University of Baltimore Law Review

Volume 36
Issue 3 *Spring 2007*

Article 8

2007

Comments: Electronic Access to Court Records: Shifting the Privacy Burden Away from Witnesses and Victims

John Losinger
University of Baltimore School of Law

ELECTRONIC ACCESS TO COURT RECORDS: SHIFTING THE PRIVACY BURDEN AWAY FROM WITNESSES AND VICTIMS

I. INTRODUCTION

On June 14, 2005 the Maryland Court of Appeals ordered that information which has historically been available in hard copy at courthouses will also be made available electronically.[1] This decision came over the protests of prosecutors and victims' rights advocates who feared that the heightened availability would further enable victim and witness intimidation.[2] Prosecutors raised concerns about the differences between electronic and traditional access to court records.[3] According to Baltimore City State's Attorney Patricia C. Jessamy, "[t]here's a marked difference between going to a courthouse and having to interact face to face to get the information and doing it anonymously at a computer terminal."[4]

Roberta Roper, the founder of the Maryland Crime Victims' Resource Center, urged the court to maintain the existing block which disallowed "the electronic dissemination of personal information of crime victims and witnesses."[5] Ms. Roper argued that the public interest concern of protecting the dignity and safety of victims and witnesses outweighs the countervailing interest of making the information available electronically.[6] Particularly, Ms. Roper pointed out that lifting the block would lead to an increased ability to be threatened.[7]

> Current practice includes that clerks notify victims and witnesses by subpoena or summons through the judicial database. Subpoenas and summons are often included in the court files. However in order to examine these documents, those viewing the files will have to sign in and show identification to view the court file. If a victim or

1. Julie Bykowicz, *Make Court Data Available Electronically, Judges Order*, BALT. SUN, June 15, 2005, at 2B.
2. *Id.*; Letter from Roberta Roper, Founder, Md. Crime Victims' Res. Ctr., to The Md. Court of Appeals (June 14, 2005) (on file with author).
3. Bykowicz, *supra* note 1. While many commentators are concerned about electronic access as it applies to all types of cases in which a person's private information is widely disseminated, the focus of this Comment is limited to the issue of access to victim and witness telephone numbers and addresses as found in criminal court records.
4. Bykowicz, *supra* note 1.
5. Letter from Roberta Roper, *supra* note 2.
6. *Id.*
7. *Id.*

> witness is intimidated, an investigation can occur to review who had access to the court file to trace and identify the potential intimidator . . . . Under the new Rules terminal access will provide anonymous access to personal information of victims and witnesses. With anonymous access, there will be no opportunity to trace who may have threatened or harmed a victim or witness . . . . There will be a chilling effect for victims and witnesses if they learn that their personal information will be electronically disseminated.[8]

The National Network to End Domestic Violence raised the point that the ability to find a victim's name and address on a court website allows a batterer or stalker to find the victim.[9] "This encroachment on privacy and the resulting threat to personal safety will discourage victims of domestic violence from seeking protection from their abusers just as it will discourage witnesses from helping to end the violence through their testimony."[10]

Despite these concerns, the Court of Appeals unanimously refused to continue the status quo as to a block on electronic information of victims and witnesses and passed Title 16, Chapter 1000, of the Maryland Rules of Procedure.[11]

Under these rules, a witness or victim whose address and telephone number has appeared in the court record will carry the burden of proactively making certain that his or her personal information does not become widely disseminated over the Internet.[12]

To achieve this goal of privacy, victims and witnesses of domestic violence or those who have obtained a protective order may request to have certain information withheld from the public record.[13] Other victims and witnesses must file a motion to have information withheld. This motion must be sent to the State's Attorney and to the defense attorney.[14] Before a permanent removal of the personal information, the victim or witness will be required to attend a hearing at which he must make a case to the judge as to why his motion should be granted and his information

---

8. *Id.*
9. National Network to End Domestic Violence, Public & Internet Access to Court Records, Safety Net: The Nat'l Safe & Strategic Tech. Project 1, 2 (on file with author).
10. *Id.*
11. Bykowicz, *supra* note 1; Janet Stidman Eveleth, *New Rules Open Court Records to Public*, MD. B. BULL., Aug. 15, 2005, at 1.
12. *See infra* notes 211-222 and accompanying text.
13. *See infra* notes 219-222 and accompanying text.
14. *See infra* note 212 and accompanying text.

should be withheld.[15] The victim's offender has a right to be present at this hearing.[16]

Additionally, Maryland law does not provide a mechanism for victims to find out about this right to request that their personal information be withheld.[17] Neither the court, nor the police are required to inform the victims of their right.[18] Victims are forced to find a knowledgeable advocate who can help them file the aforementioned request and assist them with the hearing that will follow.[19]

This is a tremendous burden to place on victims and witnesses. This Comment will argue that the burden of proving why the telephone numbers and addresses of these people should not be left in the public record should be shifted to the defendant.[20]

Part II of this Comment will examine the development and current state of electronic access to court records.[21] It will explain how electronic access is problematic and how certain jurisdictions have moved to keep victim and witness telephone numbers and addresses protected from remote access.[22] Part III will discuss the regulation of public records as a whole.[23] It will examine the courts' attempts to balance public access to court records with the privacy interests of victims and witnesses.[24]

Part IV will propose a solution that will protect the information of victims and witnesses in Maryland, without impeding the courts' move towards electronic record keeping.[25]

II. ELECTRONIC ACCESS TO COURT RECORDS

This section will examine the electronic access to court records through a discussion of the shift away from traditional paper records,[26] a synopsis of Maryland's implementation of an electronic system,[27] a discussion of how this shift affects the privacy of individuals,[28] and an analogy between remote access to court records and the electronic dissemination of public

15. *See infra* notes 211-218 and accompanying text.
16. *See* MD. R. 16-1009 (indicating that a full adversarial hearing is required before granting motion to limit access to record).
17. *See* Eveleth, *supra* note 11, at 1.
18. *See generally supra* note 11, at 1.
19. *See generally supra* note 11, at 1.
20. *See infra* Part IV.
21. *See infra* Part II.
22. *See infra* Part II.
23. *See infra* Part III.
24. *See infra* Part III.
25. *See infra* Part IV.
26. *See infra* Part II(A).
27. *See infra* Part II(B).
28. *See infra* Part II(C).

information that occurred with the passage of Megan's Law legislation.[29] It will then examine how other jurisdictions have addressed the problem of personal information in the public record being disseminated electronically[30] and will explain the current Maryland Rules and summarize the recently adopted amendments to those rules.[31]

A. The Shift from Paper Records to Electronic Records

Historically, court records were kept using the traditional means of notebooks, cabinets, and cardboard boxes.[32] In order to access these records, an interested party "had to travel to the local courthouse of a particular jurisdiction and scan the columns in a court ledger or flip through a narrow drawer of carefully alphabetized index cards."[33]

In recent years, courts have followed technological trends and have begun to shift from paper-based systems to electronic information systems.[34]

As electronic systems developed, courts were slow to make the expensive and complex jump into the age of technology.[35] Even as the price of computers decreased and the understanding of computer systems increased, electronic systems were not overly advantageous because the data entered into a computer was "trapped in the machine" and could not be shared electronically.[36]

