Wisconsin's Open Records Law

Balancing Access and Privacy in the Information Age

by

Daniel Kaneshiro

Susanne Petro

Lori Wilson

Ben Winig

Policy Analysis Workshop, Public Affairs 869
Spring 2003

La Follette School of Public Affairs
University of Wisconsin – Madison

Second Printing

For additional copies:
Publications Office
La Follette School of Public Affairs
1225 Observatory Drive
Madison, WI 53706

www.lafollette.wisc.edu

Table of Contents

Foreword

This report on the state's open records law is the result of a collaboration between the Robert M. La Follette School of Public Affairs at the University of Wisconsin–Madison and the Joint Legislative Council. The objective of this collaborative effort is to provide graduate students at La Follette the opportunity to improve their policy analysis skills while contributing to the capacity of the Joint Legislative Council to provide the legislature with high-quality analysis on issues of concern to the citizens of Wisconsin.

The La Follette School offers a two-year graduate program leading to a master's degree in public affairs. Students specialize in policy analysis or public management, but in many cases they follow a curriculum in both areas. They spend the first year and a half of the program taking courses that provide them with the tools needed to analyze public policies. The authors of this report are all currently enrolled in Public Affairs 869, *Workshop in Program and Policy Analysis.* Although acquiring a set of policy analytic skills is important, there is no substitute for *doing* policy analysis as a means of *learning* policy analysis. Public Affairs 869 provides them with that opportunity.

The students enrolled in the class were assigned to one of four project teams. One team worked on this project for the Legislative Council, while the other three teams completed projects for the Budget and Management Division of the city government in Milwaukee. The topic of this report—the open records law—was chosen by Terry C. Anderson, director of the Joint Legislative Council staff from a list of topics proposed by his staff.

Wisconsin has had a long tradition of open, transparent, and accountable government. The rights of individuals to information about their government is codified in the state's open record laws. The rapid growth in electronic records coupled with the recent development of powerful search engines has raised concern about the potential misuse of personal information that is included in government records. The purpose of this report is to explore the potential conflicts between the principle of open records and the need to safeguard individual privacy. The authors analyze the potential problems created by easy electronic access to public records and propose a number of changes to the state's open record law.

This report obviously does not provide the final word on the complex issues the authors address. The graduate student authors are, after all, relatively inexperienced policy analysts. Nevertheless, much has been accomplished. I trust that both the students and the Joint Legislative Council staff have learned a great deal about the potential problems created by Internet access to open records. The report helps define the issues and provide a foundation for further analysis and decision making.

This report would not have been possible without the support and encouragement of Terry Anderson. Robert J. Conlin, senior staff attorney on the Joint Legislative Council staff worked closely with the authors. He was generous with his time and advice. A number of other people also contributed to the success of the report. Their names are listed in the acknowledgements printed at the end of the report.

The report also benefited greatly from the active support the La Follette staff. Alice Honeywell, publications director at La Follette, edited the report and produced the final bound report. Alice, along with Terry Shelton, La Follette's outreach director, and Craig Allen, information systems manager, provided the students with constructive criticism and advice on

their oral presentations of the reports. Kari Reynolds contributed logistic support for the policy analysis projects.

It is my hope that by involving La Follette students in the tough issues faced by state government, they have not only learned a great deal about doing policy analysis, but have gained an appreciation of the complexities and challenges facing both state and local governments in Wisconsin. I also hope that this report will contribute to the work of the Joint Legislative Council and to the ongoing public discussions of the challenges to the principle of open government records created by the increasingly easy access to electronic records.

Andrew Reschovsky
May 2, 2003

Acknowledgments

We would like to thank Bob Conlin from the Legislative Council for sponsoring this project, offering his sage advice throughout the semester, and helping us refine our recommendations. We also want to thank Carole Doeppers for sharing her depth of understanding of the Open Records Law and how it specifically relates to privacy issues; State Senator Jon Erpenbach; Curt Witynski from the League of Wisconsin Municipalities, Wisconsin Assistant Attorney General Allan Lee; Dane County Register of Deeds Jane Licht; and John Dowling from the UW-Madison Administrative Legal Services. In addition, we extend a special thanks to Alice Honeywell of the UW–Madison La Follette School of Public Affairs for her editing assistance. Finally, we sincerely appreciate the guidance and advice of our professor, Dr. Andrew Reschovsky, also of the La Follette School of Public Affairs.

Executive Summary

The Legislative Council has asked us to examine problems that may result from Internet access to open records. In doing so, we explore the reasons Wisconsin's open records law is inadequate to address many of the current and emerging concerns arising from the expansion of access to electronic records. Our analysis is intended to assist legislators in fine-tuning the open records law—maintaining the law's original presumption toward openness while preserving the privacy interests of Wisconsinites to the extent possible.

We first discuss the reasons for our analysis: (1) problems with the law within government agencies, such as issues arising from access to online data, inadequate agency training, inconsistent implementation of the law, and government secondary uses of public records; and (2) private misuse of public information, such as identity theft, safety issues, and personal secondary uses. We develop our recommendations based on the principles of public access to records versus protection of privacy, security, and accountability to the public, clarity and flexibility of the law, and maintaining the spirit of the law.

