 15 U.S.C. §§ 6801–6827 (2000); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d–1320d-8 (2000).

62. E-Government Act of 2002, Pub. L. No. 107-347, § 205, 116 Stat. 2899, 2913–15.

63. *Id.*

64. U.S. CONST. amend. XIV.

differences between electronic and paper records in mind. However, from the limited number of cases addressing the question of computerized information, there is a growing recognition by courts that a very different balance must be applied. In *Whalen*, the fact that the information was compiled in a mainframe computer database was of tremendous significance to the Court.[65] Although the Court found that the system of protections established by the government passed constitutional muster,[66] Justice Brennan wrote a concurrence that was prescient as to the future problems to come:

> What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increases 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.[67]

The case that is perhaps most applicable to the problem of electronic judicial records is *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[68] In this FOIA case, Justice Stevens cited *Whalen* in rejecting the press's argument that because a person's FBI computerized rap sheet was merely a summary of public records of arrests and convictions from local state and county courthouses around the country, the FBI computerized rap sheet itself should be a public document accessible under the FOIA.[69] He observed: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[70]

---

65. Whalen v. Roe, 429 U.S. 589, 605 (1977).

66. *Id.* at 600.

67. *Id.* at 606–07 (Brennan, J., concurring).

68. 489 U.S. 749 (1989).

69. *Id.* at 762–63.

70. *Id.* at 764.

Strictly speaking, of course, the test established by Justice Stevens in *Reporters Committee for Freedom of the Press* applies only in a FOIA context to the FBI's record-keeping system (although it involved court records). However, the underlying problems in that case—the problems of balancing public access to information against concerns for individual privacy—are exactly the same. Thus, the balance reached by the Supreme Court in that case represents an extremely important precedent. The Court defined the public's interest as shedding "light on the conduct of any Government agency or official" rather than acquiring information about a particular private citizen.[71] The Court also noted "the fact that 'an event is not wholly 'private' does not mean than an individual has no interest in limiting disclosure or dissemination of the information.'"[72] As in the case of the rap sheets addressed in *Reporters Committee for Freedom of the Press*, before the advent of electronic case files, the right to "inspect and copy" court files depended on physical presence at the courthouse. The inherent difficulty of obtaining and distributing paper case files largely insulated litigants and third parties from the harm that could result from massive or unnecessary exposure, dissemination, or misuse of information provided in connection with a legal proceeding. When the U.S. Supreme Court has focused on the new world of electronic information, it recognized that it had to alter the balance formerly adopted between the competing policies of granting and limiting access to judicial records.

E. The Way Forward

If the message of *Reporters Committee for Freedom of the Press* is followed by courts about to adopt a system of electronic judicial record-keeping, it would appear that there must be a new balancing that takes place. Courts must recognize that their case files often contain private or sensitive personal information—such as medical and health records, employment records, detailed financial information, tax returns, Social Security numbers, intimate family information, intimate victim information, and other personal and identifying information. In the world of paper judicial records, the inconvenience of access provides considerable practical protection for the concerned individuals.

71. *Id.* at 773.

72. *Id.* at 770 (quoting Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26–27, 1974)).

However, when courts permit these case files to become electronic and connected to the Internet without proper safeguards, they will make all this personal information available easily and almost instantly for downloading, storage, searching, data compilation, aggregation, and massive dissemination for purposes that were never intended by either litigants, witnesses, victims, jurors, or others involved with or connected to a court proceeding.

F. Maintaining the Balance in the Movement to Online Court Records

Reaching a balance between judicial accountability and the protection of privacy was not an easy task in the days of paper-based judicial records. The cases reflect a continual struggle between the goals of ensuring open access to court records and the competing goals of ensuring the effective working of the judicial system and respecting the privacy of the participants. The decisions are fact specific and highly contextual, but they all reflect sensitivity by the courts to the importance of balancing the various competing interests at stake. In the world of electronic information, the conflict between principles of open access and privacy becomes much more sharp and difficult for courts to resolve. There is no easy solution. Ideally, courts should be free to engage in the same common law decision-making process that courts used to resolve such conflicts in the age of paper-based judicial records.