As modern networking technologies, such as the Ethernet, emerged in the 1980s, a court's desktop computer could be connected to a courthouse local area network (LAN), and by the early 1990s, courts, as much as they could afford, "were stringing their desktop computers together with network access cards and Ethernet wiring."[37] This new technology allowed court personnel to access various databases running within a courthouse.[38]

A problem that remained was that the systems "could not provide a single integrated view of all the information and data relevant to a particular case."[39]

---

29. *See infra* Part II(D).
30. *See infra* Part II(E).
31. *See infra* Part II(F).
32. 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, 176 (2004).
33. *Id.* at 176-77.
34. *Id.* at 177.
35. *Id.*
36. *Id.* at 177-78.
37. *Id.* at 178.
38. *Id.*
39. *Id.*

> For example, to access the schedule for a particular case, one might have to consult a stand-alone calendaring program; to check whether a party had filed a document in that same case, a stand-alone docketing program; and to confirm payment of a court fee, a stand-alone accounting program. Before one could achieve a single, integrated view of all the information and data relevant to a case, one would have to not only network all of the computers storing such information, but integrate the programs and information systems running on these machines as well.[40]

While this integration is a daunting task for the courts, the benefits of cost savings, error reduction, and improved performance reduce the courts' overall operating expenses.[41] An integrated, central database reduces the cost of maintaining and changing records.[42] It also reduces the opportunity for clerical errors that come with data entry, and court scheduling conflicts can easily be identified and prevented.[43]

B. Maryland's Implementation of the Judicial Information System and Its Technical Problems

In 2001, the Maryland General Assembly found a need

> (1) to create a central repository for criminal history record information; (2) to require the reporting of accurate, relevant, and current criminal history record information to the central repository by all criminal justice units; (3) to ensure that criminal history record information is kept accurate and current; and (4) to prohibit the improper dissemination of criminal history record information.[44]

The Assembly then set out to establish "an accurate and efficient criminal justice information system" that is consistent with both the need for "accurate and current" criminal history records, and the right to be free from improper and unwarranted intrusions of privacy.[45]

---

40. *Id.* at 178-79.
41. *Id.* at 179.
42. *Id.*
43. *Id.* at 180.
44. MD. CODE ANN., CRIM. PROC. § 10-202 (West 2001).
45. *Id.* § 10-203.

In order to achieve these legislative goals, the Maryland judiciary currently operates a Judicial Information System (JIS or "the System").[46] The JIS "staff develops and maintains State court system applications, operates a statewide computer network, and is responsible for data center disaster recovery capabilities."[47] In 2004, the System operated on a $19.6 million budget.[48]

The System is composed of a mainframe computer for court applications, two minicomputers for traffic citations and disbursement processing, and nine minicomputers which support the Uniform Court System.[49] The JIS serves public customers, Judicial Data Center personnel, and remote court users.[50] It connects users to various units of the judiciary, including the Circuit and District Courts, through a Wide Area Network, which connects remote court locations to the Uniform Court System.[51] "The [Uniform Court System] supports case initiation, scheduling, disposition, expungement and other record keeping."[52]

The System and external agencies can be accessed by seventy-seven local area networks, through the Internet.[53] These transmissions are controlled by a central Internet firewall.[54] Additionally, the JIS "also operates a server inside its network which supports public user dialup inquiries to court information from approximately 5,000 paying customers."[55]

A February 2005 audit of the Maryland JIS made several startling findings regarding the security and efficiency of the System. The first finding was that "the internal computer network was not sufficiently secured from untrusted networks and monitoring of network traffic was not adequate."[56]

The second was that the maintenance and administration of the firewall, which works to protect the System from unauthorized access, was outdated and inadequate.[57] The third was that the JIS communication server was not properly "configured to protect the internal network from unauthorized modification."[58]

---

46. Audit from Bruce A. Myers, Legislative Auditor, to Members of the Joint Audit Comm. (Feb. 10, 2005) [hereinafter JIS Audit] (on file with author), *available at* http://www.ola.state.md.us/reports/Fiscal%20Compliance/JIS05.pdf.
47. *Id.* at 7.
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.* at 9.
57. *Id.* at 10.
58. *Id.*

"Specifically, the Systems' communication server had weak or non-existent password and account lockout provisions for server users. In addition, authenticated users to the server were not limited to performing only designated tasks as specified by Systems' management."[59] This flaw allowed users to access information that they should not be privy to.[60]

Fourth, the measures used to protect two important network servers from having their applications improperly exposed on the Internet were inadequate.[61] "As a result of these network vulnerabilities, these servers were not adequately secured from exposures that could result in the loss of data integrity, the interruption of key services, and the improper use of these servers."[62]

Fifth, the System allowed individual users to operate under the identity of another to gain heightened access privileges.[63] Sixth, due to certain security inadequacies, changes to critical files "were not subject to review and approval by supervisory personnel."[64] This condition can easily lead to "unauthorized or erroneous changes to mainframe data files," such as court case records.[65]

These findings were observations on the current state of the JIS, as of February 2005, and were unrelated to the June 2005 hearing on electronic access to court records. However, the findings are instructive in considering that maintaining the security of electronic court files is a difficult task amidst the imperfect and still emerging technology of information systems.

C. *The Shift from Paper to Electronic Records and Its Effect on the Interest of Privacy*

In addition to the technical concerns about the security of the JIS, the development of Maryland's judicial information system created a system of electronic judicial records, in which it is imperative to offer heightened protection to individuals from invasions of their privacy.[66]

> It is temptingly easy to assume that if one applies the same set of rules to electronic judicial records that was applied in the past to paper records,

---

59. *Id.*
60. *Id.*
61. *Id.* at 11.
62. *Id.*
63. *Id.*
64. *Id.* at 12.
65. *Id.*
66. Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 314-15 (2004).

> it will result in the same balance between the various competing policies. Unfortunately, this is not the case. The assumption of parity represents a serious misunderstanding of the differences between paper records and electronic records. When the same rules that have been worked out for the world of paper records are applied to electronic records, the result does not preserve the balance worked out between competing policies in the world of paper records, but dramatically alters that balance. It shifts the balance away from individual privacy, producing little if any benefit on the side of judicial accountability.[67]

There is a basic distinction between paper records and electronic records that the Maryland General Assembly has been slow to address in its move toward open electronic dissemination.[68] The difference is that "practical obscurity" existed in the traditional systems, but not in the systems that allow electronic access.[69]

While court records have always been public, the way that they were kept allowed them to retain a high degree of "practical obscurity."[70] In the past, personal information found in a court record was public in that it could be accessed by anyone, not in the sense that it could easily be accessed by anyone with a fleeting interest.[71] "Only those with a relatively strong interest in the information would take time out of their day, wait in line at the clerk's office, fill out the necessary forms, and pay the necessary copy charges."[72] With the records available online, however, anyone can access the information with incredible ease.[73]

"The privacy protection that currently exists for public records is largely designed for a world of paper records and has been slow to adapt to an age where information can be downloaded from the Internet in an instant."[74]

---

67. *Id.* at 315.
68. *But see infra* Part II(F)(2).
69. Winn, *supra* note 66, at 316 (quoting United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762, 780 (1989)).
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.* Currently, criminal court records are available at http://casesearch.courts.state.md.us/inquiry/. While this website is in its infancy and search results are not as in-depth as they may be in the future, victim names are being disseminated over the Internet.
74. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1172 (2002).