First, we recommend that the legislature create an Open Records Council to identify and address emerging open records issues and to recommend statutory amendments or regulatory changes. This council's agenda would consist largely of the following activities: (1) training agencies to manage their open records, (2) advising and guiding agencies on how to implement the current open records law, (3) publicizing information regarding the open records law, (4) answering questions from agencies and the public regarding open records, (5) mediating disputes arising from open records requests. Its authority would be statutorily defined by the legislature.

Second, we recommend that the council mandate that state agencies perform biennial inventories of their internal public records. The council should then use this information to develop a system that classifies information according to level of security.

Third, we recommend that the legislature amend Wisconsin's open records law to require the identification of record requesters. Since the transformation to online records has far outpaced the legislature's ability to protect the privacy of citizens, we believe it is time to increase the costs of gathering online information by implementing a mail-in or in-person registration system to identify record requesters.

Fourth, we recommend that the legislature require state agencies to notify citizens before collecting or releasing their personally identifiable information on the Internet. Notices would appear on all agency forms and Web sites, informing records requesters that personally identifiable information may be subject to the open records law.

Wisconsin's Open Records Law: Balancing Access and Privacy in the Information Age

by Daniel Kaneshiro, Susanne Petro, Lori Wilson, and Ben Winig

"The open records law serves one of the basic tenets of our democratic system by providing an opportunity for public oversight of the workings of government… [Wisconsin Statutes Sections] 19.32 to 19.37 shall be construed in every instance with a presumption of complete public access, consistent with the conduct of governmental business. The denial of public access generally is contrary to the public interest, and only in an exceptional case may access be denied." Nichols v. Bennett, 199 Wis. 2d 268, 273, 544 N.W. 2d 428, 430 (1996)

The Wisconsin electorate has long demanded that government be transparent, open, and that public officials be held accountable. Although the Wisconsin Supreme Court responded to this challenge as early as 1856 when it recognized a common law right to inspect government records, it was not until the early twentieth century that the legislature attempted to satisfy this demand fully (Roang, 1994). In 1917, the legislature enacted the state's first public records law, marking a significant deviation from the restrictive practices found across the nation.[1]

Among other things, the 1917 statute afforded "any person access to public records … and established a $25 to $2,000 forfeiture for the violation of the statute" (State Bar of Wisconsin, 1983). Furthermore, the law provided that every officer of a government agency (including school districts) was the legal custodian of the agency's records and each was responsible for their care and control (p. 1). In addition, the law separated public records into the following three categories: "materials required to be kept in the officer's office, materials in the lawful possession or control of the officer and his deputies, and materials the officer is lawfully entitled to possess or control" (p. 1). For much of the twentieth century the law remained unchanged, but in 1983 it was significantly amended to constitute what is Wisconsin's current open records law.

As interpreted by the Wisconsin courts, today's open records law presumes that all government records shall be open for inspection and copying, unless (1) there is a specific statutory or common law exception, or (2) the harm done to the public interest by disclosure of a record outweighs the public's interest in access to that record (Wis. Stat. §§ 19.32 – 19.37, 1999–2000). This latter exception is referred to as the "balancing test," and it requires a record custodian to determine on a case-by-case basis whether the state's interest in non-disclosure of a particular record outweighs the public's right to access that record. The test's subjectivity has prompted much discussion and litigation. Although we assume that the law's presumption of openness should prevail, we query whether the balancing test is able to withstand new challenges brought about by ever-changing technology and widespread access to online data.

[1] The North Carolina Supreme Court, for example, ruled in 1887 that "no citizen had a right to copy the records of any public office simply because he or she so desired to do so" (*Newton v. Fisher*, 1887).

Wisconsin is not the only state grappling with the potential problem of increased electronic access to public records. In a recent New Jersey case, the state's Supreme Court aptly described the emerging dilemma. "Unlike paper records," the Court noted, "computerized records can be rapidly retrieved, searched and reassembled in novel and unique ways, not previously imagined. Thus the form in which information is disseminated can be a factor in the use of and access to records. These new considerations must be factored into the common-law balancing test between the State's interest in non-disclosure and the public's right to access" (*Higg-A-Rella, Inc. v. County of Essex*, 141 N.J. 35, 48–49, 1995). In Pennsylvania one court reasoned that "it is not a matter of whether a record is still open, but whether an electronic version is the most reasonable means of making the information public" (*Hoffman Pennsylvania v. Game Commission,* 455 A.2d 7321 734, Pennsylvania Commonwealth, 1983). In other words, the Pennsylvania court argued that just because a document is a public record does not mean it must be accessible via the Internet.

Evidently, the movement toward making data available online has reshaped the debate between public access and privacy throughout much of the nation. The Wisconsin Legislative Council has asked us to evaluate the ways in which technology and online data in Wisconsin are changing the balance between public access and private harm. Our analysis seeks to aid in the process of improving the open records law to ensure that it maintains its original presumption toward openness while simultaneously preserves the level of privacy important to Wisconsin's citizens.

