TAMING TECHNOLOGY IN THE CONTEXT OF THE PUBLIC ACCESS DOCTRINE: NEW JERSEY'S AMENDED RULE 1:38

Kristin M. Makar[*]

I. INTRODUCTION

"Your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should."[1] This quote by Dr. Ian Malcolm, a character in Steven Spielberg's thriller, *Jurassic Park*, describes the enthusiastic power of both discovery and innovative technological development, while cautioning against the dangers of technology. Although public access to court documents via the Internet does not begin to breach the subject of breeding dinosaurs, it does share the same pioneering spirit enveloping the technological possibilities of which Dr. Malcolm warned. Similarly, the debate over public access to court records through the Internet, which is part of a larger debate regarding the intersection between law and technology, embodies an inherent conflict between technological capabilities on the one hand and moral, ethical, and legal limitations on the other hand. In particular, because the Internet has the power to alter the public access doctrine by greatly expanding its capacity, it illuminates the legal tension between public access rights and individual privacy rights. As the Internet changes the way that society envisions business and pleasure, state and federal courts, forced to act as experimenters, are reflecting on their public access procedures and reviewing potential changes.

In July 2009, the Supreme Court of New Jersey amended New Jersey Court Rule 1:38[2] by completely rewriting and revising the framework of the public access doctrine under former Rule 1:38. The amended Rule fundamentally alters the former Rule's framework and the public access doctrine itself because it presumes that all court records are open for public access with the exclusion of some

[*] J.D. Candidate, May 2011, Seton Hall University School of Law; B.A., 2008, Gettysburg College. I wish to thank Professor Robert Martin for his supervision and Seth Fersko for his comments and assistance.

[1] JURASSIC PARK (Universal Pictures 1993).

[2] N.J. CT. R. 1:38 (2009).

records contained in its comprehensive and exclusive list of exceptions.[3] In effect, New Jersey courts will no longer struggle with the common law "balancing of the interests" test to determine when certain records should be available for public inspection because a presumption of openness applies unless the type of record is specifically addressed in the exceptions.[4] More significantly, although the amended Rule does not address Internet accessibility explicitly in its provisions, the Supreme Court of New Jersey adopted the recommendations of its self-appointed committee, the Special Committee on Public Access to Court Records (the "Committee"),[5] which advocate for the expansion of public access rights through remote electronic access to court documents.[6]

The recommendations approved by the Supreme Court of New Jersey address the amended Rule's failure to acknowledge Internet accessibility explicitly in its provisions. Specifically, the recommendations, advising the court to create and periodically review its policies governing the posting of court documents on the Internet, permit the court to issue policy guidelines consistent with the presumption of openness motivating the amended Rule.[7] This grant of discretion, combined with the ambiguity in the amended Rule itself, creates an opportunity for the court to consider the conflict between public access rights and individual privacy concerns when drafting its guidelines relating to Internet accessibility. This necessarily invokes a re-

---

[3] *See infra* note 117 and accompanying text.

[4] *See infra* note 117 and accompanying text.

[5] SUPREME COURT OF N.J., ADMINISTRATIVE DETERMINATIONS BY THE SUPREME COURT ON THE REPORT AND RECOMMENDATIONS OF THE SUPREME COURT SPECIAL COMMITTEE ON PUBLIC ACCESS TO COURT RECORDS 1 (July 22, 2009), *available at* http://www.judiciary.state.nj.us/pressrel/AlbinCommitteeRule_138AdministrativeDeterminations_by_the_Supreme_Court.pdf [hereinafter ADMINISTRATIVE DETERMINATIONS].

[6] *See id.* at 6 (adopting a policy of posting civil-docket and criminal-conviction information on the Internet and determining additional categories for posting in the future). As of December 2010, the New Jersey Judiciary website did not maintain a mechanism to view court documents through remote electronic access, but it did provide information about locating specific documents in accordance with Rule 1:38. *Copies of Court Records*, N.J. COURTS, http://www.judiciary.state.nj.us/superior/copies_court_rec.htm (last visited Dec. 25, 2010).

[7] SUPREME COURT SPECIAL COMMITTEE ON PUBLIC ACCESS TO COURT RECORDS, REPORT OF THE SUPREME COURT SPECIAL COMM. ON PUBLIC ACCESS TO COURT RECORDS 15 (2007), *available at* http://www.judiciary.state.nj.us/publicaccess/publicaccess.pdf [hereinafter REPORT] ("Given the rapid changes in technology, the Supreme Court should determine on a periodic basis the appropriate court data for posting on the Internet and for release in bulk electronic form. The Supreme Court should make those determinations on an administrative basis without amending the public access rule.").

view of First Amendment and common law jurisprudence as the debate over how courts should incorporate technology into the public access doctrine continues among scholars, courts, and the public.

This Comment argues that the Supreme Court of New Jersey must consider certain consequences and unanswered questions raised by amended Rule 1:38's alteration of the public access doctrine and pro-Internet initiatives, and it further proposes recommendations and solutions to these quandaries. Four circumstances exist in which the amended Rule's innovation raises perplexities. First, the Rule requires the parties to redact any confidential personal identifiers from documents submitted to the court, but it fails to provide an enforcement mechanism to punish a party's lack of compliance. Second, Internet posting incentivizes parties to draft sealing motions to protect information that practical obscurity once protected, and the Rule's strict sealing standard may force parties to make incomplete records or to turn to private forums for conflict resolution. Third, the timing of Internet release is undefined and raises questions about the Rule's applicability to records created before the Rule became effective, as well as when the Rule requires courts to release the records during a case. Finally, the question of creation and maintenance costs to support an Internet-user system is of particular concern as the State's debt continues to increase.

Permitting public access to court documents in the courthouse is fundamentally different from widely publishing such information over the Internet. This Comment does not advocate for a change in the traditional public access doctrine, but it argues only that courts treat remote electronic records differently than paper records. With the understanding that the Supreme Court of New Jersey supports and intends to begin posting at least some of its court records on the Internet, this Comment offers guidelines that the Supreme Court of New Jersey should consider when drafting the appropriate policies governing Internet accessibility. The recommendations proffered in this Comment focus on: drafting an enforcement provision to ensure compliance with the redaction requirements; restricting Internet access only to court-generated documents; limiting the release of court documents on the Internet to records created after the effective date of the amended Rule and not until the final disposition of the case; maintaining user fees to offset costs; and creating a log-in procedure before a court grants access. Contemplation of these policy recommendations will help ensure the proper balance between public access rights and individual privacy rights.

Part II of this Comment explains the history of the public access doctrine, in particular the sources of public access rights, decisions of the Supreme Court of the United States, and the underlying policy rationales for providing public access to court documents. Although the founding constitutional principles for the public access doctrine and Supreme Court decisions often focus on the public's right to attend criminal trials, rather than directly on the public's right to inspect criminal or civil court documents, lower courts have used the same rationale to extend the right to court documents and civil cases.[8] Part III examines the competing arguments over whether remote electronic access to court documents is more beneficial than harmful in the struggle between public access rights and individual privacy rights. Part IV analyzes New Jersey's former and amended Rule 1:38, which governs public access to court records, and it reviews the limited New Jersey case law on the public access doctrine. Finally, Part V addresses the possible consequences and unanswered questions raised by amended Rule 1:38, especially as they relate to the tension between protecting public access rights and individual privacy rights. Part V also recommends guidelines that the Supreme Court of New Jersey should consider when drafting its Internet policy in the face of a new and explicit presumption of openness.

II. HISTORY OF THE PUBLIC ACCESS DOCTRINE

The public access doctrine is deeply rooted in the historical notion that trials are public events. Courts support their determinations in favor of public access rights based on First Amendment and common law principles. In several prominent cases, the Supreme Court of the United States has held that the public has either a First Amendment right or a common law right to access court proceedings and documents.[9] Although the Court has never confronted the discrete issue of remote electronic access to court documents, some of its opinions have alluded to the difficulty posed by advancing technology as it relates to the public access doctrine.[10] In recent cases, the Court has acknowledged the concept of information privacy and the competing interests between public access rights and individual privacy rights.[11] In an attempt to harmonize this tension, courts fre-

[8] *See infra* note 16 and accompanying text.
[9] *See infra* Part II.B.
[10] *See infra* Part II.B.
[11] *See infra* Part II.B.

quently address the basic policy rationales that support an open judicial process.[12]

A. *Sources of Public Access Rights*

Two sources provide public access rights: the First Amendment and the common law. The First Amendment public access right is a fundamental right, which the government may limit only by demonstrating a compelling governmental interest and a limitation that is narrowly tailored to serve that interest.[13] The Supreme Court of the United States established a two-prong test to determine when a First Amendment right of public access attaches to court documents in a criminal proceeding—when the proceeding has historically been open to the public and public access promotes judicial integrity.[14] Although the Supreme Court has not applied this test in the context of public access to court documents in a civil proceeding, the circuit courts, including the Third Circuit,[15] apply the same logic for civil proceedings.[16]

The Supreme Court first recognized a common law right of access to court documents in *Nixon v. Warner Communications, Inc.*[17] In contrast to the First Amendment right, which is subject to strict scrutiny,[18] the common law right of access requires a balancing test that is easier to overcome with countervailing privacy interests.[19] De-

---

[12] *See infra* Parts II.B, II.C.

[13] 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.").

[14] Press-Enterprise Co. v. Superior Court (*Press-Enterprise II*), 478 U.S. 1, 8–9 (1986). The Supreme Court originally articulated and explained the two prongs in *Globe*, 457 U.S. at 610–11 (applying the First Amendment test to a claim for public access to a criminal proceeding).

[15] The Third Circuit is particularly notable because New Jersey is in the Third Circuit.

[16] *See* Publicker Indus., Inc. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1984) (holding that the First Amendment right of access applies equally to criminal and civil trials); *see also* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580 n.17 (1980) ("[H]istorically[,] both civil and criminal trials have been presumptively open.").

[17] 435 U.S. 589, 597 (1978).

[18] Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606–07 (1982).