The Maryland Rules in Title 16, Chapter 1000, create a heightened access to case records through electronic means, but do not temper this with a heightened security for victims and witnesses whose private information is included in the records.[75] While the case law on this matter is limited, the Supreme Court of Florida, in a 2002 decision, held that "digital storage and transfer of information changes how information can be manipulated and retrieved. Previously obscure information can be located quickly and anonymously for essentially no cost."[76] It is this inherent difference between paper files and electronic files that raised concerns for the Florida Supreme Court.[77]

> Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with the Internet revolution, public records can be easily obtained and searched from anywhere.[78]

D. Electronic Access to Public Records In Terms of Megan's Law

The inherent privacy issue that is attached to the Internet dissemination of public records was extrapolated in the passage and implementation of Megan's Law.[79]

The Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act "conditions certain federal law enforcement funding on the States' adoption of sex offender registration laws and sets minimum standards for state programs."[80] These registration laws are known as Megan's Laws; by 1996 every state and the District of Columbia had enacted some form of Megan's Law.[81]

In *Smith v. Doe*, the Supreme Court examined Alaska's variation of Megan's Law.[82] Alaska's version of the law requires that a sex offender register with local law enforcement authorities, providing "his name, aliases, identifying features, address, place of

---

75. *See infra* note 127.
76. *In re* Report & Recommendations of the Judicial Mgmt. Council of Fla. on Privacy & Elec. Access to Court Records, 832 So. 2d 712, 714 (Fla. 2002).
77. *Id.*
78. Solove, *supra* note 74, at 1139.
79. *See infra* discussion accompanying notes 89-96.
80. 42 U.S.C. § 14071(g)(2)(A) (2006); Smith v. Doe, 538 U.S. 84, 89-90 (2003).
81. *Smith*, 538 U.S. at 89-90. The laws are named for "Megan Kanka[,] a seven-year-old New Jersey girl who was sexually assaulted and murdered in 1994 by a neighbor who, unknown to the victim's family, had prior convictions for sex offenses against children." *Id.* at 89.
82. *Id.* at 90.

employment, date of birth, conviction information, driver's license number, information about vehicles to which he has access, and postconviction treatment history."[83] Those who fail to comply with these regulations are subject to criminal prosecution.[84]

The information provided is maintained in a central registry for sex offenders and is made available to the public.[85] "The Act does not specify the means by which the registry information must be made public. Alaska has chosen to make most of the non-confidential information available on the Internet."[86]

In *Smith v. Doe*, two men were separately convicted of sex offenses. After completing rehabilitative programs, they were required to submit personal information to the state for the purpose of the sex offender registry.[87] Among other things, the men argued that the widespread dissemination of their conviction was punitive and for the purpose of further humiliation.[88]

In an *amicus* brief, the Electronic Privacy Information Center[89] (EPIC) argued that

> The Alaska Megan's Law statute permits internet dissemination of stigmatizing information collected from released offenders by the state by mandating that the information in the registry be available "for any purpose . . . to any person." Because government posting of registry information makes this information widely available to individuals not living in geographic proximity to the registrant, the punishment imposed by the statute is excessive.[90]

While the *amicus* concedes that society has the ability to limit the privacy rights of criminals, it argues that the restrictions should not be more invasive than is necessary to achieve the state's purpose.[91] Widespread Internet dissemination goes beyond the purpose of locally identifying community sex offenders.[92]

---

83. *Id.* (construing ALASKA STAT. § 12.63.010(a)-(b) (2004)).
84. *Id.* (construing ALASKA STAT. §§ 11.56.835-.840 (2004)).
85. *Id.* at 90-91.
86. *Id.* at 91.
87. *Id.*
88. *Id.* at 97.
89. "[EPIC] is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values." Brief for Electronic Privacy Information Center as Amici Curiae Supporting Respondents at 1, Smith v. Doe, 538 U.S. 84 (2003) (No. 01-729), 2002 WL 1822146.
90. *Id.* at 1-2 (footnote omitted).
91. *Id.* at 2-3.
92. *See id.* at 7-10.

The Supreme Court addressed this contention and held that "[w]idespread public access is necessary for the efficacy of the scheme" and "[t]he fact that Alaska posts the information on the Internet does not alter [this] conclusion."[93]

The Court's reasoning, however, rested on the fact that there was a compelling state interest in making public the information of sex offenders.[94] Public safety was more heavily weighted in a balancing test with the encroachment on the privacy of the offenders.[95]

Conversely, in the case of the dissemination of the private information of victims and witnesses, it is difficult to envision a similar outcome in the balancing between the safety and privacy of victims and the government incentive of judicial ease.

Victims and witnesses are distinguishable from the criminally convicted in that the state does not have the right to limit their privacy and there is no overriding government interest in making their whereabouts known to the public.[96]

E. Other Jurisdictions

Some jurisdictions have recognized the problematic nature of the electronic dissemination of victim and witness information and have adjusted their rules accordingly.[97]

1. Minnesota

Rule Eight of the Minnesota Rules of Public Access to Records of the Judicial Branch deals with the issue of electronic access.[98] Subsection One of the Rule allows open access to public records in the courthouse.[99] Subsection Two addresses the "remote access to electronic records."[100] It specifies that "a custodian that maintains the following electronic case records must provide remote

---

93. *Smith*, 538 U.S. at 99.
94. *See id.*
95. *See id.*
96. *See* Stacy R. Horth-Neubert, *In the Hot Box and on the Tube: Witnesses Interests in Televised Trials*, 66 FORDHAM L. REV. 165, 166-67 & n.7 (1997); Kimberly A. Murphy, Comment, *The Use of Federal Writs of Habeas Corpus to Release the Obligation to Report Under State Sex Offender Statutes: Are Defendants "In Custody" for Purposes of Habeas Corpus Review?*, 2000 MICH. ST. L. REV. 513, *passim* (2000).
97. *See* discussion *infra* Part II(E)(1)-(3).
98. Minn. R. Pub. Access to Records of the Jud. Br., R. 8 (2005).
99. *Id.* at 8.1 ("Upon request to a custodian, a person shall be allowed to inspect or to obtain copies of original versions of records that are accessible to the public in the place where such records are normally kept, during regular working hours.").
100. *Id.* at 8.2.

electronic access to those records to the extent that the custodian has the resources and technical capacity to do so."[101]

The rule goes on to make the following exceptions:

> Notwithstanding Rule 8, subd. 2(a), the public shall not have remote access to the following data in an electronic case record with regard to parties or their family members, jurors, witnesses, or victims of a criminal or delinquent act: (1) social security numbers and employer identification numbers; (2) street addresses; (3) telephone numbers; (4) financial account numbers; and (5) in the cases of a juror, witness, or victim of a criminal or delinquent act, information that either specifically identifies the individual or from which the identity of the individual could be ascertained.[102]