Analyzing Wisconsin's Open Records Law

Government faces many challenges in maintaining accurate records to fulfill the wide array of functions and services provided for the people of Wisconsin. Complying with the open record law's presumption toward openness in light of recent developments in information technology has proven to be a particularly difficult challenge. While the Internet represents an opportunity for the state to grant citizens faster, more efficient access to public records, the current law does not provide the necessary safeguards against possible misuse, such as identity theft. Before the prevalence of technology and online data, the potential for misuse of personally identifiable information was lower because Wisconsin had the built-in safeguard of *practical obscurity*. Being forced to travel to the record custodian, appear personally, and make an oral or written request was a natural deterrent for everyone, particularly those with ill intentions who may have feared being identified. With the advent of Internet-accessible public records, however, this practical obscurity has virtually vanished.

Today more than ever, government records possess a wealth of personal information, almost all of which is open to public scrutiny. From property tax records and divorce files, to intra-agency e-mails and court proceedings, one's personal information can fall into the hands of an identity thief or stalker in a matter of seconds. Exacerbating this challenge is the amount of data currently being collected by various local and county agencies that are decentralized, both physically and administratively. Thus two sets of difficulties arise regarding Wisconsin's open records law: (1) problems related to handling information within government agencies and (2) misuse of information outside the public sector.

Problems within Government Agencies

Government agencies handle extensive public records, most of which contain some type of personally identifiable information. As electronic access to data increases, so do the problems in safeguarding that data from potential misuse.

Access to Online Data

Recent advances in technology have transformed the ways in which information collected by government agencies can be compiled, stored, and transmitted. Furthermore, with the exponential growth of the World Wide Web, information technology has revolutionized how governments and citizens interact with one another. To comply with Wisconsin's open records law, with its strong presumption toward openness, many state agencies have begun to convert public records into databases and other electronic formats that are available online. Our concern, therefore, is that many agencies are posting public records online, some of which may contain personally identifiable information, without taking appropriate precautionary measures.

The rapid transformation and increased capabilities of technology have far outpaced the state's ability to regulate and protect the privacy of its citizens. As state Rep. Mark Gundrum (R-New Berlin) noted, "criminals know that the laws are not being kept up to date" (Chaptman, 2003). Despite the growing use of the Web by state agencies, Wisconsin currently does not have an official review process to decide which public records should or should not be made available on the Internet. Thus far, Wisconsin has been fortunate with its relatively low number of identity theft and stalking cases that have occurred because of electronic access to public records. The acceleration in information technology, however, coupled with the increased sophistication among those with malicious intent create great potential for more severe problems.

Lack of Training

Primarily because turnover is high, particularly at the city and county levels, records custodians lack training and knowledge of procedural guidelines as to exactly what type of information constitutes a public record and what types of personally identifiable information should be kept private (Witynski, 2003). Records custodians must often go outside their agencies for answers. Curt Witynski, assistant director of the League of Wisconsin Municipalities, noted that his organization has two attorneys on staff who field questions on the open records law, and the most frequent questions they receive are: (1) "How long do I have before I have to respond to this request?" and (2) "What are the factors I need to take into account for the balancing test?" Inefficiency results if custodians must continually contact others to find out their responsibilities for handling open records requests.

According to Assistant Attorney General Allan Lee in the state's Justice Department, the lack of procedural guidelines given to line staff has been another weakness in the application of the open records law. He cites the example of the Madison Metropolitan School District, which received thousands of e-mails from concerned citizens when the district attempted to ban the Pledge of Allegiance. After receiving these e-mails, members of the school board deleted them without realizing they were public records. Lee also noted that school district representatives are unclear whether the phone

calls and e-mails they receive at home from parents constitute public records. Lee has received numerous inquiries from these officials and is concerned that the school districts and local officials are not properly trained to manage these records appropriately (Lee, 2003).

No Centralized Policy for Handling Open Records

Although some agencies have open records online, others do not. Some agencies have opt-out systems, which give individuals the option to have their personally identifiable information (such as home address and telephone number) excluded from the data available online, and some do not. The Wisconsin Department of Transportation (DOT), the University of Wisconsin, the Department of Natural Resources (DNR), and the Department of Regulation and Licensing (DRL) all have attempted to implement some variation of an opt-out system. Each agency, however, operates differently, and limitations vary on the extent to which a person can opt out. For example, the DNR and DRL have no specific provisions for citizens to opt out of public record requests for bulk lists containing information on 10 or more individuals, but they do have provisions for "non-bulk" requests (1999 Wisconsin Act 88).

The Office of Land Information in the Department of Administration (DOA) utilizes another approach to managing electronic access to public records. This agency allows commercial requesters, such as real estate companies, to subscribe to property tax information as a way to limit the electronic availability of information. This subscription option exists despite the fact that those same commercial companies, as well as private citizens, are allowed to request individual records in person.