[19] *See* United States v. McVeigh, 119 F.3d 806, 812 (10th Cir. 1997) ("Further, both the common law and First Amendment standards ultimately involve a balancing test, and the First Amendment right of access receives more protection than the common law right."); United States v. McDougal, 103 F.3d 651, 657–58 (8th Cir. 1996) (noting that the strong presumption of access applies for a First Amendment access right but not for a common law right); Stone v. Univ. of Md. Med. Sys. Corp.,

spite the differences in the strength of the presumption and the degree of difficulty in rebutting the presumption, most courts hesitate to decide the constitutional issue and instead elect to rely on the common law analysis.[20]

B. *Decisions of the Supreme Court of the United States Concerning the Public Access Doctrine*

The Supreme Court has never heard a case addressing the issue of remote electronic access to court documents. To understand the current debate over Internet accessibility to court documents, however, one must explore the holistic development of the public access doctrine. The modern public access doctrine developed when the Supreme Court decided several seminal cases in the 1970s and 1980s. In one of the earliest cases, *Whalen v. Roe*, the Court recognized a constitutional right to information privacy.[21] Although the Court upheld a state statute requiring the storage of centralized computer files to record patient information, the Court framed the debate as: (1) the interest in avoiding disclosure of personal matters and (2) the interest in independence in making important decisions.[22] Perhaps more notably, in light of the modern debate regarding the intersection of law and technology, Justice Brennan, in his concurrence, noted that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on technology."[23] The majority and the concurring opinions suggest that courts apply a different privacy right or a different level of privacy when electronic files are subject to public inspection and when dissemination of personal matters is more prolific.

855 F.2d 178, 180 (4th Cir. 1988) (comparing the standards to overcome the right of access under the common law and the First Amendment).

[20] Laurie Kratky Dore, *Secrecy by Consent: The Use and Limits of Confidentiality in the Pursuit of Settlement*, 74 NOTRE DAME L. REV. 283, 320 (1999). This proposition is consistent with the concept of constitutional avoidance, which is the idea that courts will avoid determining the constitutionality of an issue unless no other alternative foundation exists on which to make a decision. *See* Cromwell v. Benson, 285 U.S. 22, 62 (1932) ("[E]ven if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.").

[21] *See* 429 U.S. 589, 605 (1977) (recognizing that the right to collect data for public purposes is accompanied by a corollary duty to avoid unwarranted disclosures, and sometimes such a duty "arguably has its roots in the Constitution").

[22] *Id.* at 600–01.

[23] *Id.* at 607 (Brennan, J., concurring).

In 1978, the Court decided a second case, *Nixon*, which recognized a common law right of access to court documents but cautioned that the right is not absolute, particularly when the individual's interest to restrict access outweighs the public's interest.[24] The Court pronounced that each individual court has supervisory power over its own records and that courts have the discretion to deny access when courts determine that documents may become a vehicle for improper purposes.[25] After this decision, several federal courts began to recognize a common law right of access as creating a rebuttable presumption in favor of public access to documents filed in connection with a pretrial motion.[26] The circuit courts are split, however, as to the type of document to which the presumption attaches.[27]

In the early 1980s, the Court decided two cases that focused on the First Amendment right of access to court proceedings but that also informed the debate regarding public access rights in the context of court documents and civil proceedings. In *Richmond Newspapers, Inc. v. Virginia*, the Court held that criminal trials must be open to the public under the protection of the First Amendment.[28] In *Globe Newspaper Co. v. Superior Court*, the Court articulated the appropriate considerations to determine when a First Amendment right of access exists for criminal proceedings: whether the proceeding has been

[24] *See* Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 598, 610–11 (1978) (holding that the litigant's individual interests to restrict access outweighed the common law public right to access tapes released during the trial).

[25] *Id.* at 598. The Court provided examples of when documents may become a vehicle for improper purposes, including promoting public scandal, encouraging libelous statements, or revealing harmful business information. *Id.*

[26] *See* F.T.C. v. Standard Fin. Mgmt. Corp., 830 F.2d 404, 409 (1st Cir. 1987) (applying the common law standard to financial statements introduced in an adjudicatory proceeding and permitting public access); Bank of Am. Nat'l Trust & Savs. Ass'n v. Hotel Rittenhouse Assocs., 800 F.2d 339, 344 (3d Cir. 1986) (applying the common law standard to settlement agreement papers and permitting access); *In re* Knoxville News-Sentinel Co., Inc., 723 F.2d 470, 476 (6th Cir. 1983) (applying the common law standard and permitting the removal of exhibits from the public court file to protect privacy and identity); Crystal Grower's Corp. v. Dobbins, 616 F.2d 458, 461 (10th Cir. 1980) (applying the common law standard to a party's brief and keeping it under seal).

[27] *Compare* Leucadia, Inc. v. Applied Extrusion Tech., Inc., 998 F.2d 157, 164 (3d Cir. 1993) (holding that the mere filing of documents creates the presumption of public access), *with* United States v. Amodeo, 44 F.3d 141, 145 (2d Cir. 1995) (holding that the presumption applies only to documents used in adjudicating the case), *and* Anderson v. Cryovac, Inc., 805 F.2d 1, 12 (1st Cir. 1986) (holding that the presumption applies to those documents relevant to the functioning of the judiciary).

[28] 448 U.S. 555, 575, 581 (1980) (discussing the long history of open trials during the enactment of the First Amendment and holding that the criminal trial at issue must be open to the public).

historically open to the public and whether the right of access plays a significant role in the functioning of the judicial process.[29] The Supreme Court rearticulated these considerations in a subsequent case regarding a claimed First Amendment right of access to court documents.[30]

Finally, in the most recent case addressing the public access doctrine, *United States Department of Justice v. Reporters Communication for Freedom of the Press*, the Court held that a request for records stored by the government, rather than shedding light on the functioning of the government, was an unwarranted invasion of privacy.[31] Although the Court decided the case under the Freedom of Information Act[32] and the case did not directly pertain to court documents,[33] the Court addressed privacy concerns related to the public access doctrine.[34] The Court stated, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files . . . and a computerized summary located in a single clearinghouse of information."[35] The Court concluded that common law understandings of privacy include an individual's control of information concerning his person.[36] As in *Whalen*, the Court suggested that electronic records raise different concerns from traditional paper records in the context of privacy and the public access doctrine.

C. *The Rationale Underlying the Public Access Doctrine*

Five fundamental policy rationales exist to justify providing public access to court proceedings and documents.[37] These policy ratio-

[29] 457 U.S. 596, 605–06 (1982). This is often referred to as the "experience and logic" test. Press-Enterprise Co. v. Superior Court (*Press-Enterprise II*), 478 U.S. 1, 9 (1986).

[30] *See Press-Enterprise II*, 478 U.S. at 8–9, 13 (applying the test to a claim for public access to court transcripts of a preliminary hearing and holding that the First Amendment right of access to criminal trials applies to preliminary hearings).

[31] 489 U.S. 749, 780 (1989) (holding that the invasion was unwarranted under the Freedom of Information Act because the request was not made to obtain official information about a government agency, but only to retrieve records stored by the government).

[32] Freedom of Information Act, 5 U.S.C. § 552 (2006).

[33] *Reporters Comm. for Freedom of the Press*, 489 U.S. at 751, 780.

[34] *See id.* at 764 (discussing the definition of privacy as information unavailable to the public and differentiating between scattered information and compiled information in relation to privacy matters).

[35] *Id.*

[36] *Id.* at 763.

[37] Peter W. Martin, *The New "Public Court": Online Access to Court Records—From Documents to Data, Particulars to Patterns*, 53 VILL. L. REV. 855, 857–58 (2008).

nales guide courts in their analyses under both the First Amendment and the common law tests. The principles are salient because they transcend technological differences and because they inform many of the arguments in favor of treating paper and remote electronic records equally.

First, a policy endorsing public access guarantees that court proceedings are fair, enhancing public confidence in the judiciary.[38] Public confidence ensures judicial independence because increased transparency limits the prospect of public attack which may undermine judicial autonomy.[39] Second, public access allows citizens to monitor and scrutinize the judiciary, administering judicial accountability to ensure proper judicial performance.[40] Third, open access provides a forum for public concerns relating to crime, including an opportunity for the public to view courts dispensing justice properly to vindicate their concerns.[41] Fourth, open access promotes public education about the functions and processes of the judiciary in its decision-making capacities.[42] And fifth, public access ensures that the discussion of governmental affairs is an informed one and helps citizens actively participate and contribute to their government to the extent that they understand how courts enforce society's laws.[43]

III. THE DEBATE OVER REMOTE ELECTRONIC ACCESS TO COURT DOCUMENTS

The debate concerning electronic access penetrates the forefront of the public access doctrine because of the recent advances in modern technology. Juxtaposed between First Amendment and common law rights and individual notions of privacy, the arguments

---

[38] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 570 (1980).

[39] T.S. Ellis, III, *Systematic Justice: Sealing, Judicial Transparency and Judicial Independence*, 53 VILL. L. REV. 939, 948 (2008).

[40] Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606 (1982).

[41] Press-Enterprise Co. v. Superior Court (*Press-Enterprise I*), 464 U.S. 501, 508–09 (1984).

> Criminal acts, especially violent crimes, often provoke public concern, even outrage and hostility; this in turn generates a community urge to retaliate and desire to have justice done. When the public is aware that the law is being enforced and the criminal justice system is functioning, an outlet is provided for these understandable reactions and emotions.

Id.

[42] Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 587 (1976) (Brennan, J., concurring) ("[F]ree and robust reporting, criticism, and debate can contribute to public understanding of the rule of law and to comprehension of the functioning of the entire criminal justice system . . . .").

[43] *Globe*, 457 U.S. at 604–05.

supporting and opposing remote electronic access illuminate the broader debate over law and technology. While these issues are not distinct from the landmark cases decided by the Supreme Court in the 1970s and 1980s, today's courts must view the issue in light of improving technology and the vast capabilities of the Internet.

Prior to the 1990s, when the Internet began generating significant usership, the general public could not retrieve data effortlessly with the click of a mouse.[44] The modern Internet, with its capacity to disseminate information instantly worldwide, has been the source of significant legal debate. In the public access area, the Internet has generated questions about the effect of advancing technology on privacy rights because it makes personal information immediately accessible, and despite this problem, courts are turning to the Internet, instead of the clerk's office, to provide the public with access to court records. More significantly, the debate over remote electronic access to court documents sheds light on just how far society is willing to engage the legal system in the technological phenomenon, perhaps ever so mindful of Dr. Malcolm's heed.

The proliferation of the Internet revolution has forced legislatures, courts, and administrative agencies to devise laws, rules, and policies to address the role the Internet should play in administering justice. The debate focuses on two discrete proposals for the treatment of electronic records. One ideology is to treat remote electronic records the same as paper records and thereby ignore, or at least nullify, technological distinctions.[45] The other position advocates limiting remote electronic access to court documents while maintaining the complete paper record on file at the courthouse.[46] This approach recognizes the different roles that technology plays in the legal system. Advocates of both positions do not propose eliminating or reducing traditional public access to court documents, which would conflict with existing case law.[47] Rather, the disagreement resides in whether traditional notions of openness extend equally beyond paper records at the courthouse, protected to some extent by

[44] MANUEL CASTELLS, THE INTERNET GALAXY: REFLECTIONS ON THE INTERNET, BUSINESS, AND SOCIETY 12, 16–17 (2001).