The rule defines remote access as "information in a court record [that] can be electronically searched, inspected, or copied without the need to physically visit a court facility."[103]

The language of the rule makes clear that the state of Minnesota has recognized the distinction between the ability to access court records from afar on the Internet and from being forced to physically visit the courthouse to obtain information found in court records, and has tempered this difference with limited access to on-line records.[104]

2. Colorado

On April 8, 2005, the Colorado Judicial Department adopted a new policy regarding the public's access to court records.[105] The policy came after "[a] Public Access Committee was established . . . to develop policy regarding the information to be released to the public from court records including court records maintained in the Integrated Colorado Online Network . . . system."[106]

The Colorado policy, like the Minnesota Rules, defines remote access as "the ability to electronically search, inspect, or copy information in a court record without the need to physically visit the Judiciary Branch facility or location where the court record is maintained."[107]

---

101. *Id.* at 8.2(a).
102. *Id.* at 8.2(b).
103. *Id.* at 8.2(d).
104. *See supra* notes 98-103 and accompanying text.
105. Colo. Judicial Dep't, Public Access to Court Records (Apr. 8, 2005).
106. *Id.* § 3.00(a).
107. *Id.* § 3.30.

According to the policy, court records are assumed to be subject to remote access, except as otherwise specified.[108] The judiciary makes very clear in its list of specifications that certain types of information will not be open to the public by any means.[109] It also specifies what types of information will be available at the courthouse, but not through remote access.[110]

Most specifically, information regarding victims and witnesses is only available at the courthouse, not through remote access.[111]

3. Wisconsin

The Wisconsin court system employs a system called Wisconsin Circuit Court Access (WCCA) which, in conjunction with the Consolidated Court Automation Programs (CCAP), allows public Internet access to court records.[112] The disclosure policy governs the privacy of victims, witnesses and jurors by recommending "that court personnel entering information concerning crime victims into court documents use initials and dates of birth rather than full names whenever doing so would not defeat the purpose of the court document."[113]

The Wisconsin policy is different from Colorado's and Minnesota's in that it does not protect victims and witnesses by removing their personal information from court records.[114] However, the policy states that court personnel should avoid entering information that is not necessary to the purpose of the court record.[115] While this approach leaves open the possibility for

---

108. *Id.* § 4.20.

109. *Id.* § 4.60(a). These records that are not open to the public include:

> Probation [ ] files, Social Security Numbers (as collected by the court on court issued or standardized forms), Deposited Wills, Victim's name or identifying information in sexual assault case[s], Drug/Alcohol treatment information, Paternity tests, cases and records, Genetic testing, HIV/AIDS testing information, Medical, mental health sociological, intelligence testing, Scholastic achievement data on individuals, Adoption Records, Relinquishment Cases, Juvenile Delinquency Cases, Dependency & Neglect Records, Mental Health Cases, Expunged Records, Sealed files, data or information, Files/field/codes concerning the deliberative process, Draft opinions, notes or internal memos, Driver History, Judicial bypass cases, Juror questionnaires, CBI criminal background check reports.

Id.

110. *Id.* § 4.60(b). The personal information of the crime victims is not available in electronic format. *Id.*

111. *Id.*

112. Wisc. Policy on Disclosure of Public Information Over the Internet, http://wcca.wicourts.gov/AB0304.xsl (last visited Dec. 30, 2006).

113. *Id.*

114. *Id.*

115. *Id.*

error by court personnel, it still recognizes the vulnerability and importance of the privacy of victims and witnesses.[116]

F. Maryland Rules

Title 16, Chapter 1000, of the Maryland Rules is the applicable authority in terms of guarding the personal information of victims and witnesses from electronic dissemination.[117]

Rule 16-1001 defines a court record as "(1) an administrative record; (2) a business license record; (3) a case record; or (4) a notice record."[118] This Comment is focused on case records, which are "document[s], information, or other thing[s] that [are] collected, received, or maintained by a court in connection with one or more specific judicial actions or proceedings."[119] More narrowly, this Comment is concerned with the telephone numbers and addresses of victims and witnesses which are included in case records as a matter of course.[120]

As a general policy, these rules provide a presumption of openness.[121] However, Rule 16-1005 allows the following exceptions:

> [A] custodian shall deny inspection of a case record or any part of a case record if inspection would be contrary to:
>
> (1) The Constitution of the United States, a Federal statute, or a Federal regulation adopted under a Federal statute and having the force of law;
>
> (2) The Maryland Constitution;
>
> (3) A provision of the Maryland Public Information Act that is expressly adopted in the Rules in this Chapter;
>
> (4) A rule adopted by the Court of Appeals; or
>
> (5) An order entered by the court having custody of the case record or by any higher court having jurisdiction over
>
> (A) the case record, or
>
> (B) the person seeking inspection of the case record.[122]

116. *See generally supra* notes 114-115.
117. MD. R. 16-1001 to -1009.
118. MD. R. 16-1001.
119. *Id.*
120. Letter from Roberta Roper, *supra* note 2.
121. MD. R. 16-1002.
122. MD. R. 16-1005.

The Rules also specify certain categories of case records which carry an automatic prohibition of inspection.[123] These categories include adoption and guardianship actions, certain delinquency hearings, certain records pertaining to a marriage license, any case records concerning child abuse or neglect, confidential attorney grievance matters, and Pro Bono Legal Service Reports.[124] Additionally, in criminal actions, various types of information, including expunged records, certain records pertaining to search and arrest warrants, records of spousal privilege, records containing certain medical information, and records of income tax returns carry a required denial of inspection.[125]

Rule 16-1007 further denies the inspection of specific information in case records if the inspection would reveal:

> (a) The name, address, telephone number, e-mail address, or place of employment of a person who reports the abuse of a vulnerable adult . . . . (b) . . . the home address or telephone number of an employee of the State or a political subdivision of the State. (c) Any part of the social security or Federal Identification Number of an individual, other than the last four digits. (d) Information about a person who has received a copy of a sex offender's or sexual predator's registration statement.[126]

Rule 16-1008 states that "a court record that is kept in electronic form is open to inspection to the same extent that the record would be open to inspection in paper form."[127] The Rule further specifies that, for the purpose of providing electronic access to court records, including case records, the court is authorized

> (A) to convert paper court records into electronic court records; (B) to create new electronic records, databases, programs, or computer systems; (C) to provide computer terminals or other equipment for use by the public; (D) to create the ability to inspect or copy court records through remote access; or (E) to convert, supplement, modify, or replace an existing electronic storage or retrieval system.[128]

123. MD. R. 16-1006.
124. *Id.*
125. *Id.*
126. MD. R. 16-1007.
127. MD. R. 16-1008(a)(1).
128. MD. R. 16-1008(a)(2).

The Rule also defines remote access as the availability to the public through "dial-up modem, web site access, or other technology."[129]

1. Recently Adopted Amendments to the Maryland Rules

In its One Hundred Fifty-Sixth Report to the Court of Appeals, the Rules Committee proposed amendments to Rule 16-1008.[130] "The proposed amendments to Rule 16-1008 limit remote access to identifying information of victims and nonparty witnesses in criminal cases."[131] The Rules Committee also recommended that the amendments be adopted immediately so that the rule would become effective before the identifying information could be posted on the Internet.[132]