Other agencies have run into problems by failing to post certain records on the Internet, even though the law does not explicitly require public records to be released electronically. For example, a report by the Environmental Integrity Project of Washington, D.C., looked at the availability of online information in five midwestern states. They determined that Wisconsin lags in posting public records regarding enforcement actions against polluters (Bergquist, 2003).

"Government" Secondary Uses

Technological innovations have broken down administrative barriers, allowing state agencies to share information for purposes for which it was not originally intended. This secondary use of information can be a valuable tool for more efficient government, such as tracking and apprehending criminal offenders with the assistance of All Points Bulletin (APB) alerts. Another example of government secondary use involves the registration and tracking of convicted sex offenders in what is widely known as Megan's Law databases.

Secondary uses of personally identifiable information, however, may raise some privacy issues by allowing the government to record actions of average citizens and keep them on file permanently. While many citizens may approve of the government using information found in public records for law enforcement and to ensure public safety, they also value personal privacy, which is compromised with excessive secondary use of information.

Private Misuse of Information

While government agencies can exert some internal control on how records that contain personally identifiable information are used, allowing public records to be posted on the Internet opens the door for various types of possible misuse by private citizens. This private misuse of information is difficult to regulate, and therefore must be addressed when developing policies regarding online dissemination of public records.

Identity Theft

The open records law has resulted in government that is more open, transparent, and accountable to average citizens. At the same time, electronic technology has given potential identity thieves quicker access to personal information that can be found within online public records. The availability of online data increases the chance for an individual to pool several pieces of personal information that were presumably collected for legitimate purposes, and use them for criminal actions, such as stealing identities or stalking. Identity theft occurs when one individual obtains personal information about another individual, such as a Social Security number, date of birth, account numbers, addresses or phone numbers, with the explicit purpose of committing some type of fraud. For example, thieves will assume the identities of their victims in order to gain access to their financial assets.

In 2001 the Federal Trade Commission (FTC) reported 86,168 instances of identity theft nationwide (Federal Trade Commission, 2001). The most commonly reported offenses were credit card fraud (42%), telecommunications/utility fraud (20%), bank fraud (13%), employment fraud (9%), attempted identity fraud (10%), loan fraud (7%), and government document and benefits fraud (6%). According to an FTC study, 80 percent of those affected had no knowledge of how their personal information was collected, and 87 percent did not know the perpetrator personally. The U.S. General Accounting Office (GAO) reported that although comprehensive crime statistics have been collected only since 1998, identity theft has been increasing in the United States (General Accounting Office, 2002). According to the GAO, seven-year fraud alerts on consumer credit files saw a 65 percent increase between 1999 and 2000, from 65,000 to 89,000, respectively. [2] Furthermore, the Social Security Administration tracked 65,000 reports of identity fraud involving Social Security numbers in 2001, up from 11,000 in 1998. Federal law enforcement officials also reported an increase in identity theft arrests from 579 in 1998 to 645 in 2000 (General Accounting Office, 2002).

Wisconsin's reported identity theft offenses more or less followed national trends in 2001. However, the state had a higher incidence of complaints in telecommunications/utility fraud (26%) and attempted identity fraud (13%) than the national rates of 20 percent and 10 percent, respectively. All in all, in 2001 Wisconsin residents reported 908 cases of identity fraud, and ranked 22nd in the nation in terms of the total number of complaints and 33rd in the number of victims per capita (Federal Trade Commission, 2002).

[2] When credit fraud is reported, consumer credit companies track accounts to note and investigate fraudulent activities for a period of 7 years.

The Wisconsin legislature has recently responded to this increase in identity theft by proposing a new bill that "would allow Wisconsin prosecutors to take jurisdiction of identity theft cases, even those that occur outside the state, as long as the victim is a Wisconsin resident" (Chaptman, 2003). This new bill, sponsored by Rep. Mark Gundrum (R-New Berlin) would also expand the definition of what constitutes personally identifiable information to "computer passwords or account numbers that could be used to obtain anything of value, DNA profiles and biometric data such as fingerprints, voice prints and eye scans of the iris or retina" (Chaptman, 2003). Furthermore, it would prohibit the unauthorized use of information that belonged to a deceased person, "bar possession of another person's identifying information with intent to use it to commit identity theft, and penalize the theft of personally identifying information by impostors who intend to harm the reputation, property, person or estate of an individual" (Chaptman, 2003).

While these are important measures and we applaud Representative Gundrum for introducing this bill, we suggest that strong preventative steps are needed as well. Our recommendations discussed below offer some preventative measures that, if taken together with this new bill, would result in substantial protection for Wisconsin's citizens.

Safety Issues

Safety issues may also arise as the availability of personal information on the Internet increases. In particular, electronic access to public records that contain personally identifiable information increases the chances for stalkers and abusers to cause harm. By conducting a simple open records request, a potential stalker could get a victim's date of birth, race, gender, alias, address, and phone number. Furthermore, victims of domestic violence, knowing that information will be made public may be reluctant to seek help from the courts, such as restraining orders for protection (Study Committee on Public Records, 2003).