[45] OFFICE OF JUDGES PROGRAMS, ADMIN. OFFICE OF THE U.S. COURTS, PRIVACY AND ACCESS TO ELECTRONIC CASE FILES IN THE FEDERAL COURTS 9–10 (1999).

[46] *Id.*

[47] *See supra* Part II.B.

practical obscurity,[48] to remote electronic records posted on the Internet.

A. Arguments in Favor of Equal Treatment of Paper and Remote Electronic Records

Proponents advocating for equal treatment of paper and remote electronic records reject the idea that the Internet changes the legal landscape in the public access doctrine. In effect, these proponents argue that the principle of openness inherent with paper records should evolve to include remote electronic records.[49] The argument is predominantly one of increased judicial transparency,[50] but supporters proffer several arguments involving issues of equality,[51] public policy,[52] attorney and client benefits,[53] and administrative convenience.[54] Given all of the arguments, the focus on equality is perhaps the most remarkable in light of the emphasis on fairness and equality offered in the American justice system. The argument contends that equal treatment of paper and remote electronic records levels the playing field geographically, temporally, and indiscriminately for parties and the interested public at large.[55]

Public policy propositions often evoke the basic policy rationales that support public access to court documents and proceedings.[56] For instance, proponents of equal treatment argue that remote electronic access offers the public the ability to aggregate and combine court

[48] Practical obscurity refers to the idea that court documents remain open to the public to the extent that interested individuals are willing to travel to the courthouse, wait in line, search through records, and pay copying fees to access information. Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 316 (2004).

[49] *See* DAVID RAUMA, FED. JUDICIAL CTR., REMOTE PUBLIC ACCESS TO ELECTRONIC CRIMINAL CASE RECORDS: A REPORT ON A PILOT PROJECT IN ELEVEN FEDERAL COURTS 15 (2003), *available at* http://ftp.resource.org/courts.gov/fjc/remotepa.pdf (commenting that chief judges, clerks, and defense attorneys regard remote public access as reinforcing the idea that courts are an "open, public institution").

[50] *See infra* notes 58–59 and accompanying text.

[51] *See infra* note 55 and accompanying text.

[52] *See infra* notes 60–64 and accompanying text.

[53] *See infra* notes 65–68 and accompanying text.

[54] *See infra* notes 69–72 and accompanying text.

[55] *See* RAUMA, *supra* note 49, at 15 (noting that equal access levels the playing field for attorneys who cannot easily access the courthouse); Lynn M. LoPucki, *Court-System Transparency*, 94 IOWA L. REV. 481, 514 (2009) (arguing that equal access levels the playing field by making the same information available to all parties); Martin, *supra* note 37, at 858 (suggesting that equal treatment ensures equal access for those unable to physically attend the proceedings).

[56] *See supra* Part II.C.

data to stimulate public debate on important policy issues.[57] Additionally, advocates insist that remote electronic access, because of its wide audience and transparency function, aids citizens in understanding the laws by which they are required to live.[58] Similarly, remote electronic access exposes and reduces corruption because the public is capable of monitoring the judiciary and imposing appropriate accountability.[59]

Advocates also advance several other public policy arguments. First, supporters assert that remote access to an electronic database helps promote due diligence and market research because of the ease with which information flows, which enhances the quality of business transactions and legal services.[60] A second proposition contends that the transparency achieved through remote electronic access demonstrates to legislatures how courts are implementing their laws and permits the legislatures to address and correct interpretive discrepancies.[61] Third, expansive public access through remote electronic methods helps form and shape societal norms in the context of law and justice observed in courts.[62] In particular, transparency has contributed to the condemnation of sexual harassment and domestic violence.[63] Finally, some proponents argue that providing remote access to the public discourages data re-sellers from copying and selling the information online for profit, thereby undermining any privacy protections maintained for the general public.[64]

---

[57] *Compare* Martin, *supra* note 37, at 859 ("Debate on important policy issues can also be aided by review of multiple cases of a particular type."), *with* Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 604–05 (1982) (noting that public access promotes informed discussion and encourages citizen participation).

[58] *Compare* LoPucki, *supra* note 55, at 484–85 ("It would expand the power of citizens and legislators over the courts and make the actual rules that govern society visible to the public."), *with* Nebraska Press Assn. v. Stuart, 427 U.S. 539, 587 (1976) (Brennan, J., concurring) (positing that public access educates the public about the laws and the judicial system).

[59] *Compare* LoPucki, *supra* note 55, at 485 (arguing that transparency exposes and reduces corruption and provides a basis for the public to evaluate the judiciary), *with Globe*, 457 U.S. at 606 (mentioning that public access permits the public to monitor and scrutinize the judiciary).

[60] Martin, *supra* note 37, at 868.

[61] LoPucki, *supra* note 55, at 496–97.

[62] Andrew D. Goldstein, *Sealing and Revealing: Rethinking the Rules Governing Public Access to Information Generated Through Litigation*, 81 CHI.-KENT L. REV. 375, 383 (2006).

[63] Judith Resnik, *Uncovering, Disclosing, and Discovering How the Public Dimensions of Court-Based Processes Are at Risk*, 81 CHI.-KENT L. REV. 521, 536–37 (2006).

[64] SUBCOMM. ON PRIVACY & PUB. ACCESS TO ELEC. 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

In addition to public policy arguments, advocates of equal treatment highlight the benefits of remote electronic access for attorneys and their clients. Remote electronic access reduces the price of legal services because electronic documents serve as a "form book" for attorneys to conveniently copy thereby saving time and effort.[65] In fact, the argument extends beyond the mere cost advantages for legal services. Remote electronic access reveals patterns to help attorneys predict the outcomes of litigation.[66] Predictability has two benefits. First, predictability informs litigation strategy and facilitates settlement based on expected outcomes.[67] Second, and more broadly, predictability increases societal productivity by promoting private economic planning in accordance with the certainty of outcomes.[68]

Finally, another set of arguments underscores the administrative convenience served by equal treatment. In one instance, remote electronic access has the potential to reduce common errors made by attorneys by detecting missing information, redacting sensitive information automatically, and reminding attorneys about filing deadlines.[69] This, of course, would require certain informational systems to create the appropriate functional technology. In response to the opponents' arguments about the cost to implement technologies and proper databases, proponents suggest outsourcing the labor and maintenance to private or public sector groups so as not to burden courts or the public.[70] Advocates also highlight that both the federal courts and Congress have successfully embraced equal access of electronic and paper records through the E-Government Act of 2002[71] and the implementation of the Public Access to Court Electronic Records (PACER) system.[72]

ELECTRONIC CASE FILES 7 (2001) (amended 2006) [hereinafter JUDICIAL CONFERENCE COMMITTEE].

[65] LoPucki, *supra* note 55, at 534.

[66] *Id.* at 498–99.

[67] *Id.* at 506–07.

[68] Edward A. Morse, *Reflections on the Rule of Law and "Clear Reflection of Income": What Constrains Discretion?*, 8 CORNELL J.L. & PUB. POL'Y 445, 456–57 n.52 (1999).

[69] LoPucki, *supra* note 55, at 511.

[70] Martin, *supra* note 37, at 880.

[71] 44 U.S.C. § 3501 (2006).

[72] Gregory M. Silverman, *Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records over the Internet*, 79 WASH. L. REV. 175, 203 (2004); *see also* Martin, *supra* note 37, at 864 ("The federal courts did not establish computer-based case management systems or subsequent electronic filing and document management systems in order to provide the public with better access to court records. Those systems were created because they offered major gains for judges and court administrators.").

B. Arguments in Favor of Restricting Remote Electronic Access to Court Documents

Opponents of equal treatment for paper and remote electronic records recognize that there is something inherently dissimilar about the methods of access to court documents. The disparities between paper records and remote electronic records involve several issues, including administration and cost, public safety, and litigation, discrimination, and privacy concerns. Opponents do not necessarily object to a policy permitting remote electronic access to court documents in its entirety, but rather, they argue that unfettered access is undesirable. While many of the arguments focus on the unique problems of remote electronic access, other concerns are present with respect to paper records as well, and these concerns may be further exacerbated in the electronic context.

One significant argument for opponents, which is also one of the most difficult questions posed to proponents of equal access, is the question of the cost of the technological infrastructure required to maintain electronic databases that provide remote access to the public. The cost issue expands beyond the necessary technological equipment and addresses certain labor concerns, such as converting paper files to electronic files and hiring personnel to provide security and maintenance for the databases.[73] The cost issue has intensified as legislatures and courts determine whether to charge the public for remote electronic access, and if so, how to establish fee systems.[74] Aside from monetary costs, remote electronic access to court documents raises concerns about the administrative burdens of physically providing access to databases and the increased opportunities for clerical error and data-entry mistakes.[75] The questions of administrative burdens, accountability, and responsibility become important with the introduction of redaction requirements into the public access doctrine.

[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 8 (2002) [hereinafter CCJ/COSCA GUIDELINES].

[74] *See* Victoria S. Salzmann, *Are Public Records Really Public?: The Collision Between the Right to Privacy and the Release of Public Court Records over the Internet*, 52 BAYLOR L. REV. 355, 375–76 (2000) (discussing the dilemma states face as they determine how to provide electronic access to the public).

[75] *See id.* at 375 ("Although clerical error has long been dealt with by the courts, the introduction of computer technology brings forth a renewed opportunity for data entry mistakes.").

Opponents also make several arguments highlighting how remote electronic access compromises public safety. For example, one concern is that the public, fearful of the release of private information over the Internet, might hesitate to comply with the government.[76] This is particularly apparent in two different circumstances. First, it raises a possibility that victims and witnesses will hesitate to come forward and citizens will be unwilling to serve as jurors.[77] Second, access to sensitive information may result in decreased suspect cooperation, which in turn could increase the number of cases that proceed to trial in lieu of disposal through plea agreements.[78] An additional public safety concern posits that remote electronic access to personal information increases and eases the opportunity for mischievous viewers to commit identity theft.[79] Furthermore, posting court records on the Internet may entice blackmail, stalking, extortion, and other crimes that threaten public safety.[80]

Opponents also focus on litigation concerns generated with a policy allowing remote electronic access to court documents. One concern is that posting court records on the Internet will burden courts further because of increased litigation by parties raising motions to seal records or requesting protective orders to shield their private information from public viewing.[81] A second concern introduces the possibility that Internet posting might increase pretrial publicity and taint the jury pool, which would perhaps prejudice the parties' right to a fair trial.[82] As advanced technology enhances communication through wireless networks and smart phones, serious ap-

[76] *Id.* at 377.