The amendments, which were approved by the Court of Appeals on March 7, 2006, and are to go into effect on July 1, 2006, add the following provision to Rule 16-1008:

> Except for identifying information relating to law enforcement officers, other public officials acting in their official capacity, and expert witnesses, a custodian shall prevent remote access to the address, telephone number, date of birth, e-mail address, and place of employment of a victim or nonparty witness in (1) a criminal action.[133]

This amendment limits the remote access of victim and witness information by making the rule subject to specific, limiting language.[134]

This amendment followed consideration of "the request of the Maryland Crime Victims' Resource Center, Inc. and the Maryland State's Attorneys Association."[135] The Reporter's Note summarized the reasoning:

> Victims' representatives and prosecutors fear that remote access to victim and witness information in criminal cases would facilitate and increase the ease with which a person from anywhere in the world, using an internet search engine, could harass, harm, intimidate, stalk, or threaten victims and witnesses. The criminal justice

129. MD. R. 16-1008(a)(4)(B).
130. 32 Md. Reg. 1819 (Nov. 14, 2005).
131. *Id.* at 1820.
132. *Id.*
133. 33-7 Md. Reg. 620, 621 (Mar. 31, 2006).
134. *Id.*
135. 32 Md. Reg. 1821 (Reporter's Note).

> system would be harmed by an increase in the already significant reluctance of victims and witnesses to report crimes and testify. Remote access would have a chilling effect on the reporting of rape and other crimes if a victim can forever be identified and stigmatized as a rape victim by a simple name search on the internet.[136]

The amendments take the same route as Minnesota rules and Colorado policy, by protecting victims and witnesses from having their addresses and telephone numbers disseminated electronically.[137]

2. Proposed Legislation

In addition to these amendments to the Court Rules, during the 2006 Legislative Session, Governor Robert L. Ehrlich, Jr. proposed legislation that would limit electronic access to victim and witness information.[138] Along with the Governor's Bill, Senator Norman R. Stone, Jr. and Delegate Joseph F. Vallario, sponsored similar bills to protect victim and witness information from electronic dissemination.[139] While each of these Bills failed,[140] they were proposed to prevent electronic access to public records that contain the personal information of victims and witnesses.[141]

Like the proposed amendments to the Maryland Rules, these Bills were limited to protecting victim and witness information from electronic access.[142] However, the problem goes beyond remote access.[143] The larger issue is that the heavy burden of limiting what information is included in the court record falls upon the victims.[144] Forthcoming proposed rule changes should not only protect victims and witnesses from improper remote access,

---

136. *Id.*
137. *See* discussion *supra* Part II(E)(1)-(2).
138. Daniel Ostrovsky, *Bill Would Block Access to Some Court Records*, THE DAILY REC., Jan. 31, 2006, at 1B.
139. H.D. 632, 2006 Leg., 421st Sess. (Md. 2006) (withdrawn), *available at* http://mlis.state.md.us/2006rs/billfile/hb0632.htm; H.D. 323, 2006 Leg., 421st Sess. (Md. 2006) (Senate took no action after Apr. 6, 2006), *available at* http://mlis.state.md.us/2006rs/billfile/hb0323.htm; S. 232, 2006 Leg., 421st Sess. (Md. 2006) (Senate took no action after Jan. 31, 2006; House took no action), *available at* http://mlis.state.md.us/2006rs/billfile/sb0232.htm; S. 162, 2006 Leg., 421st Sess. (Md. 2006) (Senate took no action after Jan. 31, 2006; House took no action), *available at* http://mlis.state.md.us/2006rs/billfile/sb0162.htm. The differences between these bills are immaterial to the scope of this Comment.
140. *See supra* note 139.
141. *Id.*
142. *Id.*
143. *See infra* Part III.
144. *See infra* Part IV.

but also from traditional courthouse access to their personal information.[145]

III. THE REGULATION OF PUBLIC RECORDS

This section will first examine the regulation of public records through a discussion of how public records were examined at common law,[146] and how the passage of the Freedom of Information Act affected the open examination of court records.[147] Next, it will examine the jurisprudence of striking a balance between public access and privacy.[148] It will follow with a discussion of legislation passed to protect personal information that had become public through state departments of motor vehicles.[149] It will conclude with a discussion of Maryland's laws concerning public access to court records, including the applicable discovery rules.[150]

A. Common Law

Following English common law, early U.S. courts normally only granted access to non-court records where there was a special interest.[151] "Today, however, this discretion has been significantly reduced by state and federal freedom of information laws."[152]

More specifically, the public's ability to inspect court records has traditionally been open and includes "a general right to inspect and copy public records and documents, including judicial records and documents."[153]

The Supreme Court has, however, provided discretion to the court to protect privacy in court files by holding that "[i]t is uncontested . . . that the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files and access has been denied where court files might have become a vehicle for improper purposes."[154]

---

145. *See infra* Part IV.
146. *Infra* Part III(A).
147. *Infra* Part III(B).
148. *Infra* Part III(C).
149. *Infra* Part III(D).
150. *Infra* Part III(E).
151. Solove, *supra* note 74, at 1155.
152. *Id.* at 1156.
153. Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978); Solove, *supra* note 74, at 1156.
154. *Nixon*, 435 U.S. at 598.

Despite this discretion, the presumption is in favor of open access to court records.[155] This places a burden on the party seeking confidentiality.[156]

B. The Freedom of Information Act

In 1966, the passage of the Freedom of Information Act (FOIA), and the similar state legislation that followed, created a "strong commitment to openness and transparency."[157] "The Freedom of Information Act of 1966 . . . provides that Government agencies shall make available to the public a broad spectrum of information."[158]

The FOIA was passed to tighten up ambiguities that existed under the previous applicable statute.[159] "The provisions of the Freedom of Information Act stand in sharp relief against those of [the former statute]."[160] The FOIA was "plainly intended to set up concrete, workable standards for determining whether particular material may be withheld or must be disclosed."[161]

The FOIA made all public records as open as court records had been under the common law.[162] The basic congressional purpose of the Act was to reflect "a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language."[163] Its effect on access to court records was to codify the presumption of openness.[164] This presumption continues today and is evident in the Maryland Rules.[165]

---

155. Solove, *supra* note 74, at 1158 (citing United States v. El-Sayegh, 131 F.3d 158, 159 (D.C. Cir. 1997) (stating that the public has a presumptive right of access to court records); Pansy v. Borough of Stroudsburg, 23 F.3d 772, 782 (3d Cir. 1994) (same); SEC v. Van Waeyenberghe, 990 F.2d 845, 848 (5th Cir. 1993) (same); Anderson v. Cryovac, Inc., 805 F.2d 1, 13 (1st Cir. 1986) (same).

156. Solove, *supra* note 74, at 1158 (citing FTC v. Standard Fin. Mgmt. Corp., 830 F.2d 404, 408-11 (1st Cir. 1987) ("[T]hose seeking to keep the datum hidden from view . . . must carry the devoir of persuasion.")).