Unfortunately, the most important decisions will not take place as a matter of case-by-case decision making, but will be the decisions that courts make as an administrative matter when they select the computerized record-keeping system they will use and when they establish the rules governing the use of that system. The balance must be worked out in the way administrative agencies make decisions—presumably after notice, public participation, comment, and thoughtful reflection on the costs and benefits of the various alternatives. A thoughtful set of guidelines for public access to court records has been produced by the National Center for State Courts and the Justice Management Institute.[73] In the same vein, the Canadian Judicial Council

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

has released a very thoughtful discussion paper on open courts, electronic access to court records, and privacy.[74]

G. *The Experience of the Federal Courts*

Perhaps the most significant development in the context of this debate is the *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files* (Report).[75] Before the Judicial Conference Committee on Court Administration and Case Management (Committee) issued the Report, a study of the problem was prepared by the staff of the Administrative Office of the United States Courts.[76] The staff white paper described two general approaches to the problem.[77] One approach was to treat electronic judicial records as governed by exactly the same rules as paper records—what the white paper calls the "public is public" approach.[78] The second approach advocated treating electronic and paper files differently in order to respect the practical obscurity of paper case files, urging that the rules regulating electronic court records reflect the fact that unrestricted online access to court records would undoubtedly, as a practical matter, compromise privacy, as well as increase the risk of personal harm to litigants and third parties whose private information appeared in case files.[79] The white paper suggested that different levels of privileges could be created to govern electronic access to court records.[80] Under this approach, judges and court staff would generally have broad, although not unlimited, remote access to all electronic case files, as would other key participants in the judicial process, such as the

74. SUBCOMM. FOR THE JUDGES TECH. ADVISORY COMM., CANADIAN JUDICIAL COUNCIL, DISCUSSION PAPER ON OPEN COURTS, ELECTRONIC ACCESS TO COURT RECORDS, AND PRIVACY (2003), *available at* http://www.cjc-ccm.gc.ca/english/publications/OpenCourts-2-EN.pdf.

75. SUBCOMM. ON PRIVACY & PUB. ACCESS TO ELECTRONIC CASE FILES, JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON COURT ADMINISTRATION AND CASE MANAGEMENT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES (2001) [hereinafter REPORT], *available at* http://www.courtaccess.org/federal/documents/report-elecfiles2001.pdf. The Judicial Conference is charged with the responsibility for making policy with regard to the administration of the United States courts. 28 U.S.C. § 331 (2000).

76. OFFICE OF JUDGES PROGRAMS, ADMIN. OFFICE OF THE U.S. COURTS, PRIVACY AND ACCESS TO ELECTRONIC CASE FILES IN THE FEDERAL COURTS (1999), *available at* http://www.uscourts.gov/privacyn.pdf.

77. *Id.* at 7.

78. *Id.*

79. *Id.* at 7.

80. *Id.* at 10.

U.S. Attorney, the U.S. Trustee, and bankruptcy case trustees.[81] Litigants and their attorneys would have unrestricted access to the files relevant to their own cases.[82] The general public would have remote access to a subset of the full case file, including, in most cases, pleadings, briefs, orders, and opinions.[83] Under this approach, the entire electronic case file could still be viewed at the clerk's office, just as the paper file is available now for inspection, but would not generally be made available on the Internet.[84]

Unfortunately, at least with respect to civil cases and bankruptcy cases, few, if any, of the suggestions contained in the staff white paper were ultimately adopted in the Report.[85] Instead, the Committee adopted the "public is public" approach to the problem, rejecting the view that courts have a responsibility to adopt rules governing the use of their computer systems to try to recreate in cyberspace the practical balance that existed in the world of paper judicial records.[86] In supporting this decision, the Committee took the position that attempting to recreate the "practical obscurity" of the brick and mortar world was simply too complicated an exercise for the courts to undertake.[87] The Report does appear to recognize a limited responsibility on the part of the courts to adopt rules in order to limit the foreseeable harms of identity theft and online stalking.[88] The Report recommends that certain "personal data identifiers," such as Social Security numbers, dates of birth, financial account numbers, and names of minor children, be partially redacted by the litigants.[89]

With respect to the problem of protecting individual privacy, the Report places the burden on parties and counsel to anticipate these questions, and advises them to use motions to seal and for protective orders on a case-by-case basis.[90] Although it is reasonable to hold the

---

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.*

85. *See* REPORT, *supra* note 75, at 3–7.

86. *See id.* at 4.

87. *Id.*

88. *See id.* at 6.

89. *Id.* at 3–5. Social Security case files were excluded entirely from online access, presumably because of the large amount of personal health information contained in such files. *Id.* at 5.

90. *Id.* at 3. The Committee's Report recognizes that the public access requirement of the Bankruptcy Code, 11 U.S.C. § 107 (2002), appears to preclude bankruptcy courts from sealing any

parties and their attorneys primarily responsible to protect their own privacy, the Report could have and should have done more in this respect. For instance, its guidelines could have included more explicit warnings to attorneys to exercise caution when filing any personal identifying number, such as a driver's license number, medical records, treatment and diagnosis, employment history, individual financial records, information pertaining to children, or proprietary or trade secret information.[91] The most significant weakness in the Report is that it leaves unanswered the question of how the system will protect the privacy of pro se litigants or third parties who are not litigants or have not voluntarily chosen to enter the justice system—foremost among these are jurors, witnesses, victims of crimes, and their family members.[92]