[77] Winn, *supra* note 48, at 328–29.

[78] *See* Letter from Michael A. Battle, Dir., Executive Office for U.S. Attorneys, U.S. Dep't of Justice, to James C. Duff, Sec'y, Judicial Conference of the U.S. (Dec. 6, 2006) (suggesting that placing documents online creates a "cottage industry" that republishes court records on websites exposing cooperators and leads to targeting witnesses, intimidation, harassment, and retaliation).

[79] Winn, *supra* note 48, at 317.

[80] Lynn E. Sudbeck, *Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence: An Analysis of State Court Electronic Access Policies and A Proposal for South Dakota Court Records*, 51 S.D. L. REV. 81, 83 (2006).

[81] *See* Winn, *supra* note 48, at 326 (arguing that federal courts may experience increased litigation demanding motions to seal or protective orders under the PACER system).

[82] *See* George F. Carpinello, *Public Access to Court Records in New York: The Experience Under Uniform Rule 216.1 and the Rule's Future in a World of Electronic Filing*, 66 ALB. L. REV. 1089, 1108 (2003) (discussing the problems of pretrial publicity and tainting the jury pool on the parties' right to a fair trial, particularly in cases that generate significant public attention).

prehension about jurors accessing the Internet and case information prior to or during trials creates cause for concern.[83]

A fourth point of contention addressed by opponents regarding the consequences of permitting remote electronic access to court documents concentrates on discrimination. Opponents argue that remote electronic access may promote inequality because litigants with the resources to resort to private judicial forums will have the option to do so, particularly if they have sensitive privacy concerns, while the remaining public must choose to either forego justice or litigate in the public courts.[84] This represents the phenomenon of the "vanishing trial" and recognizes the potential for an increase in litigants seeking alternative dispute resolution (ADR) mechanisms.[85] In fact, there may be a correlation between the expanding public access doctrine and the increase in contracts drafted with mandatory arbitration clauses to avoid public disclosures, and such clauses are potentially harmful to consumers.[86]

Another discrimination concern raises the idea that widespread availability of court information over the Internet may encourage employers and other entities to search and ultimately discriminate based on information present in the court documents.[87] For example, ChoicePoint Inc., a private company, has compiled and aggregated data on millions of individuals from various public records, which the government and employers use to screen and investigate

---

[83] Mary Flood, *Windows Opening and Doors Closing—How the Internet is Changing Courtrooms and Media Coverage of Criminal Trials*, 59 SYRACUSE L. REV. 429, 431 (2009); John Schwartz, *As Jurors Turn to Google and Twitter, Mistrials Are Popping Up*, N.Y. TIMES, Mar. 18, 2009, at A1.

[84] *See* Lewis A. Kaplan, J., S.D.N.Y., *Litigation, Privacy and the Electronic Age*, 4 YALE SYMP. L. & TECH. 1 (2001) (discussing the growing dissatisfaction with privacy mechanisms in the public courts, particularly in the electronic age, and the competing privacy benefits of alternative dispute resolution methods for those who can afford it); Winn, *supra* note 48, at 328–29.

> The world of cyber-justice should not be permitted to degenerate into a world . . . 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.

Id.

[85] Nancy S. Marder, *From "Practical Obscurity" to Web Disclosure: A New Understanding of Public Information*, 59 SYRACUSE L. REV. 441, 444–45 (2009).

[86] *Id.* at 445–46.

[87] James B. Jacobs, *Restorative Justice: Mass Incarceration and the Proliferation of Criminal Records*, 3 U. ST. THOMAS L. J. 387, 394, 401–02 (2006).

current and prospective employees.[88] Although the question of how ChoicePoint accessed this information in the past remains unclear, whether it accessed information through paper or electronic records, one can only imagine that remote electronic access to court documents will hasten and simplify the task.

A final area of concern relates to privacy rights and reaches the core of the First Amendment and common law disputes over the public access doctrine. Much of the conflict between proponents and opponents of remote access reveals the tension between public access rights and individual privacy rights. The question of privacy protection permeates all areas of law but is particularly controversial, especially with modern technology, in this area of information privacy. In *Whalen*, the Supreme Court of the United States indicated that privacy includes the interest in avoiding disclosure of personal matters.[89] More significantly, the Court suggested that the duty to avoid unwarranted disclosures "arguably has its roots in the Constitution."[90] Additionally, in *Reporters Committee for Freedom of the Press*, the Court noted that common law understandings of privacy include the premise that an individual has control over information concerning his person.[91] The struggle to define the appropriate balance between privacy and public access rights is even more ambiguous because the Supreme Court held that every court has supervisory power over its own records.[92]

One of the more significant privacy concerns that opponents raise to justify differential treatment focuses on the decline of practical obscurity.[93] More specifically, the practical obscurity of court records combined with the physical limitations of paper composition and storage capabilities creates an expectation of privacy that withers away with electronic records that are potentially available forever.[94] Arguably, this expectation of privacy due to practical obscurity and past technological limitations made additional protections for infor-

[88] Daniel J. Solove, *Modern Studies in Privacy Law: Notice, Autonomy and Enforcement of Data Privacy Legislation: Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1151 (2002).

[89] Whalen v. Roe, 429 U.S. 589, 599–600 (1977).

[90] *Id.* at 605.

[91] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

[92] Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 598 (1978).

[93] *See* discussion *supra* note 48.

[94] *Id.* at 316–17 (discussing a new concern in the electronic age about escaping the past and burying skeletons in the closet only for them to resurface many years later in an Internet search).

mation contained in court documents unnecessary—nonetheless, as the Internet continues to change the shape of communications, opponents argue that the time has come to revisit Justice Brennan's forewarning in *Whalen* and to reexamine the meaning of privacy and methods to ensure adequate privacy protection.[95]

Practical obscurity also serves an important role in minimizing the potential damage resulting from a mistake in the record. When records on the Internet contain mistakes, courts and citizens do not have the means to undo the damage.[96] With paper records, viewership is limited; however, with online dissemination, the chance that millions of people will have access to the information before parties and courts correct it is significantly greater.[97] Even if the responsible parties eventually correct the mistake, the courts and Internet viewers may have electronically stored and further disseminated incorrect versions. According to opponents, the risk of mistakes and Internet dissemination is disturbing because many individuals appear in court records involuntarily.[98] Generally, non-litigants do not have the opportunity to defend allegations and their reputations before the court to protect their interests.[99]

Providing remote electronic access to court documents also threatens individual privacy by providing viewers with the opportunity and ability to easily aggregate and disseminate information gleaned from online court documents at low costs, leading to the potential commercialization of court records.[100] The advancements made possible by the Internet encourage privatization of public information by enterprises engaged in the lucrative data-mining industry.[101] Although the data-mining industry evolved before the Internet and

[95] *See Whalen*, 429 U.S. at 607 (Brennan, J., concurring); *see also supra* notes 48, 94 and accompanying text.

[96] Marder, *supra* note 85, at 446–47.

[97] *Id.*

[98] *See* Natalie Gomez-Velez, *Internet Access to Court Records—Balancing Public Access and Privacy*, 51 LOY. L. REV. 365, 410 (2005) (arguing that people required to appear in court often do not willingly volunteer to participate in a public process). This argument may be less compelling for litigants, who arguably consent to publicizing their information presented in the court and who may have some control over what information is, in fact, presented.

[99] Carpinello, *supra* note 82, at 1107.

[100] *See* Winn, *supra* note 48, at 316 ("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.").

[101] *See* Gomez-Velez, *supra* note 98, at 378, 415–16 (discussing the virtual privatization of public information and vendor interest in reselling information found in court records).

electronic recordkeeping came to fruition, posting court documents online will increase the ease with which such information is accessed and aggregated.

C. Committee Reports and Positions

As courts and legislatures confront the intersection of technology and the public access doctrine, various committees have circulated guidelines and reports in response to the quandary. Two committees in particular have issued influential and conflicting reports: the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files ("JCC Guidelines")[102] and the Conference of Chief Justices and the Conference of State Court Administrators ("CCJ/COSCA Guidelines").[103] Although the Committees' advocate opposing positions, both Committees recognize that the judiciary must deny remote electronic access to certain records in some instances.

The JCC Guidelines recommend that in civil cases, the public should have equal access to both paper and electronic documents.[104] This recommendation aligns with the proponents' position advocating for equal treatment of paper and electronic records.[105] With respect to criminal cases, however, the JCC Guidelines stipulate that the public should not have remote electronic access to such cases at present.[106] The recommendations suggest that the Committee revisit the issue if the Committee learns that the benefits of public access

---

[102] The special Subcommittee was formed upon the request of the Judicial Conference of the United States to its Committee on Court Administration and Case Management directing an examination of the public access doctrine. JUDICIAL CONFERENCE COMMITTEE, *supra* note 64, at 1. The Subcommittee consisted of seven judges and one attorney. *Id.* Congress created the Judicial Conference of the United States to initiate and review policies governing the administration of the federal courts. *Judicial Conference of the United States*, U.S. COURTS, http://www.uscourts.gov/judconf.html (last visited Mar. 22, 2011).

[103] This project combined the efforts of the Justice Management Institute, the State Justice Institute, the Conference of Chief Justices, the Conference of State Court Administrators, the National Association of Court Management, and the National Center for State Courts. CCJ/COSCA GUIDELINES, *supra* note 73, at vi. These bodies endeavored to complete a comprehensive review of state court policies pertaining to the public access doctrine, ultimately drafting the Guidelines to provide a model policy for states to adopt. *Id.*

[104] JUDICIAL CONFERENCE COMMITTEE, *supra* note 64, at 6. As an exception, the JCC Guidelines recommend that Social Security cases be exempted from remote electronic access. *Id.*

[105] *See supra* Part III.A.

[106] *Id.* at 8.

significantly outweigh the dangers.[107] The Committee reasoned that safety concerns in criminal cases, including risks to cooperative defendants and law enforcement personnel, outweigh public access rights.[108]

In contrast to the JCC Guidelines, the CCJ/COSCA Guidelines assert that courts should restrict certain documents from online access based on the nature of the information.[109] The CCJ/COSCA Guidelines recommend excluding contact information, Social Security numbers, account numbers, graphic photographs, medical records, family law records, abuse-and-neglect records, and names of minor children.[110] In this respect, the Committee agrees with the opponents' arguments by advocating for differential treatment of paper and electronic records.[111]

IV. NEW JERSEY'S RESPONSE TO REMOTE ELECTRONIC ACCESS TO COURT DOCUMENTS

Just as state and federal courts across the nation addressed their public access doctrines in the face of changing technologies, New Jersey took action to review its rule governing public access to court documents. Amended Rule 1:38 represents a fundamental change in the public access doctrine as compared to the former Rule's framework because it endorses a presumption of openness unless exempted. Although the amended Rule's provisions do not address Internet accessibility explicitly, the Committee's recommendations, adopted by the New Jersey Supreme Court, discuss the gradual evolution of remote electronic accessibility. Consistent with the Rule's transformation, existing New Jersey case law advances a presumption of open access to court proceedings and documents.