157. Solove, *supra* note 74, at 1161.

158. EPA v. Mink, 410 U.S. 73, 74 (1973), *superseded by statute on other grounds as stated in* Zweibon v. Mitchell, 516 F.2d 594, 642 (D.C. Cir. 1975).

159. *Id.* at 79.

160. *Id.*

161. *Id.*

162. *See id.*

163. S. REP. NO. 89-813, at 3 (1965).

164. *Id.*

165. *See infra* notes 210-217.

C. *The Balance Between Privacy and Public Access*

1. The Supreme Court has Held that Privacy Outweighs Public Access

Despite the general presumption of openness, "[t]he Supreme Court has consistently found that the right to privacy outweighs the public's right to access."[166] In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[167] the Court held that the disclosure of an FBI rap-sheet to a third party, was an unwarranted invasion of privacy of the subject of the rap-sheet.[168]

The rationale hinged on the existence of specific statutory and regulatory provisions that limit the public access to rap-sheet information.[169] The Court explained that "[t]his careful and limited pattern of authorized rap-sheet disclosure evidenced a congressional intent to protect the privacy of the rap-sheet subjects."[170]

This case indicates that the Court will carefully balance privacy and openness on a case-by-case basis.[171] Furthermore, the Supreme Court has stressed the limitations of openness when sensitive personal information is at issue.[172]

In *Nixon v. Administrator of General Services*, the Supreme Court made the distinction that President Nixon had a privacy interest in records of his communications with his family, but not in records of his official duties.[173]

> In framing th[e] balance [between public access and the privacy rights of individuals], courts are sensitive to protect not only the personal privacy of litigants, but also the harm that can come to others, such as witnesses, victims, jurors, and other third parties, who may have no control over the information so disclosed.[174]

166. 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, 363 (2000).
167. 489 U.S. 749 (1989).
168. *Id.* at 780.
169. *Id.* at 764-65.
170. *Id.* at 765.
171. *Id.*
172. *See, e.g., infra* notes 173-174 and accompanying text.
173. 433 U.S. 425 (1977).
174. Winn, *supra* note 66, at 312.

2. *Westinghouse* Factors

In *Westinghouse Electric Corp. v. United States*,[175] an employer, the Westinghouse Electric Corporation, sought to protect its employees' medical records from being examined by the National Institute for Occupational Safety and Health.[176] The court attempted to balance the interest of maintaining occupational safety and health and the privacy of employees.[177] Five factors were laid out for consideration in the balance between personal privacy and the governmental interest in the disclosure of health records.[178]

> The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the types of records requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[179]

The court held that the National Institute for Occupational Safety and Health should be allowed access to the medical records, assuming that the employees were given reasonable notice and an opportunity to object.[180] Courts have subsequently applied the *Westinghouse* factors in deciding whether the disclosure of personal health information is appropriate.[181]

The examination of the balancing of privacy and the interest in inspecting medical records is instructive because it is comparable to the balance that is made between privacy and the inspection of court records.[182]

Professor Winn has summarized the balance between privacy and public access as follows:

---

175. 638 F.2d 570 (3d Cir. 1980).
176. *Id.* at 572.
177. *Id.*
178. *Id.* at 578.
179. *Id.*
180. *Id.* at 582.
181. Winn, *supra* note 66, at 313 (citing Doe v. Borough of Barrington, 729 F. Supp. 376, 378, 382 (D.N.J. 1990); Woods v. White, 689 F. Supp. 874, 876 (W.D. Wis. 1988), *aff'd without opinion*, 899 F.2d 17 (7th Cir. 1990)).
182. *Id.*

> The pragmatic reasons supporting the need for public access . . . are typically balanced against the pragmatic reasons supporting the need to restrict public access. While courts are vigilant in protecting the public right of access when it is consistent with ensuring the credibility of the judicial system, they are also quick to protect individuals from the exploitation of their personal information when it bears little relationship to ensuring the integrity of the judicial process. This common law and constitutional balance, carefully worked out on a case-by-case basis over the course of many years, represents the finest form of judicial lawmaking.[183]

3. Solove's Paradigm

Professor Solove argues that the overarching problem in this area of law is what he refers to as the "secrecy paradigm."[184] This traditional concept of privacy revolves around secrecy and the idea that once information is disclosed, the privacy is lost.[185] This model is embedded in our culture, as privacy is "often represented visually by a roving eye, an open keyhole, or a person peeking through Venetian blinds. Further, this paradigm explains why the Big Brother metaphor has become so widely used for depicting privacy problems."[186]

This paradigm has greatly influenced privacy law.[187] For example, in Fourth Amendment analyses the Supreme Court has held that there is no reasonable expectation of privacy in situations where something could have been seen or heard in public, or by a third person.[188]

---

183. *Id.* at 313-14.
184. Solove, *supra* note 74, at 1176.
185. *Id.*
186. *Id.* at 1177.
187. *Id.*
188. *Id.* (citing Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that "the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment" due to the fact that the images are generally available to public view)); *but see* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that thermal imaging technology that allows insight into the home, into information that is not generally in public view is a violation of the Fourth Amendment); *see also* California v. Greenwood, 486 U.S. 35, 40-41 (1988) (no reasonable expectation of privacy exists in curbside garbage because it was made public to the trash collectors); Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (no reasonable expectation of privacy exists in a pen register because the information is made public to phone company); United States v. Miller, 425 U.S. 435, 442-43 (1976) (no reasonable expectation of privacy exists in bank records because they are made public to the

The law treats privacy in a black-and-white manner, categorizing information as either wholly public or wholly private.[189] If information remains a secret, it will remain private, but once information becomes public, it will enter the public domain, will be available for any use, and can no longer be claimed to be private.[190]

While Professor Solove urges a retreat from the traditional "secrecy paradigm," the courts have been slow to make such a move.[191] As the professor points out, in *Scheetz v. Morning Call, Inc.*, the court upheld the disclosure of a police report, alleging spousal abuse, to the press, despite the fact that no charges had been filed and that the married couple sought to keep the information private.[192] The court reasoned that "[t]he police could have brought charges without her concurrence, at which point all the information would have wound up on the public record, where it would have been non-confidential."[193]

The case law indicates that once personal information becomes public, or even could become public, it will rarely be constitutionally protected by the right to privacy.[194] Therefore, victim and witness information, once it becomes available in the public court record, according to the secrecy paradigm, will never be considered private again.

D. Protection of Personal Information in Terms of the Driver's Privacy Act

A major problem with the lack of privacy and the increased ease of access is that the personal information of victims and witnesses being disseminated, can and will be used for the purpose of intimidation or harassment.[195] The increased access that comes with electronic access can directly "facilitate blackmail, extortion,

---

bank), *limited by statute on other grounds as stated in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980).

189. Solove, *supra* note 74, at 1177.

190. *Id.*

191. *Id.* at 1182, 1184.

192. *Id.* at 1182 (citing Scheetz v. Morning Call Inc., 946 F.2d 202 (3d Cir. 1991)).

193. *Id.* (quoting *Scheetz*, 946 F.2d at 207).