The Report recommends that criminal court records not be placed online, for the present, finding that any benefits of remote electronic access to criminal files would be outweighed by the safety and law enforcement risks such access would create.[93] The Report expressed the concern that allowing defendants and others easy access to information regarding the cooperation and other activities of co-defendants would increase the risk that the information would be used to intimidate, harass, and possibly harm victims, defendants, and their families.[94] In addition, the Report noted that merely sealing such documents would not adequately address the problems of online access, since the fact that a

---

court records to protect the privacy of individuals. REPORT, *supra* note 75, at 6. The Committee responds to this concern by suggesting that Congress amend 11 U.S.C. § 107 to address this problem. *Id.* In the meantime, it would presumably be possible for a court to order that certain records be filed publicly in the clerk's office, but kept off-line. In addition, it would appear to be possible, as some bankruptcy courts have done, to adopt local rules requiring certain types of information—such as Social Security numbers, numbers of financial accounts, and names of minor children—not be placed in the court file at all, while still providing this information to key participants in the system. *Id.*

91. *See, e.g.*, Bankruptcy Court of the Northern District of Texas, Privacy-Related Rules Changes (Nov. 24, 2003) (implementing explicit procedures related to privacy and public access to electronic court files), *available at* http://www.txnb.uscourts.gov/notices/20031124_Privacy.pdf.

92. The problem of protecting innocent third parties from harm is particularly pressing in bankruptcy cases. For instance, in large Chapter 11 cases, "First Day" orders typically provide for the payment of back wages of employees of the debtor. These orders typically contain large amounts of sensitive personal information, including salaries, health benefit information, and Social Security numbers. Innocent third parties, usually family members, are also usually implicated in individual bankruptcy cases.

93. REPORT, *supra* note 75, at 5.

94. *Id.*

document is sealed signals probable defendant cooperation and covert law enforcement initiatives.[95]

Of course, as federal courts have converted to electronic filing systems, criminal records are filed electronically as well. However, for criminal cases, access to electronic criminal records is controlled through a system of privileges. Judges and law clerks have full access to criminal court records, as do defense attorneys and prosecutors in those cases in which they are counsel. While members of the general public do not have online access to the criminal court files, copies of indictments and other documents that were publicly available in the past continue to be publicly available—by request in person at the clerk's office. There is no technological reason why, on a case-by-case basis, a third party—such as a newspaper reporter or other interested member of the public—could not request similar electronic access to the case file. However, this access would be permitted only after notice to the other parties in the case who could be heard if electronic public access might involve any special risks.

From the limited experience in criminal cases, it appears that courts do have the capacity to implement an electronic system that uses different levels of privileges to recreate in cyberspace a system that protects the same values that were protected by the practical obscurity of paper records. Implementing a system of privileges does not appear to present any serious technological problems—the architecture of the federal PACER system is the same for both civil and criminal judicial records. However, if this is a correct evaluation of the current technology used by clerks in federal courts, a somewhat disturbing conclusion follows. It would appear that the Committee, at least in the case of civil and bankruptcy cases, simply made a decision to ignore the legal decisions with respect to the existence of a right to privacy in the practical obscurity of judicial records—or to have made a determination that these cases represented the wrong public policy. If so, one would hope that the Committee could have expressed the underlying basis of its decision more clearly. As it is, the Report leaves an outside observer with the disquieting feeling that the Committee may be using technology not as a reason, but as an excuse.

Under the mandates of the E-Government Act, the federal judiciary will continue to review and monitor the process of online access.[96] The

95. *Id.*

96. E-Government Act of 2002, Pub. L. No. 107-347, § 205, 116 Stat. 2899, 2913–15.

Report itself recognizes that the federal courts will ultimately have to revise their rules and procedures about electronic access to judicial records in the light of experience.[97] In doing so, the Committee will have to consider the concrete experience of both federal and state courts as they experiment with different models of information protection. In the meantime, both federal and state courts are likely to see considerably more litigation regarding motions to seal records and for protective orders. In the context of this litigation, parties desiring to protect personal information but unable to meet the standard for a seal or a protective order, may consider requesting the intermediate relief that documents filed electronically in their civil cases simply be kept off-line, in the same manner as criminal case files in the federal court. Under this approach, the parties might continue to have electronic access to their court file, and the court file would continue to be available for public viewing at the clerk's office, or be made available electronically on the filing of a notice of appearance by any interested person. The parties should have the right to request that their personal information—and the personal information of others—simply not be made available for unrestricted access on the Internet.