A. *Former and Amended Rule 1:38*

Similar to courts and legislatures in other jurisdictions, New Jersey has recently considered the arguments in support of and against permitting remote electronic access to court documents. In 2006, the Chief Justice of the Supreme Court of New Jersey charged the

---

[107] *Id.*

[108] *Id.*

[109] CCJ/COSCA GUIDELINES, *supra* note 73, at 1 ("The nature of certain information in some court records, however, is such that remote public access to the information in electronic form may be inappropriate, even though public access at the courthouse is maintained.").

[110] *Id.* at 40.

[111] *See supra* Part III.B.

Supreme Court Special Committee on Public Access to Court Records (the "Committee") to conduct a comprehensive review of New Jersey's rules regarding public access to court records.[112] This was not the first time that the court addressed technology's ability to transform the public access doctrine. In 1994, the Information Systems Policy Committee, in conjunction with a special subcommittee on public access, issued a report that the court adopted in 1996.[113] The report concluded that, because electronic information is as public as paper records, court information should be available online.[114] At the time, however, technological limitations created obstacles to posting court information on the Internet.[115]

Now that technological advancements offer a practical solution to previous obstacles preventing remote electronic access, New Jersey unsurprisingly reevaluated its public access laws. This time, the court focused its assessment on Rule 1:38, which governs the public access doctrine in New Jersey. Pursuant to the Committee's report and recommendations, the supreme court adopted amended Rule 1:38 on July 22, 2009, which became effective on September 1, 2009.[116] The changes from former Rule 1:38 to amended Rule 1:38 are significant and represent a fundamental change in New Jersey's public access doctrine.[117]

Former Rule 1:38, as compared to the amended Rule, was narrow and incomplete. Former Rule 1:38 defined court records available for public access as only those records that were "required by statute or rule to be made, maintained or kept on file by any court, office or official within the judicial branch."[118] The Rule proceeded

[112] Letter from Barry T. Albin, Associate Justice and Chair of the Supreme Court Special Committee on Public Access to Court Records, Supreme Court of New Jersey, to Stuart Rabner, Chief Justice, Supreme Court of New Jersey, at i (Nov. 29, 2007), *available at* http://www.judiciary.state.nj.us/publicaccess/publicaccess.pdf [hereinafter Letter from Justice Albin to Chief Justice Rabner].

[113] REPORT, *supra* note 7, at 26–27.

[114] *Id.*

[115] *Id.*

[116] ADMINISTRATIVE DETERMINATIONS, *supra* note 5, at 1.

[117] *See* REPORT, *supra* note 7, at 9 ("This approach [amended Rule 1:38] is a significant departure from the current version of Rule 1:38 . . . . The proposed rule is intended to replace the common law 'balancing of interests' test with an absolute right of access to all non-exempt court and administrative records."). Under the former Rule, if a request for access fell outside the scope of Rule 1:38, the requester would have to assert a common law right of access claim and the court would have to balance the parties' interests. *Id.* at 34. Under the amended Rule, an absolute right exists unless explicitly exempted. *Id.*

[118] N.J. CT. R. 1:38 (1969) (amended 2009) ("All records which are required by statute or rule to be made, maintained or kept on file by any court, office, or official

to list ten exceptions for records exempted from public access.[119] Despite the listed exceptions, several other exceptions were scattered throughout the court rules, statutes, and case law.[120]

In contrast to former Rule 1:38, amended Rule 1:38 attempts to address many of the inadequacies and inconsistencies plaguing New Jersey's public access doctrine. The Committee undertook its review with the general presumption that court records are open to the public.[121] In fact, the amended Rule presumes that court records are open to the public unless exempted, and the amended Rule codifies all of the allowable exceptions to this presumption.[122] The amended Rule's policy statement pronounces that court records "within the custody and control of the judiciary are open for public inspection and copying except as otherwise provided in this rule."[123] While the exceptions to this general presumption of openness are numerous, the amended Rule indicates that "[e]xceptions enumerated in this rule shall be narrowly construed in order to implement the policy of open access to records of the judiciary."[124]

within the judicial branch of government shall be deemed a public record and shall be available for public inspection and copying, as provided by law, except . . . .").

[119] N.J. CT. R. 1:38 (a)–(j). The exceptions excluded personnel and pension records, criminal, family, and probation records, completed jury questionnaires and the preliminary lists of jurors, records required to be kept confidential under statute, rule, or court order, records pertaining to pretrial intervention programs, cases approved for mediation, reports by judges that are submitted to the Administrative Director of the Courts, records maintained by the Judicial Performance Committee, and certain discovery materials relating to pre-indictment discovery, prearraignment conferences, plea offers, arraignment/status conferences, pretrial hearings, and pretrial conferences. *Id.*

[120] Letter from Justice Albin to Chief Justice Rabner, *supra* note 112, at i.

[121] *Id.*; *see also* REPORT, *supra* note 7, at 25 ("An open and transparent court system is an integral part of our democratic form of government.").

[122] Letter from Justice Albin to Chief Justice Rabner, *supra* note 112, at i.

[123] N.J. CT. R. 1:38-1 (2009). Court records are defined as:

> (1) any information maintained by a court in any form in connection with a case or judicial proceeding, including but not limited to pleadings, motions, briefs and their respective attachments, evidentiary exhibits, indices, calendars, and dockets; (2) any order, judgment, opinion, or decree related to a judicial proceeding, (3) any official transcript or recording of a public judicial proceeding, in any form; (4) any information in a computerized case management system created or prepared by the court in connection with a case or judicial proceeding; (5) any record made or maintained by a Surrogate as a judicial officer.

N.J. CT. R. 1:38-2.

[124] N.J. CT. R. 1:38-1. For the most part, the various exceptions in the amended Rule embody all of the exceptions listed in the former Rule, along with additional provisions. *Compare* N.J. CT. R. 1:38 (a)–(j) (1969), *with* N.J. CT. R. 1:38-3 (a)–(f) (2009). It is worth noting how a rule that provides for more exceptions to access can

Two significant departures from the former Rule to the amended Rule involve the amended Rule's mandatory redaction of confidential personal identifiers ("CPIs") and the sealing procedure. Amended Rule 1:38 requires parties to redact CPIs from any documents submitted to the court, including Social Security numbers, driver's license numbers, vehicle plate numbers, insurance policy numbers, active financial account numbers, and active credit card numbers.[125] Additionally, the amended Rule explicitly establishes a standard for sealing court records by codifying the common law test of good cause.[126] More so, amended Rule 1:38 also provides for the unsealing of court records by motion and places the burden on the non-movant to prove that good cause to continue sealing the record still exists.[127] Former Rule 1:38 made no direct reference to redaction requirements for confidential information or sealing and unsealing procedures.

Although the provisions in amended Rule 1:38 do not address Internet posting explicitly, the Committee's recommendations, ultimately approved by the supreme court, suggest that the judiciary consider posting court documents on the Internet.[128] The fundamental change from former Rule 1:38 to the creation of a presumption of openness unless exempted in amended Rule 1:38 fuels the question of how far this presumption carries in the context of Internet posting. Notably, the Committee emphasized that not all records are appro-

still result in greater access. The exceptions in the amended Rule are the only restrictions placed on public access in the universe of court records. The former Rule mandated public access *only* to records required to be made or maintained by the judiciary and further restricted access by providing for exceptions.

[125] N.J. CT. R. 1:38-7(a) (2009). The Rule permits that an "active financial account number may be identified by the last four digits when the financial account is the subject of the litigation and cannot otherwise be identified," or, in the case of other personal identifiers, when statutes, rules, administrative directives, or court order requires such identifying information to remain in the documents. N.J. CT. R. 1:38-7(b). The Rule does not require a party to redact a driver's license number that the New Jersey Motor Vehicle Commission requires to be included in documents relating to the suspension and reinstatement of licenses. N.J. CT. R. 1:38-7(e).

[126] N.J. CT. R. 1:38-11(a)–(b). The Rule defines good cause as when "(1) [d]isclosure will likely cause a clearly defined and serious injury to any person or entity; and (2) [t]he person's or entity's interest in privacy substantially outweighs the presumption that all court and administrative records are open for public inspection pursuant to R. 1:38." N.J. CT. R. 1:38-11(b)

[127] N.J. CT. R. 1:38-12.

[128] *See* REPORT, *supra* note 7, at 14 ("As resources permit, the Judiciary should develop and implement a public access system whereby records are made available over the Internet without charge."). The recommendations suggest that Internet posting begin with civil docket and criminal conviction information. *Id.*

priate for online dissemination.[129] In particular, the recommendations acknowledge that "there is a difference between releasing electronic records in response to a specific request and actively publishing those records on the Internet."[130] Furthermore, the Committee recognized the tension between public access rights and individual privacy rights and stated that "[b]ecause of privacy concerns, the Judiciary should proceed cautiously with Internet posting after further study."[131]

The Committee's report specifies particular areas where differential treatment of paper and remote electronic records is advisable. One area involves the content of the information posted on the Internet. The recommendations propose that courts exclude an individual's full date of birth and home address and include only the birth year and the municipality and state of residence for remote electronic records, but not for paper records available at the courthouse.[132] The Committee reasoned that differential treatment was appropriate because of concerns about identity theft with mass proliferation of sensitive information over the Internet.[133] Another area where unequal treatment evolves is in the type of records permitted for online posting. For instance, the Committee advised against posting family and municipal docket information on the Internet at present until courts conduct further analysis.[134] Additionally, the recommendations advocate for Internet posting of conviction-only criminal-docket information.[135] The Committee expressed concern about courts publishing information in the case of wrongly accused and overcharged defendants whom the courts have found not guilty.[136]

The Supreme Court of New Jersey responded to the Committee's report by approving a majority of the recommendations underlying the amendments to Rule 1:38, including all of the recommen-

---

[129] *Id.* at 12–13 ("[N]ot all electronic records should be posted on the Internet.").

[130] *Id.* at 14 ("Internet posting results in a hyper-dissemination of court records, raising concerns different from those related to specific requests for court records.").

[131] *Id.*

[132] *Id.*

[133] *Id.* at 35.