194. *Id.* (citing Cline v. Rogers, 87 F.3d 176, 179 (6th Cir. 1996) (holding that "one's criminal history is arguably not a 'private personal' matter at all, since arrest and conviction information are matters of public record"); Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994) ("An individual cannot expect to have a constitutionally protected privacy interest in matters of public record.")).

195. *See supra* text accompanying notes 5-10. Professor Winn discusses the commercialization of the personal information found in court records as a major concern that comes with electronic dissemination. Winn, *supra* note 66, at 316. While this concern is the crux of many arguments against a shift from paper records, it is beyond the scope of this Comment.

stalking, sexual assault, subornation of perjury, identity theft, and fraud."[196]

Personal information is the most sensitive and the most likely to be subject to misuse.[197] In terms of public court records, the personal information that is of great concern to victims' rights advocates are the addresses and telephone numbers of the victims and witnesses who are named in the public record.[198]

In 1994, Congress addressed the issue of harm being facilitated by information gathered from public records.[199] Congress considered a highly publicized case in which the actress Rebecca Shaeffer was shot and killed by a person who obtained her address through the California Department of Motor Vehicles.[200] In the House, there was a discussion of gangs who took license plate numbers of expensive cars, found out the addresses of the car owners through the DMV and robbed the houses.[201] In the Senate, there was an account of a California man who sent threatening letters to young women after using their license plate numbers to obtain their addresses from the DMV.[202]

These cases involved information culled from public records at state departments of motor vehicles and led to the passage of the Driver's Privacy Protection Act of 1994.[203] However, the exact same information, an individual's name and address, could have just as easily been obtained from court records.[204] "Personal information that facilitates these kinds of wrongs should not be accessible to the public either at the courthouse or over the Internet. It places an individual in jeopardy of physical, psychological, and economic harm without furthering any of the benefits of public access to court records."[205]

The purpose of public access to the court system is multi-faceted. There is a government interest in promoting public trust and confidence in the court system and showing that the nation's laws are being upheld and enforced.[206] There is also an interest in educating citizens and keeping the public informed as to how the

196. Silverman, *supra* note 32, at 206.
197. *Id.* at 207.
198. *See* Silverman, *supra* note 32, at 207; Letter from Roberta Roper, *supra* note 2.
199. Silverman, *supra* note 32, at 207-08.
200. 139 CONG. REC. 27, 327 (1993) (statement of Rep. Moran); Silverman, *supra* note 32, at 207-08.
201. 139 CONG. REC. 27, 327 (1993) (statement of Rep. Moran); Silverman, *supra* note 32, at 207.
202. 139 CONG. REC. 29, 466 (1993) (statement of Sen. Boxer); Silverman, *supra* note 32, at 207.
203. Silverman, *supra* note 32, at 208.
204. *Id.*
205. *Id.* at 208-09.
206. *Id.* at 209.

courts operate and what conclusions the courts have reached on the issues before them.[207]

> Withholding sensitive personal information from the public when they access court records will neither undermine nor subvert any of these benefits. The adjudicatory facts upon which a court relies to dispose of a case or controversy according to the rule of law need never include the specific, arbitrarily assigned street address of a person's home, the precise series of numerals composing his or her telephone number, or the exact digits of his or her Social Security number. That a person has a Social Security number may be relevant to the just and rational disposition of a case, but the specific number will not be. Similarly, the general education that an individual might be expected to acquire from the perusal of court records does not include committing to memory the street addresses of fellow citizens, their Social Security numbers, or their bank accounts. Accordingly, such information should be omitted from publicly accessible court records and documents, irrespective of their form or the public's method of accessing them.[208]

E. Current Applicable Maryland Provisions

1. Rule 16-1009—Preliminary Shielding Upon Motion

Rule 16-1009 applies to court records irrespective of whether they are being accessed electronically or at the courthouse.[209]

Rule 16-1009 allows the court to deny the inspection of case records on a case-by-case basis.[210] For the court to review a request for a denial of inspection of a case record, a motion must be filed by "[a] party to an action in which a case record is filed, including a person who has been permitted to intervene as a party, and a person who is the subject of or is specifically identified in a case record."[211] Under this rule, a victim or witness who is named in a case record must file a motion which must be served on all parties to the action, if she wishes to have her address and telephone number kept out of the public court record.[212] After the

---

207. *Id.*
208. *Id.* at 209-10.
209. *See* MD. R. 16-1008(a), 16-1009.
210. MD. R. 16-1009.
211. MD. R. 16-1009(a)(1).
212. MD. R. 16-1009(a)(2).

victim files the motion, the record will be preliminarily shielded for five business days while the court determines whether or not to issue a temporary order precluding or limiting inspection.[213] This temporary order will be issued when an affidavit or statement under oath indicates that:

> (A) there is a substantial basis for believing that the case record is properly subject to an order precluding or limiting inspection, and (B) immediate, substantial, and irreparable harm will result to the person seeking the relief if temporary relief is not granted before a full adversary hearing can be held on the propriety of a final order precluding or limiting inspection.[214]

Following the issuance of the temporary order and a full adversary hearing, the court may issue a final order.[215] In making the determination of whether to issue a final order, the court shall consider any "special or compelling reason[s]" to limit inspection.[216] Under the Rules, a heavy burden rests on a person identified in the case record who wishes to have his personal information removed from the public record.[217] Additionally, this person carries the burden of acquiring information about the rights afforded to victims and witnesses and the possibility of having personal information shielded from the public record.[218]

2. Amendment to Rule 16-1009—Shielding Upon Request

In July 2006, the Maryland Court of Appeals amended Rule 16-1009, allowing victims of domestic violence and victims who have acquired peace orders to have their information shielded upon "request," without filing a motion.[219] If the victim's request is granted, the shield on the personal information will remain "in effect until terminated or modified by order of court. If the request is denied, the person seeking to shield information may file a motion . . . ."[220] A criminal witness or victim who is not a victim of domestic violence or who has not obtained a peace order must continue to file a motion, and will be unaffected by the July 2006 Amendment.[221]

---

213. MD. R. 16-1009(b).
214. MD. R. 16-1009(c)(2).
215. MD. R. 16-1009(d).
216. MD. R. 16-1009(d)(4).
217. MD. R. 16-1009(d).
218. *See generally* Eveleth, *supra* note 11, at 1.
219. 33 Md. Reg. 1433 (Aug. 18, 2006).
220. *Id.*
221. *Id.*

The Amendment to Rule 16-1009 makes it easier for certain victims to ask the court to shield their personal information from the public record, without going through the tedious process of filing a motion.[222] It also continues to place the burden on victims to take certain statutory steps in order to have their personal information withheld from the public record.