"Personal" Secondary Uses

Although some observers express concern about excessive secondary uses by the government, others suggest that secondary uses by private citizens is also a problem. For example, many Web surfers use Google to conduct extensive Internet searches. Sophisticated search engines like Google are able to access comprehensive Internet databases, lowering the cost of searching for information significantly.

Since having access to public records via the Internet virtually eliminated the notion of practical obscurity, there is an increased ability of "information, telecommunications, and imaging technologies to link, share, and integrate disparate bits of information without the information provider's knowledge or consent" (ACLU, April 2003). Private citizens and other nongovernmental entities can download such information and use it for their own personal, nongovernmental purposes. For example, an employer or landlord is currently able to search the Wisconsin Circuit Court Access (WCCA) Web site to see if a potential hire or tenant has an arrest record. The individual could then use the information to discriminate against the potential hire or tenant without his or her knowledge. Last semester, for example, a UW-Madison law student attempted to break up a fight outside a popular Madison bar. The student argued that a witness misidentified him as the instigator, and the student was subsequently charged with

disorderly conduct. This case has yet to be resolved, this student's name, phone number, address, race, gender, and date of birth are now all posted on WCCA, even though he has not been convicted of anything.

Electronic access to public records, therefore, has proven to be a double-edged sword. On the one hand, citizens have more efficient and freer access to information about governmental actions and decision-makers. On the other hand, it is the citizens themselves who are at an increased risk of being victimized by individuals or government agencies who misuse their personal information.

Guiding Principles

The Legislative Council asked us to analyze Wisconsin's open records law addressing these emerging concerns in the process. The following principles guided our analysis and are intended to facilitate policymakers in their efforts to amend Wisconsin's law.

1. *Balancing Public Access and Privacy*

   A critical feature of Wisconsin's representative democracy is the guarantee of openness throughout all levels of government. While the open records law presumes that government records are to be open, the advances in information technology have shifted the balance toward public access at the cost of individual privacy. Realizing that the original intent of Wisconsin's law was to allow citizens to monitor their government, not each other, our analysis suggests realigning this balance without impeding the spirit of openness found in the current law.

2. *Ensuring Security and Accountability*

   Once government became a broker of sensitive personal information, it also became accountable for the conscientious collection and dissemination of that data. The capabilities to mix, merge, and match data electronically only added to this responsibility. Currently, more than 15 state agencies participate in some sort of data exchange with each other. For example, DOT collects names, addresses, and digital photographs and shares this information with local and state law enforcement personnel for the purposes of tracking down individuals with warrants for their arrest. While these cooperative efforts often improve the efficient operations of government, merging may also compromise the confidentiality of that data.

3. *Enhancing Clarity and Allowing Flexibility*

   In order to be useful over time, the open records law should be clear enough to be employed by government agencies successfully and flexible enough to adapt to future changes in technology and the social climate. Our recommendations are intended to serve as clear guidelines for government agencies and legislators to assist them in understanding and implementing those sections of the law that apply to their particular data needs. Our proposals also reflect the dynamic nature of technological development and its impact on the quantity and speed of open records access. They also acknowledge that policy decisions often reflect the

culture, history, political priorities, and institutional memory of government agencies.

4. *Maintaining the Spirit of the Law*

   Where information policy and technology meet, concerns arise on how to maintain the spirit of the law. The American Civil Liberties Union (ACLU) has highlighted several specific concerns, including: (1) the ability of agencies to "link, share, and integrate data without consent"; (2) the "loss of control" over how personal information is used; (3) the "consolidation and centralization" of personal data, and how that may affect the integrity of that information; and (4) the appropriate "standards of fair information practices" to ensure that data are not mishandled (ACLU, April 2003). Although the ACLU's position emphasizes their concern with privacy issues, we believe their worries are nonetheless valid. Our analysis affirms the open records law's presumption toward openness, and our recommendations aim to ensure that the balancing test is able to withstand new challenges brought about by the prevalence of technology and online data.

Recommendations

Given the rapid advances in information technology, states are quickly developing policies to address the issue of electronic access to public records. The majority of states are examining electronic access under the Freedom of Information Acts. In general, most states agree on the following positions:

- All records are presumed to be open
- Exceptions primarily weigh issues of privacy against states' interests
- States determine policy guidelines, local agencies determine policy implementation
- An accurate inventory of records is needed
- An electronic information management agency is needed
- Additional staff should be hired to deal specifically with electronic records requests
- The law should maintain flexibility to adjust for future advances in information technology (Reporters Committee for Freedom of the Press, 2001).

After analyzing the current issues and potential problems that could and do arise from Internet access to open records, exploring the reasons for the inadequacy of Wisconsin's current implementation of the open records law, and considering our guiding principles, we offer the following proposals. We do not suggest that this is a comprehensive list or that we have recognized all the logistical details of each proposal. Instead, we identify several recommendations that may merit further consideration by the legislature. These recommendations relate to either the open records law in general, or to the issue of electronic access to public records specifically.