[134] REPORT, *supra* note 7, at 14. The recommendations do not specify who should conduct further analysis, although the Committee did recommend that the Administrative Director appoint a permanent Advisory Committee on Public Access. *Id.* at 59. The Administrative Director and the Advisory Committee would work with the supreme court to address future concerns regarding public access to court documents. *Id.* at 9–10.

[135] *Id.* at 15.

[136] *Id.* at 54–55.

dations involving remote electronic access.[137] The court did, however, modify and reject some of the other recommendations that were unrelated to Internet access, which complicates the predictability of future outcomes in disputes regarding the public access doctrine and interpretations of the amended Rule.[138]

B. *New Jersey Court Decisions*

Traditionally, New Jersey courts have determined that the public has a broad right to inspect court documents, although cases addressing the public access doctrine itself are relatively rare. The cases that concentrate on the public access doctrine rely on a common law right of access claim, and courts have made their decisions based on the common law "balancing of the interests" test. Accordingly, the case law primarily involves balancing the parties' interests in the context of sealing motions and does not readily rely on former Rule 1:38 as a decision-making tool.[139] Nonetheless, understanding the roots of the public access doctrine in New Jersey is important to assess the potential future impact and consequences of the amended Rule.

In New Jersey, the Legislature recognized the public right to attend judicial proceedings as early as the 1677 Concessions and Agreements of West New Jersey.[140] In 1879, the New Jersey Supreme Court acknowledged the existence of a public right to inspect court

[137] *See* ADMINISTRATIVE DETERMINATIONS, *supra* note 5. The full supreme court reviewed the Committee's report and subsequently drafted its Administrative Determinations concerning the Committee's recommendations.

[138] *Id.* For instance, the court broadened the presumption of openness by rejecting the Committee's recommendation that complaints alleging indictable and disorderly person offenses be deemed confidential. *Id.* at 7. But the court also narrowed the presumption by modifying the recommendation concerning financial records of guardians and requiring that such records remain confidential as to unrelated parties. *Id.* at 7–8.

[139] For reasons why, see *supra* note 117 and accompanying text. Recently, the New Jersey Supreme Court relied on Rule 1:38 to justify eliminating the initial pleadings exception to the fair-report privilege in defamation cases because the exception contradicted the Rule's principles and purpose with respect to expanding public access to filed pleadings. Salzano v. North Jersey Media Group Inc., 993 A.2d 778, 790 (N.J. 2010).

[140] Hammock v. Hoffman-Laroche, Inc., 662 A.2d 546, 553 (N.J. 1995); *see generally* 1677 Concessions and Agreements of West New Jersey, *reprinted in* SOURCES OF OUR LIBERTIES 188 (Richard L. Perry ed., American Bar Foundation, 1959) ("That in all publick courts of justice for tryals of causes, civil or criminal, any person or persons, inhabitants of the said Province may freely come into, and attend the said courts, and hear and be present, at all or any such tryals as shall be there had or passed, that justice may not be done in a corner nor in any covert manner.").

documents when it awarded a citizen the right to inspect tax records subject to litigation.[141]

The leading case on the public access doctrine in New Jersey is *Hammock v. Hoffman-Laroche, Inc.*[142] In *Hammock*, the New Jersey Supreme Court held that there was a common law presumption of public access to court documents, and the court established a reasonableness standard to determine when a party properly rebuts the presumption.[143] The court noted that the presumption applies to all materials filed with the court if they are relevant to any material issue in the case.[144]

After the *Hammock* decision, the lower courts indirectly addressed the presumption of open access in the context of Internet accessibility. In *Smith v. Smith*, the court warned that "[l]ooming technological developments may warrant the judiciary to reconsider, prospectively, the current balance of interests in favor of open court proceedings."[145] The court emphasized that technology permits remote research by "prospective employers, business associates, loan officers, government regulators, social clubs, and perhaps even would-be Saturday night dates."[146] Nearly five years later and with the aid of amended Rule 1:38, the time has come for the judiciary to determine

---

[141] Ferry v. Williams, 41 N.J.L. 332, 339 (N.J. Sup. Ct. 1879).

> The present controversy relates to a matter of public police of universally recognized importance, concerning a traffic which, in the opinion of many, largely adds to the disorders of society and the burdens of taxation; and it cannot be alleged that private interests are not as much involved in its due regulation by law as they are in other public questions about which heretofore individuals have maintained a standing in this court.

Id.

[142] 662 A.2d 546, 546 (N.J. 1995).

[143] *Id.* at 556. The court outlined that the need for secrecy must be specific to each document and must be based on a current justification for privacy protection. *Id.* at 559.

[144] *Id.* at 558–59.

[145] 879 A.2d 768, 775–76 (N.J. Super. Ct. Ch. Div. 2004). "It is not hard to imagine that each scurrilous allegation contained in some court filing could eventually turn up in a 'Google search.'" *Id.* at 775.

[146] *Id.* at 775. In a recent decision, the Supreme Court of New Jersey declared that the plaintiff did not have a reasonable expectation of privacy in conviction information, despite an expungement order, because court documents are widely disseminated and available for public access over the Internet. G.D. v. Kenny, A-85 (September Term 2009), 2011 N.J. LEXIS 87, at *39–40 (N.J. Jan. 31, 2011) ("The expungement statute—enacted at a time when law enforcement and court documents may have been stored in the practical obscurity of a file room—now must coexist in a world where information is subject to rapid and mass dissemination.").

how technology will alter the balance between public access rights and individual privacy rights.[147]

V. UNANSWERED QUESTIONS AND CONSEQUENCES RAISED BY AMENDED RULE 1:38 AND PROPOSED ANSWERS AND RECOMMENDATIONS

Amended Rule 1:38 does not reference Internet access to court documents explicitly.[148] This ambiguity challenges any assessment of the future impact of the Rule as it relates to the public access doctrine. The recommendations promulgated by the Committee and ultimately approved by the Supreme Court of New Jersey manifest that Internet accessibility will come to fruition in the near future. As courts transition to posting documents on the Internet, however, several unanswered questions and consequences remain. Many of these consequences echo the concerns of those advocates in favor of placing restrictions on Internet access. Because amended Rule 1:38 fundamentally alters the former Rule and leaves the future of Internet accessibility to the discretion of the supreme court,[149] New Jersey may face some unique obstacles as it embarks on its quest to provide remote electronic access to the public. Fortunately, by leaving a majority of the implementation policies open to further analysis and review, the court can create guidelines to ensure compliance with the recommendations and the founding principles of amended Rule 1:38 while simultaneously balancing necessary individual privacy protections.

A. *The Necessity for an Enforcement Provision Appended to the Redaction Requirements*

One gap in amended Rule 1:38 that must be addressed pertains to the redaction of confidential personal identifiers (CPIs).[150] The

[147] *See infra* note 149 and accompanying text.

[148] The recommendations state that, "[t]he statute should not include references to any specific technology, given the rapidly changing technological environment in which the courts operate." ADMINISTRATIVE DETERMINATIONS, *supra* note 5, at 9.

[149] *Id.* at 6–7 ("Given the rapid changes in technology, the Supreme Court should determine on a periodic basis the appropriate court data for posting on the Internet . . . . The Supreme Court should make those determinations on an administrative basis without amending the public access rule."). Whether the supreme court will view this proclamation as merely a discretionary grant of power or as a responsibility to remain pro-active and vigilant when monitoring the policy remains unclear. The language of the statement, particularly the word *should*, appears to support the latter interpretation.

[150] *See* N.J. CT. R. 1:38-7 (2009) ("A party shall not set forth confidential personal identifiers as defined in R. 1:38-7(a) in any document or pleading submitted to the

Rule does not include an enforcement provision for attorneys and parties who fail to redact. Proper compliance with this provision becomes especially important as the court implements guidelines and policies to govern the dissemination of information on the Internet. Because of the wide audience and their ability to easily view court documents on the Internet, the inadvertent release of confidential information, such as a Social Security number or an active financial account number, could be devastating to the victim.[151] The court, by approving the recommendations and provisions of amended Rule 1:38, recognized the importance of concealing such confidential information from public access in both paper and electronic records.[152]

Amended Rule 1:38 places the burden of redacting CPIs on attorneys and parties as opposed to court personnel.[153] The Rule requires parties to certify that they have redacted CPIs from any documents that they have submitted to the court.[154] But a certification requirement may not be potent enough to deter negligent filing. The Rule is unclear about the consequences of providing certification without proper redaction. Two outcomes are likely to result from this ambiguity. First, courts could choose to adopt the procedure established in Rule 1:4-8.[155] Rule 1:4-8 states that by signing the

court unless otherwise required by statute, rule, administrative directive, or court order . . . .").

[151] *See* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & TECH. 1, 12–13 (2008) (discussing how the Internet eases the process of data aggregation and significantly increases the opportunity for identity theft); *Identity Theft*, THE NAT'L CTR. FOR VICTIMS OF CRIME, http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32359#5 (last visited Dec. 25, 2010) (discussing the effects of identity theft on victims, including poor credit status, time and effort to correct mistakes, costs, and psychological scars).

[152] *See* R. 1:38-7 (requiring the redaction of personal identifiers from all documents submitted to the court); *see also* ADMINISTRATIVE DETERMINATIONS, *supra* note 5, at 1 (indicating that some personal identifiers should remain confidential and should be redacted from court documents).

[153] *See* R. 1:38-7(c) (declaring that a *party* must avoid placing CPIs in court documents, and requiring *parties* to certify pleadings and Case Information Statements in accordance with the redaction requirements); *see also* REPORT, *supra* note 7, at 11 ("Court staff should not be required to redact confidential personal identifiers in existing court records or included in court records filed in the future . . . .").

[154] If a Case Information Statement is required, it must include a certification statement indicating that CPIs have been redacted. R. 1:38-7(c)(1). If no Case Information Statement is required, parties must, in the first filed pleading, include the language, "I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b)." *Id.* R. 1:38-7(c)(2).

[155] N.J. CT. R. 1:4-8 (1994). This Rule governs frivolous litigation in the form and execution of papers. *Id.*

document, the attorney certifies that he has read the document and that the information is accurate.[156] If no signature appears or if the signed document contains deficiencies, the document is stricken and an adverse party or the court may seek sanctions.[157] In the case of a party's failure to redact information in violation of the certification requirement, courts could apply a similar rationale to Rule 1:4-8 and equate the certification with the signature of approval of the truthfulness and accuracy of the document. Alternatively, a client injured as a result of an attorney's failure to redact the proper CPIs might file a legal malpractice claim against the negligent attorney.