3. Discovery Rules and the *Coleman* Case

Coleman v. State[223] is a case involving drug-related crimes.[224] "The case demonstrates the dominant extent to which the rampant illicit dealings in drugs have intruded, both flagrantly and insidiously, into the life of the community and the lives of the people."[225]

The defendants in the case appealed the trial court's decision to withhold, from the defendants, the names of the prosecution's key witnesses.[226] The names of the witnesses were withheld because this was a classic case of witness intimidation.[227] The applicable rule of discovery in this case is Rule 4-263(b)(1) which states that "upon the request of the defendant, the State's Attorney shall . . . [d]isclose to the defendant the name and address of each person then known whom the State intends to call as a witness."[228]

The broad exception to this rule is that the State is not required to disclose any "matter if the court finds that its disclosure would entail a substantial risk of harm to any person outweighing the interest in disclosure."[229] In *Coleman*, the Court of Appeals used this exception to uphold the trial court's decision to withhold the witness information from the defendants.[230]

"The privilege of the State to withhold certain matters from defendants in criminal causes has long been recognized, not only in Maryland but throughout the country. The privilege is especially important in the enforcement of narcotic laws, since it is most difficult to obtain evidence for prosecutions."[231] In this particular case, the Court of Appeals held that the trial judge did not abuse her discretion when she did not allow the defendants discovery of the witness information.[232] The reasoning was that

222. *Id.*
223. 321 Md. 586, 583 A.2d 1044 (1991).
224. *Id.* at 589, 583 A.2d at 1045.
225. *Id.* at 589, 583 A.2d at 1045.
226. *Id.* at 591, 583 A.2d at 1046.
227. *Id.* at 595-96, 583 A.2d at 1048.
228. MD. R. 4-263(b)(1).
229. MD. R. 4-263(c)(3).
230. *Coleman*, 321 Md. at 604, 583 A.2d at 1052.
231. *Id.* at 602, 583 A.2d at 1051 (citations omitted).
232. *Id.* at 603, 583 A.2d at 1052.

the safety of the witnesses outweighed the rights of the defendants to have access to the names and addresses of the witnesses.[233]

This case indicates that once the names and addresses of witnesses become an issue, the burden will be on the defendants to show that their interest in obtaining the information outweighs the interest in keeping the information closed from discovery.[234] However, in order to become an issue, the first and most important burden is on the victim or the witness to request that the information be protected from discovery and withheld from the court record.[235]

The discovery rules and the *Coleman* case must be considered together with Section 11-205 of the Maryland Code of Criminal Procedure.

4. Sections 11-205 and 11-301 of the Maryland Code of Criminal Procedure

The victim's burden is further cemented in sections 11-205 and 11-301 of the Maryland Code of Criminal Procedure.[236] Section 11-205 deals with requests made prior to trial.[237] The section states that:

> On request of the State, a victim of or witness to a felony or delinquent act that would be a felony if committed by an adult, or a victim's representative, a judge, State's Attorney, District Court commissioner, intake officer, or law enforcement officer may withhold the address or telephone number of the victim, victim's representative, or witness before the trial or adjudicatory hearing in a juvenile delinquency proceeding, unless a judge determines that good cause has been shown for the release of the information.[238]

Similarly, section 11-301 deals with motions made during a trial.[239]

---

233. *Id.*
234. *See supra* notes 228-229.
235. *See supra* note 231. In *Coleman*, the State made the request to withhold the witness information because of the obvious witness intimidation aspect of the case. *Id.* It is in situations where witness or victim privacy is not evident to the prosecutor that the burden falls solely on the shoulders of the witnesses and victims to see to it that their personal information is withheld from the public record.
236. MD. CODE ANN., CRIM. PROC. §§ 11-205, 11-301 (West 2005).
237. *Id.* § 11-205.
238. *Id.*
239. *Id.* § 11-301.

> On motion of the State or on request of a victim or witness, during a criminal trial or a juvenile delinquency adjudicatory hearing, a court may prohibit the release of the address or telephone number of the victim or witness unless the court determines that good cause is shown for the release of the information.[240]

While these sections give the court the discretion to withhold victim and witness information, the discretion is not triggered until a request is made.[241] As a practical matter, this places the burden on the victims or witnesses to proactively prevent their personal information from becoming a part of the public court record. Although the statutes and discovery rules indicate that once victim and witness information is of issue before the court, the burden will shift to the defendant to show why the information should be in the record, the first burden is on the victim or witness to seek advice as to his rights and then to make the appropriate request.[242]

IV. SOLUTION—SHIFTING THE BURDEN

The Maryland Code, in conjunction with Maryland Rule 16-1009, shows that the addresses and telephone numbers of victims and witnesses are presumed to be open to the public.[243] The Maryland Rules also indicate that with the advent of new technologies this information will be available electronically from remote locations.[244]

While the Rules Committee has adopted amendments that would limit the electronic availability of victim and witness information, and that allow victims and witnesses to request to have their information shielded, it has done nothing to remedy the root of the problem. The basic burden is still placed on the victims or witnesses to have their personal information blocked from the public record.[245]

Electronic access to victim and witness telephone numbers and addresses is simply a publicized mutation of a larger problem of general public access to this information. In order to solve the problem, the legislature should go beyond the approach taken by the amendments to the Rules and the proposed legislation. While these solutions narrowly protect victims and witnesses from remote access problems, they should give the victims and witnesses broad

240. *Id.*
241. *Id.* §§ 11-205, 11-301.
242. *Id.*; *supra* Part III(E); *see generally* Eveleth, *supra* note 11, at 1.
243. *Supra* note 121.
244. *Supra* note 127.
245. *See supra* Part III(E).

protection by placing the burden on the defendant to show why the personal information is vital to the court record.

This goal can be accomplished by changing the language of sections 11-205 and 11-301. Both sections currently state that the addresses and telephone numbers of victims and witnesses "may" be withheld from the court record upon request.[246] This wording places the burden on the innocent victim or witness to see to it that information be withheld.[247] As most victims and witness are not represented by counsel, it is unrealistic to assume that innocent people who find themselves in the middle of the criminal justice system, as non-parties, will have the knowledge to request that their personal information be withheld from the record. As the system stands, the addresses and telephone numbers of unrepresented victims and witnesses are being disseminated in the court record due to the fact that the citizenry is not aware of the need to make the appropriate requests.

The burden must be shifted away from the unrepresented non-parties to defendants who often have a Constitutional right to be represented by counsel. Sections 11-205 and 11-301 should be replaced with a statute that reads:

> On motion of the defendant, prior to or during a criminal trial or a juvenile delinquency adjudicatory hearing, a court may permit the release of the address or telephone number of the victim or witness if the court determines that good cause is shown for the release of the information.

This proposal creates a presumption that victim or witness addresses and telephone numbers will not be a part of the court record. It does not disturb a defendant's right to confrontation, as the victims' and witnesses' names will remain part of the court record. The only aspects of the record that would be withheld are the actual numbers that constitute the victims' or witnesses' telephone numbers and street addresses. The benefit of this withholding will be increased privacy for the innocent third parties who are neither defendants nor prosecutors in the criminal justice system.

This change would not conflict with the general presumption of openness, as the integral parts of the court record would remain accessible to the public, both at the courthouse and electronically. It would, however, shift the burden from the victim or witness, to the defendant, to prove that the telephone number and address of the victim or witness is crucial to the record.

---

246. *Supra* note 236.
247. *See supra* Part III(E)(3).

The change to the criminal procedure code would allow the move toward electronic and remote access to occur without endangering the rights and welfare of victims and witnesses. The change would also allow victims and witnesses to move on after their innocent involvement in the criminal justice system, without their privacy being forever lost with their personal information being unnecessarily included as a part of the public record.

John Losinger