1. The legislature should create an Open Records Council to identify and address emerging issues and to recommend statutory amendments or regulatory changes.

One way to address many of the problems pertaining to government agencies, including the lack of a centralized policy and inadequacy of training, as well as to safeguard against the personal misuse of information, is to create an Open Records Council. The council would consist of stakeholders representing a wide array of interests, including (but not limited to) the following: registers of deeds, attorneys, clerks of the court, law enforcement personnel, health care professionals, special interest groups, and private citizens. In addition, this group would include others representing privacy interests, such as the ACLU, as well as those advocating openness, such as the media. The governor and the legislature would nominate committee members to serve staggered, fixed terms. This should facilitate the council members in developing expertise and following open records issues through several political cycles. The council would be modeled after the New Jersey Government Records Council. Its duties would include the following:

1) Replying to questions and complaints about the open records law from private citizens and government agencies that maintain open records
2) Issuing advisory opinions and drafting reports for the legislature and state and local departments regarding how well agencies are complying with the open records law
3) Publicizing information (on the Internet and in print form) about the law and the services provided by Open Records Council
4) Training agencies on how to implement the law, such as how to establish protocols for denying requests and what categories of information are subject to the open records law
5) Offering mediation of disputes about access to government records to mitigate the impact the open records law has on the court system

The council's responsibilities to inform the public and assist agencies in complying with the law would be ongoing because the dynamic nature of technology requires more than a one-time legislative fix. As the law is interpreted by the courts and amended by the legislature, guidance would be required on how to implement those changes. Moreover, to ensure that the council has the necessary legal backing to perform these duties, the legislature should amend the law to require agencies to look to the Open Records Council for guidance.

A full-time director and a limited professional and clerical staff would be responsible for daily operations, while council members would serve without pay. Funding would come from program revenue raised by assessing a charge for the various services provided, such as charging agencies subscription fees for mediation and training materials. Any additional financial resources needed from general purpose revenue (GPR) could be justified by benefits such as decreased litigation costs and improved efficiency of open records custodians.

The responsibilities of the council are consistent with our guiding principles. First, because a team of experts can address advances in technology, stakeholder concerns, and interpretation of information categories, the Open Records Council would

ensure an appropriate balance between public access and individual privacy. In addition, it would provide guidance to local and state government to help them collect only that information needed to comply with the law. Further, it would conduct annual reviews of the information categories defined in our recommendation #2, to assess whether specific data should continue to be released as public information, or whether it should be exempt from the open records law for security or other reasons.[3]

Second, the council would monitor security and enforcement issues. For example, the council might make recommendations for additional security measures, such as opt-out or notice policies. These new rules might be needed to ensure that citizens' privacy rights are not compromised as technology changes (Study Committee on Public Records, 2003). In addition, the council would provide a mechanism outside the court system to reconcile different interpretations of the law.

Third, the council would monitor laws and provide training about the open records law and its provisions and requirements of employees of state and local agencies. For example, the council would continue reevaluating the tiered data system (as identified in recommendation #2) to make sure it is consistent with the law. If not, the council would propose new standards to the agencies.

Finally, the Open Records Council would ensure that any statutory or regulatory changes would reflect the goals of the open records law. The council would present recommendations to the legislature or the appropriate municipal or state agencies when it determines that changes are necessary. This obligation would require the council to consult regularly with agencies and citizens to discern any needs they may have for future regulations or statutory changes.

2. The Open Records Council should require state agencies to inventory their public records, which the council could use to develop a tiered, information classification system.

The current open records law lacks guidance and clear security definitions regarding online access to public records. Depending on the agency, some public records are treated with the same extent of openness, regardless of whether the request is made in person, by mail, or through an anonymous database search. The problem with this policy is that some of these records contain highly sensitive, personally identifiable information such as Social Security numbers, dates of birth, mothers' maiden names, and financial account information. In addition, because of the lack of a uniform policy among state agencies for posting online records, by *not* posting public records on the Internet, some agencies are running the risk of violating the law's presumption toward openness.

Therefore, Wisconsin needs a clear set of guidelines regarding the types of information made available on the Internet. The Open Records Council should develop these guidelines.

1) The council would identify certain types of personally identifiable information that should not be released online.

[3] Note: We suggest that the rapid development of technology requires at least a biennial review of categories.

2) The council would have the legal authority to mandate agencies to conduct inventories on the types of records being collected currently.
3) Agencies would then report to the council with a comprehensive inventory on the types of records that the agency is currently collecting, whether these records contain personally identifiable information, and whether these records are currently being placed on the Internet.
4) The council would assess the agencies' responses, and develop a tiered, security system based on access and the types of records currently collected. The council would then submit a set of guidelines for electronic access to that information to agencies.
5) Agencies would be advised to update their online databases to comply with the guidelines.
6) The council would have continuing oversight and could conduct a biennial review of security classifications.