The problem with these two alternatives is their restrictiveness. For instance, Rule 1:4-8 benefits only the parties because the parties are the sole entities—aside from the court itself—in a position to make a motion to impose court-ordered sanctions.[158] Rule 1:4-8 does not adequately protect third parties who, quite conceivably, are injured by an attorney's failure to redact their confidential information. Similarly, malpractice claims are obviously deficient if the individual affected by the release of the confidential information is not the attorney's client but is in fact a third party.[159]

An enforcement provision specific to the failure to redact in accordance with Rule 1:38 might remedy the inadequacies of the certification requirement and provide stronger protections. Unlike Rule 1:4-8 or a legal malpractice claim, the enforcement provision could be available not only to clients and parties but also to other persons involved in the litigation and third persons affected by the non-compliant party's negligence.[160] This would ensure protection, or at least recourse, for the personal information of witnesses and victims

[156] N.J. CT. R. 1:4-8(a).

[157] N.J. CT. R. 1:4-8(a)–(b).

[158] N.J. CT. R. 1:4-8(a). Although courts may order sanctions *sua sponte*, they may be unwilling to do so for any number of reasons.

[159] The New Jersey Supreme Court has loosened the privity requirement obstructing many third-party legal malpractice suits, and held that an attorney has a limited duty to specific non-clients. Petrillo v. Bachenberg, 655 A.2d 1354, 1357–59 (N.J. 1995). The duty extends to third parties whom the attorney should have known would rely on the lawyer's professional work. *Id.* at 1359. A third party affected by the attorney's failure to redact would unlikely qualify as a non-client to whom the attorney owes a specific duty, which is a necessary element to assert a legal malpractice claim.

[160] *Cf.* R. 1:4-8(a)–(b) (stipulating that only an adverse party or the court can raise the prospect of sanctions); *see supra* note 159 and accompanying text.

identified in the court record.[161] By expanding the reach of the redaction requirements and the potential liability risks, the enforcement provision might deter carelessness and encourage attentiveness. An enforcement provision is an especially relevant concern because the results of a pilot study performed in the federal courts, which authorized remote electronic access to criminal case records, revealed that a redaction requirement similar to Rule 1:38's requirement was a disaster to implement.[162] In fact, in certain circumstances, the experience resulted in complete failure to redact any confidential information from documents posted online.[163] Rather than comply with the redaction requirements, some courts merely added exceptions to the list of documents excluded from online access because redaction was simply too difficult.[164] Defense attorneys in several districts reported that courts often waived sanctions for a party's failure to redact.[165]

Including appropriate penalties in the enforcement provision is important in order to grant significance to the redaction requirements. For example, the enforcement provision might resemble the sanctions embodied in N.J. Court Rule 1:20-15A, which governs attorney misconduct and discipline.[166] One such sanction may include reprimand or admonition, but more serious or repetitive violations could result in censure or suspension from the bar.[167] Other penalties might include sanctions similar to those established in Rule 1:4-8, including monetary payments to the court or to the victim.[168] Additionally, the enforcement provision should include language that a showing of actual harm caused by the exposure is not necessary and that any penalties are prophylactic, available merely on the basis that information required to be redacted under Rule 1:38 was not in fact

[161] The names and addresses of victims or alleged victims of domestic abuse or sexual offenses are statutorily excluded from public access. N.J. CT. R. 1:38-3(c)(12) (2009).

[162] RAUMA, *supra* note 49, at 12–14.

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] N.J. CT. R. 1:20-15A (2009) (describing sanctions and conditions for disciplining members of the bar).

[167] *See* N.J. CT. R. 1:20-15A (3)–(6) (listing examples of possible sanctions for attorney misconduct).

[168] N.J. CT. R. 1:4-8(b) (1994). As mentioned previously, Rule 1:4-8 is itself insufficient to protect victims from an attorney's negligent failure to redact CPIs. *See supra* note 158 and accompanying text. But, the type of sanctions listed in the Rule provides a possible framework for the creation of an enforcement provision.

redacted. Requiring victims to show actual harm to punish negligent attorneys and litigants who violated a court rule is insulting.

B. RESTRICTING INTERNET ACCESS TO COURT-GENERATED DOCUMENTS ONLY

Another consequence of New Jersey's transition towards remote electronic access to court documents is the possibility of increased litigation, particularly in the form of sealing motions.[169] Conceivably, parties worried about shielding their information from public viewership on the Internet will run to courts to request sealing orders. Even with the redaction requirements, the category of CPIs is quite limited, and embarrassing and sensitive information will most likely fall outside the reach of the redaction requirements. In the past, parties relied on practical obscurity to protect their interests,[170] mitigating the need for greater protections beyond the occasional sealing orders requested for particularly sensitive information. But as the Internet threatens to erode practical obscurity, the litigation strategy is changing and forcing parties to pursue additional judicial mechanisms to protect information that was, at one time, virtually hidden from public inspection.

Rule 1:38 establishes a lofty standard to seal records, which further complicates the problem. The test requires the existence of good cause, which is present only when disclosure will cause a serious and specific injury and the individual's privacy substantially outweighs the public's right to access.[171] While this standard essentially codifies the prior common law test,[172] it may theoretically result in a stricter standard because the Rule now expresses an absolute presumption of openness unless exempted. Moreover, the Rule provides for an unsealing procedure and places the burden on the proponent to prove that good cause still exists to justify maintaining the seal.[173]

[169] *See* Winn, *supra* note 48, at 326.

[170] *Id.* at 316 ("The 'practical obscurity' of old records generates an expectation of privacy that has been recognized as legitimate by common law courts.").

[171] N.J. CT. R. 1:38-11(a)–(b) (2009).

[172] REPORT, *supra* note 7, at 9.

[173] N.J. CT. R. 1:38-12. The "reverse burden" was adopted by the court based on its decision in *Hammock*. REPORT, *supra* note 7, at 44. In *Hammock*, the court determined that

> [t]he person with the burden of proof [the proponent for continued sealing] must present evidence to show why public access to the documents should be denied currently rather than rely on the fact that a protective order was entered earlier. When a person intervenes in a case to inspect and copy documents that have been sealed, a reassess-

With a more stringent sealing standard and the threat of public exposure looming large, two circumstances are likely to occur. First, parties may fail to make a complete record to preserve their privacy.[174] This raises due process concerns about the right to a fair trial when a party must choose between privacy and fairness. Second, parties with adequate resources might turn to private forums, including ADR alternatives, to settle their disputes.[175] While this scenario may lighten the courts' workloads, particularly as courts are already overcrowded and overburdened, the negative consequences outweigh the benefits. Specifically, this situation presents concerns about economic discrimination and threatens the integrity of the judicial system.[176] If a consequence of the Rule is that it promotes the use of private resolution mechanisms because the public feels that the courts are inadequate to protect its interests, then the public trust in the judiciary is negatively affected. This is perverse because the goal of the Rule is to increase judicial transparency and public confidence in courts.[177]

One solution to combat the increase in sealing motions and the migration to private forums is to restrict Internet access to court-generated documents only, including opinions, judgments, dockets, indexes, and calendars.[178] Many courts, including the New Jersey state courts, already post some of these documents on their websites.[179] The benefit of this compromise is two-fold: it preserves judicial transparency and balances individual privacy rights. In particular, it would

> ment of whether documents should remain under seal must be based on a *current* justification for privacy.

Hammock v. Hoffmann-Laroche, Inc., 662 A.2d 546, 559 (N.J. 1995) (emphasis added).

[174] *See* Salzmann, *supra* note 74, at 377 ("Individuals will be hard pressed to release personal information to the government if they believe that information will be distributed around the world.").

[175] Marder, *supra* note 85, at 444–45.

[176] *See* text accompanying note 84.

[177] *See* REPORT, *supra* note 7, at 30, 44 (declaring that transparency is the guiding principle supporting the Rule and that public trust and confidence in the judiciary is only achieved through open access to court documents).

[178] *See* Sudbeck, *supra* note 80, at 119–20 (arguing to restrict Internet access to court-generated documents only because such a policy would still demonstrate to the public how the judiciary is functioning, which is one of the central tenets of the public access doctrine).

[179] REPORT, *supra* note 7, at 25 (noting that since its launch in 1995, the Judiciary Website includes decisions of all New Jersey state courts, "the Rules of the Court, jury charges, legal forms, and step-by-step kits for self-represented litigants"). For examples of the materials, see *New Jersey Courts*, N.J. JUDICIARY, http://www.judiciary.state.nj.us/ (last visited Mar. 22, 2011).

protect the long-established expectation of practical obscurity[180] and discourage parties from zealously seeking sealing orders or resorting to private forums. Additionally, this recommendation is consistent with the presumption of openness because the entire case file would remain available at the courthouse.[181] For further review, the interested public could still opt to travel to the courthouse to retrieve the complete paper record.

C. Questions of Timing

1. Limiting the Time Frame for Release to Records Filed After September 1, 2009

One of the unanswered questions evinced in the wake of Rule 1:38's ambiguities concerns the timing for Internet posting. The recommendations pronounce that the redaction requirements for CPIs apply prospectively.[182] Neither the Rule nor the recommendations address whether and to what extent courts will place old records on the Internet without the protections offered by the redaction requirements. Prior to the enactment of amended Rule 1:38 in July 2009, parties did not necessarily expect to discover their cases files displayed on the Internet, and therefore, parties may have relied on practical obscurity in lieu of taking more proactive steps to protect their private information, such as seeking to seal certain documents.[183]

One possible resolution is to limit the time frame for release. Specifically, the guidelines should clarify that court records filed before September 1, 2009—the effective date of amended Rule 1:38[184]—are not eligible for Internet posting. Not only would posting prior records compromise expectations of privacy, but it would also place

[180] *See* Sudbeck, *supra* note 80, at 121 ("Requiring the public to access these files in the courthouse rather than in their living room will provide some protection to this public information, as is currently provided by the concept of the 'practical obscurity' of these files in the clerks' offices.").

[181] *Id.* at 119–20 (advocating for courts to permit electronic public access to all documents at public terminals located in the courthouse, which eases public accessibility and administrative convenience).

[182] REPORT, *supra* note 7, at 11.

[183] Although the Supreme Court of New Jersey adopted the recommendations of the Information Systems Policy Committee in 1996, which implicated the judiciary's desire to expand the public access doctrine to include the Internet, the technological reality at the time was dubious. *Id.* at 26–27. Therefore, parties likely would still suspect that their private information would continue to be hidden by practical obscurity.

[184] ADMINISTRATIVE DETERMINATIONS, *supra* note 5, at 1.

burdens on court personnel to transform paper records into electronic form or electronic records into compatible data forms.[185] Additionally, parties have not been required to redact prior records, and forcing upon court personnel the overwhelming task to sift through prior records to redact sensitive information is plainly contrary to the Rule's designation of redaction burdens.[186] In the worst-case scenario, courts could post prior records containing personal identifiers, which would certainly lead to abuse and criminal mischief. Again, this recommendation will not compromise the public access doctrine because prior records will remain available in full at the courthouse.