H. Tentative Suggestions

In ruling on motions to protect personal information from online invasions of privacy, as well as in the process of fashioning local rules governing online access, the *Westinghouse* test[98] may prove to be a model of how courts may have to determine what type of information parties should be permitted to protect. Is it the type of information that society as a whole is prepared to recognize as involving a reasonable expectation of privacy? What is the potential for harm to the person in the disclosure of that information? What is the potential for harm to the relationship in which the information was generated (that is, is there any confidential relationship involving broader societal policies protecting those relationships)? What safeguards can be put in place to protect the information in electronic form in the courthouse or remotely? What procedures and criteria should there be for allowing access in specific instances to otherwise confidential or private information, or in specific instances protecting sensitive or private information when it would

97. *See* REPORT, *supra* note 75, at 2.

98. *See supra* note 43 and accompanying text.

otherwise be publicly accessible? And finally, what is the need for access of the public and the press?

III. CONCLUSION

This is obviously only a beginning sketch. The problem requires a great deal more reflection and thought. What is clear, however, is the need for more focus on the concrete ways in which information in judicial records is being used in our society. The general principles to be used in establishing the right balance are well established. There should be a general presumption in favor of public access, especially when it ensures judicial accountability and facilitates the administration of justice. However, courts must take steps to restrict public access when indiscriminate access conflicts with the administration of justice, when it unnecessarily causes invasions of privacy, or when it exposes litigants, witnesses, and other innocent third parties to threats from the potential misuse of their personal information. The courts should also frame their rules of procedure—local and national—and their instructions to attorneys and litigants to ensure that attorneys and unrepresented litigants know how to take responsibility for identifying sensitive personal information that should be candidates for protection, and are capable of doing so.[99] The courts can facilitate this process by encouraging the use of protective orders and motions to seal.

Ironically, it appears that a technological revolution that was supposed to be labor saving will require greater exertion than before from courts and attorneys. In the face of the difficulty of this project, there is a strong temptation to adopt the "public is public" approach, dismissing the concept of "practical obscurity" altogether. However, the temptation to permit indiscriminate electronic public access to court records should be resisted, for it threatens to eviscerate years of careful judicial labor in which courts struggled to achieve an appropriate balance between the competing goals of public access and privacy. In this vein, rejection of the values underlying the concept of "practical obscurity" can be seen as nothing more than a policy decision by the courts to shift the risk of harm to litigants, witnesses, victims, jurors, and

99. For an excellent analysis of the potential malpractice liability of attorneys for failure to take reasonable care to protect their clients' sensitive personal information in the context of online court filings, see Michael Caughey, Comment, *Keeping Attorneys from Trashing Identities: Malpractice as Backstop Protection for Clients Under the United States Judicial Conference's Policy on Electronic Court Records*, 79 WASH. L. REV. 407 (2004).

other innocent third parties whose personal information becomes implicated in judicial proceedings.

This Article has discussed how the use of electronic information makes it much more difficult to balance the need to maintain judicial accountability against the need to protect personal information in court files. As we struggle to maintain this balance, we may discover that the problem is not limited to what is filed in the clerk's office and that we ultimately have to see this problem in the context of the more general issue of how to regulate the flow of information throughout the judicial system. Traditionally, information exchanged between attorney and client received presumptive protection, while information contained in court files was presumptively open. As electronic information flows from clients to their lawyers and into online court filings, we may be forced to modify this traditional presumption in order to recognize the fact that different types of information have different potentials for misuse depending on their different legal contexts. Even now, the decision of the Committee to keep electronic criminal records off-line marks an important change in our understanding of the need to handle "public" information in court files responsibly. Given the obvious dangers of placing information in criminal case files online, the federal courts were simply forced to treat this information differently from how they treat information in civil files. As more and more courts go online, we may be forced to adopt different rules for access to information in different types of legal proceedings, depending on the potential for that information to be misused.

We have lived in a very forgiving world. The "practical obscurity" of paper judicial records largely sheltered us from the danger of information misuse, while we prided ourselves on our "public" judicial system. The world of electronic information is a far less forgiving place. It is now forcing us to recognize—by our actions, if not yet by our words—that the simple abstract rules developed for a world of paper-based information may no longer suffice to resolve the complex problems of judicial information management. Courts have traditionally been vigilant in protecting individuals from the misuse of sensitive personal information. They must now rise to the difficult task of designing rules to protect litigants and third parties from cyber-mischief and victimization. The failure of the legal system to maintain the ancient balance between access and privacy will lead to the greatest danger of all—inhibiting citizens from participating in the public judicial system. The world of cyber-justice should not be permitted to degenerate into a

world where victims of crimes are reluctant to come forward; where people are more unwilling to be witnesses or jurors; and where the rich can seek out private judicial forums to resolve their disputes, while the poor and middle classes are faced with an impossible choice—either foregoing justice to maintain their privacy and security; or permitting their sensitive personal information to be commercialized or stolen, and allowing the intimate details of their personal lives to be made available all over the Internet.