Our recommendation upholds the current degree of openness that citizens enjoy under the current open records law with regard to requests made in person, but assigns additional security to records available for online access. For example, our recommendation would maintain the current security measures for in-person and mail access, which continue to preserve practical obscurity, but it would limit anonymous, unrestricted online access to both commonly published and unpublished information (see Table 1). In addition, we recommend some form of online identification verification, like that discussed in recommendation #3. This would permit access to bulk record requests for ten or more records containing at least one type of personally identifiable information. Table 1 demonstrates a system that the Open Records Council might develop based on input from the agency inventories.

This model has four levels of access, including two levels of access based on the current open records law, and two additions to the law for online access.

- *In Person Access* includes records that are released to individuals who request it in person. This level of access is currently granted under the open records law.
- *Request by Mail,* includes records that are released because of a request by mail. This level of access is currently granted under the law.
- *Internet Access with Online ID Verification* refers to records that will be released to an individual or company who has gained rights to this level of access by registering in person with the prospective agency. According to recommendation #3, the provisions of this verification would need to be determined.
- *Unrestricted Internet Access* includes records that would be available to anybody with an Internet connection, regardless of registration.

This model also has five levels of security assigned to public records from the most open public information at the top to the most sensitive, restricted information on the bottom.

- *Common, Published Information* includes records that have been published and are commonly archived at the state library, such as state budget reports and agency annual reports.
- *Common, Unpublished Information* includes records that should be public, but are not necessarily published in hard copy form, including political campaign contributions, draft bills, meeting minutes, and contact information for government representatives.
- *Bulk Requests* for 10 or more records that contain personally identifiable information includes bulk requests for records that may contain sensitive personal information.
- *Single Requests for records that contain personally identifiable information* includes a single record that may contain sensitive personal information, including one's own record.
- *Highly Sensitive, personally identifiable information* includes requests for social security numbers, birth dates, personal tax records, ongoing criminal investigations, welfare records, medical records, and other types of records that are currently protected by Wisconsin's privacy statutes. This level of security would be further developed by Open Records Council.

TABLE 1: POSSIBLE SECURITY GUIDELINES OF PUBLIC RECORDS

Yes = Access ***No = No Access***

	Access based on the Current Open Records Law		**Additions to Current ORL regarding Internet Access**	
Level of Security, Types of Information	**In Person Access**	**Request by Mail**	**Online Access with ID Verification**	**Unrestricted Internet Access**
Common published information	Yes	Yes	Yes	Yes
Common unpublished information	Yes	Yes	Yes	Yes
Bulk requests (10+) for records containing at least one type of personally identifiable information	Yes	Yes	Yes	No
Requests for a single record containing at least one type of personally identifiable information	Yes	Yes	No	No
Highly sensitive personally identifiable information	No	No	No	No

A tiered system such as this would help agencies in the short term to manage their information during the initial inventory phase. Unknown future advances in information technology may change this security matrix, so the Open Records Council would continue to reevaluate these categories of security and access. Establishing a baseline inventory would also prepare Wisconsin for future challenges in open records online management. In short, agencies would have guidelines on how to manage the online dissemination of public records, as well as an inventory of the types of information currently collected.

3. The legislature should amend Wisconsin's Open Records Law to require the identification of record requesters.

On March 31, 2003, a person known only as "J. Rice" demanded that two state representatives comply with Wisconsin's open records law by releasing a list of e-mail addresses of their constituents who receive legislative updates. Rice also asked for the names and addresses of these people. According to the *Milwaukee Journal Sentinel,* one representative, Sheldon Wasserman (D-Milwaukee), supplied the list of names to Rice, but is still deciding whether to release the street addresses (Maller, 2003). Before releasing the names, however, an aide to Wasserman replied to Rice, asking him or her to identify himself or herself and the motive for the request. Rice declined, responding that Wisconsin's open records law does not require a record requester to identity himself or herself or to explain the motive for the request.

Rice is correct. Wisconsin state law does not require that record requesters be identified. In theory, anyone, including criminals and those with malicious intent, can request information under the provisions of the open records law. As exemplified above, such requests are often approved because of the strong presumption of public access inherent in the law. Before the prevalence of online data, the potential for misuse of personally identifiable information was less problematic because Wisconsin had the built-in safeguard of practical obscurity. Now, however, those with ill intentions are only a few mouse clicks away from retrieving the information they need to cause harm.

Undoubtedly, increased Internet access to public records has significantly reduced the costs of gathering information. Although these reduced costs may have a minimal effect on those who intend to harm a particular individual (because one can still go to a record custodian and request specific information), the effect is much more substantial on those who are in the business of searching for potential victims. Internet technology allows one to explore numerous databases and retrieve vast amounts of information from the comfort of one's home. Because the transformation to online records has far outpaced the legislature's ability to protect the privacy of citizens, we believe it is time to increase the costs of gathering online information by requiring the identification of record requesters.