2. Establishing a Time Schedule that Permits Immediate Remote Electronic Access to Limited Documents upon Filing

Another timing concern involves determining at what stage in the proceedings courts will be required to release particular documents. For instance, if the presumption of openness applies immediately upon filing, then courts must make documents available in real time for public inspection in the courthouse or over the Internet.[187] This would permit access prior to any actual proceedings taking place, at least with respect to pleadings, discovery, and pre-trial motions. One major concern is that premature release will create pre-trial publicity and prejudice the jury.[188] This prospect threatens the integrity of the court process, and it impinges upon the founding principles of fairness and justice.[189] Because of the concern about the spread of pretrial information, applying the same timing principle for both paper and electronic records is appropriate. This notion, how-

---

[185] *See* Daniel J. Lynch, *Litigation: Assessing the Electronic Case Filing Experience in the District of New Hampshire*, 47 N.H. BUS. J. 12, 16 (2006) (discussing how electronic filing has increased the time-intensive workload of intake and case managers, particularly because court personnel must scan and upload paper records into the computer system to create an electronic docket). The question is whether this would even be practicable, particularly for county courts, which are already overtaxed with their current workloads.

[186] *See* REPORT, *supra* note 7, at 16 ("Court staff should not be required to redact confidential personal identifiers in existing court records or included in court records filed in the future . . . .").

[187] For example, the federal PACER system posts case information on its Internet server in real time, once the information is updated in a court's case management system. *Frequently Asked Questions*, ADMIN. OFFICE OF THE U.S. COURTS, http://pacer.psc.uscourts.gov/faq.html#AR6 (click on "Case Related" tab and then "How Soon after a document is filed will it be in PACER?") (last visited Dec. 25, 2010). For more information on the PACER system, *see infra* note 201.

[188] Carpinello, *supra* note 82, at 1108.

[189] *See id.*

ever, is more pressing in light of Internet accessibility because of the relative ease and simplicity with which potential jurors and news broadcasters could access such information.[190] The results create a serious interference with justice and hinder the ability of courts to perform their duties effectively. In addition, if courts release the records immediately upon filing, parties do not have any lag time to seek a motion to seal sensitive information or correct mistakes. Once released, the damaging information is available to the entire public, regardless of whether the information was eligible for sealing under Rule 1:38.

Three possible sets of time schedules exist to guide courts. First, courts could release documents immediately upon filing. As previously noted, this is inadequate to protect the case from pretrial exposure.[191] Another approach is to release all records, both at the courthouse and on the Internet, only after final adjudication of the matter. This time schedule provides lag time for the parties to make a motion to seal information they hope to protect before courts release it to the public. This answer is not without tribulations, however, because cases today are heavily motion-based and the stages leading to the trial are quite prolonged.[192] Unless the motion is dispositive, such as a summary judgment motion, courts may not release the case records for a substantial period of time after the parties file their initial pleadings.[193] A third middle-ground approach would require courts to release records available at the courthouse immediately upon filing while delaying the release of the entire record on the Internet, possibly until final disposition. Courts could release certain information, such as court-generated documents, on the Internet immediately.[194] This approach maintains the presumption of openness while alleviating many of the timing concerns because the limited online materials immediately provide the interested public with enough information to seek complete files at the courthouse.

---

[190] Flood, *supra* note 83, at 431; Schwartz, *supra* note 83.

[191] *See supra* notes 82–83, 188 & 190 and accompanying text.

[192] Statistics from New Jersey indicate that the case processing time from filing to disposition for civil cases at the trial level range from 12–24 months, depending on the track. NAT'L CTR. FOR STATE COURTS, CASE PROCESSING TIME STANDARDS IN STATE COURTS, 2007 app. B (2009), *available at* http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/ctadmin&CISOPTR=1409.pdf. For criminal cases at the trial level, the time from complaint to pre-indictment disposition is two months, while the time from indictment to post-indictment disposition is four months. *Id.*

[193] *See id.* (discussing the case processing times in New Jersey trial courts).

[194] *See supra* Part V.B.

This timing schedule also protects much of the information from hyper-dissemination on the Internet prior to final judgment.

D. Establishing a Fee System to Offset Costs

Rule 1:38 raises an additional unanswered question regarding the creation and maintenance of an Internet database and associated costs. Neither the recommendations nor the provisions of Rule 1:38 specify how to create and maintain the appropriate databases or how the judiciary will fund the project. The issue of cost arises in a time of financial strife and as the State of New Jersey has an outstanding debt of nearly $35 million.[195] The cost issue is significant because it ultimately affects the taxpayers and the general public.

One suggestion to assist with the costs of providing remote electronic access, advocated by proponents of equal access for paper and electronic records, is to privatize the task of creating and maintaining the databases.[196] Privatizing database management, however, leads to several different issues, including the extent to which the private sponsors might actually restrict access through usage costs and user provisions.[197] Clearly, this would defeat the purpose of the amended Rule, which is to open up the channels for public access.[198]

Another suggestion is to charge user fees for Internet access to court documents.[199] The benefit of access fees is that such fees would help the State recover the significant costs involved in creating and maintaining the infrastructure necessary to provide Internet accessi-

---

[195] Dustan A. McNichol, *A Budget Weighed Down by Old Debt*, N.Y. TIMES, Apr. 12, 2009, at NJ1.

[196] *See* text accompanying note 70.

[197] *See* Gomez-Velez, *supra* note 98, at 417 ("[T]he primary concern should not be in the provision of wider (or 'jazzier') public access by private vendors but rather should be focused on providing effective access and avoiding circumstances under which private vendors might seek to 'privatize' and restrict access to public information."); Martin, *supra* note 37, at 880 ("By leaving court data in the custody of a private firm, however, the outsourcing of electronic filing and document management systems opens a completely new set of issues around public access . . . .").

[198] *See* REPORT, *supra* note 7, at 25 (discussing the context for the public access policy and the amended Rule as requiring an open court system to enhance a democratic society).

[199] The Committee considered the question of user fees to help recover the costs associated with initiating Internet access, but recommended that the judiciary conduct a cost-benefit analysis before making any decision regarding fees. *Id.* at 50. The Committee determined that the records should be posted without charge until such analysis is performed, at which time the judiciary should revisit the question of user fees. *Id.*

bility.[200] Additionally, charging a modest access fee will likely deter mischievous and casual perusal while still providing access to interested individuals. An example of a successful fee system is the federal PACER system.[201] PACER charges users $0.08 per page that results from any search, and the fee applies irrespective of whether or not the user views, prints, or downloads the pages.[202]

E. Creating a Login Mechanism

One additional suggestion that relates generally to guide the process of providing remote electronic access to court documents is to permit access only to those users who have registered and received a username and password. The login mechanism has two benefits: it creates an electronic trail to track viewers in case a problem does arise,[203] and it deters wandering eyes from viewing sensitive information with the intent to abuse it. Again, the PACER system provides an appropriate example of what a login procedure might entail. PACER requires a user to register with their personal information to obtain login and password information necessary to access the Internet postings.[204]

VI. CONCLUSION

As technology continues to develop, federal and state courts must decide how technology will affect public access rights. The introduction of the Internet into the public access doctrine amplifies the inherent tension between public access rights and individual privacy rights in the context of First Amendment and common law right

---

[200] *See* D. MASS. R. 4.5 app. A (2007) (installing an electronic-public access fee schedule, in accordance with Congress and the Judicial Conference, mandating federal courts to charge user fees to fund and provide electronic access to the PACER system); Alabama State Bar, *AOC Now Charges AlaCourt Subscribers Per-Page Fee*, 70 ALA. LAW. 139, 139 (2009) (indicating that Alabama state courts must now charge a fee for electronic access to court documents because the combination of electronic storage and budgetary constraints is cost prohibitive without generating such funds).

[201] *Public Access to Court Electronic Records Overview*, ADMIN. OFFICE OF THE U.S. COURTS, http://pacer.psc.uscourts.gov/pacerdesc.html (last visited Dec. 25, 2010). PACER is the federal version of an electronic-public access service permitting users to access court documents over the Internet. *Id.*

[202] *Frequently Asked Questions*, ADMIN. OFFICE OF THE U.S. COURTS, http://www.pacer.gov/psc/faq.html (click on the "How much does PACER cost? link) (last visited Feb. 19, 2011).

[203] JUDICIAL CONFERENCE COMMITTEE, *supra* note 64, at 6.

[204] *Public Access to Court Electronic Records*, ADMIN. OFFICE OF THE U.S. COURTS, http://www.pacer.gov/ (click on the "How Do I Access PACER" tab) (last visited Mar. 22, 2011).

of access claims. When courts post documents on the Internet, it exacerbates the opportunity for hyper-dissemination and misuse of the information as compared to the practical obscurity protecting documents available at the courthouse. In several opinions, the Supreme Court of the United States has insinuated that the analysis requires different privacy rights and varying levels of privacy as technology alters the legal landscape in the public access doctrine.

In July 2009, the Supreme Court of New Jersey adopted amended Rule 1:38 and approved the recommendations promulgated by its self-appointed Committee thereby fundamentally altering its public access doctrine. The amended Rule's explicit, absolute presumption of openness unless specifically exempted, fashions unanswered questions and specific consequences that the supreme court must address as it endeavors to create a policy for posting court documents on the Internet. Although the Rule does not address Internet posting explicitly in its provisions, the recommendations approved by the court urge the judiciary to begin posting certain documents online for remote electronic access by the public leaving it to the court to construct policy guidelines to govern Internet accessibility.

Because traditional access to court documents at the courthouse differs from remote electronic access over the Internet and because the policy is relatively undefined, several unanswered questions and consequences arise that the court must address when it implements its policies to balance public access rights and privacy rights. The questions and consequences focus on the enforcement of the redaction requirements, increased litigation burdening courts, the timing schedules for release of court documents over the Internet, and the costs of providing Internet accessibility. This Comment made recommendations and proposed solutions to these issues, including advocating for the creation of an enforcement provision for failure to redact, maintaining a policy of posting only court-generated documents online, creating an appropriate time schedule for release, charging user fees to offset costs, and requiring a login procedure with username and password information.

By considering these recommendations and resolutions, the court will ensure a healthy balance between public access rights and individual privacy rights even in the face of technological advancements. In response to Dr. Malcolm's warning, venture capitalist John Hammond retorted, "How could we stand the light of discovery and

not act?"[205] Unfortunately, the law is not as idealistic as a line in a movie.

[205] JURASSIC PARK (Universal Pictures 1993).