As with any recommendation, it is critical to identify the ramifications of enactment. Specifically, four issues must be addressed. First, to which records would this new rule apply? In line with our tiered data system set forth in the previous recommendation, this rule would apply anytime a requester attempts to access records that contain highly sensitive, personally identifiable information. For example, if one wanted to access family court records that contain someone else's full name, employer,

income level, and Social Security number, then such records would be released only after the requester's identify has been verified. Not only would this permit the most frequent requests (those that do not contain personally identifiable information) to remain unhindered, but it would also aid in criminal investigations by enabling law enforcement personnel to review a list of record requesters should a crime like identity theft arise. In addition, it would act as a deterrent to potential criminals because they would presumably know that their requests for information can be traced back to them by the authorities.

Second, would the list of requesters become a public record? Although there is an explicit presumption toward openness in Wisconsin's open records law, we see no benefit in permitting the list of requesters to become a public record. In this particular instance, it is important to err on the side of privacy in order to maintain the spirit of openness. Despite this apparent anomaly, it would be prudent to prohibit such a list from becoming a public record because the public should feel free and undeterred to request public records. Knowing that one's name would become a public record may decrease civic participation and thus contradict one of the core values inherent in Wisconsin's open records law.

Third, what are the effects on people who must identify themselves? Assuming that the list of record requesters would remain confidential, the effects on those who must verify their identity are minimal. First of all, because the vast majority of those seeking records do so for legitimate purposes, we believe few would oppose being asked to verify their identity, especially if they believed that their names would be kept confidential. Second, although the added costs of providing identification may reduce civic participation somewhat, we do not believe the costs are substantial enough to affect such participation significantly. However, a more detailed study is needed to address fully the concern of a potential "chilling effect" among current and future record requesters.

Fourth, and most difficult, how would one's identity be verified over the Internet? Even before the verification process, each government Web site containing public records should provide a notice, detailing the rules of and penalties for violating Wisconsin's open records law. This would provide a caveat to all records requesters that they may be prosecuted if the information they request is used for illegal means. In effect, the notice would act as a new, albeit diminished, form of practical obscurity.

In addition, a registration system should be implemented on all government Web sites that contain public records with at least one type of personally identifiable information. This would place agencies in conformity with state administrative rule 12.05(3), which seeks to "maintain confidentiality or restricted access to records or records series maintained in electronic format, *limiting access to those persons authorized by law, administrative rule or established agency policy"* (emphasis added). Registration would require a single trip to the record custodian, where the requester would provide identification such as a driver's license or Social Security card.[4] In return, the requester would receive a username and password that would act as "verifiers." These "verifiers" would then be used when attempting to locate records containing personal

[4] For those who live far from record custodians, or for those unable to make such a trip (i.e., the severely disabled), a mail-in application would suffice. One would simply fill out the application, attach a copy of his or her driver's license or Social Security card, and await a username and password in the mail.

identifiable information from one's home computer. For example, when accessing particular records on Wisconsin Circuit Court Access (WCCA), a screen would appear asking for a username and password. Once verified, the user would have access to every record that is available at the courthouse.

We foresee this recommendation being used in conjunction with, or in addition to, a policy of removing personally identifiable information before a record is posted on the Internet. In at least two ways, however, using a system of identification would be superior to relying simply on a policy of redaction. First, redaction is not a perfect mechanism. Not only does redaction subject citizens to human error, but also not every local agency has the human resources or even the technological capacity to implement a uniform redaction policy. Second, although the initial costs of implementing an identification system would be high, the long-term costs would be lower than maintaining a policy of redaction because agencies would no longer need to employ someone to sift through records and redact personally identifiable information.

Although enacting this recommendation may tilt the scale slightly in favor of privacy, it is nonetheless consistent with our guiding principles. First, it maintains an appropriate balance between public access and privacy by permitting complete electronic access to public records in a more secure environment. Second, in terms of security and accountability, requiring identification will not only act as a deterrent to identity thieves and other potential criminals, but it will also provide investigators with the necessary information to track down any wrongdoers after a crime has occurred. Third, by clearly defining under what circumstances identity verification would be necessary, this recommendation provides clarity for government agencies and legislators. This recommendation maintains the spirit of the law by adhering to the presumption of openness.

4. The legislature should require state agencies to notify individuals when collecting and releasing personally identifiable information on the Internet.

This recommendation attempts to address some of the issues brought to light by government and private secondary use. It should be the government's responsibility to inform citizens when their personally identifiable information is being used for government purposes, or when such information is being made accessible online. The simplest type of notification could come in the form of notices posted on all government documents and Web sites stating that personally identifiable information collected by the agency may be subject to Wisconsin's open records law.

When choosing to make public records accessible via Internet databases or Web sites, government agencies should notify and inform those individuals whose personally identifiable information is involved. Beginning after a designated start date (to be determined by the legislature), an informed consent form should be presented to the individual at the front end, namely, at that point where the information is collected.

Wisconsin should consider requiring agencies to adopt notification and consent forms, both at the point of collection and at the release of personally identifiable information. Issuing notice at the point of collection serves two purposes. First, it would inform the individual about the potential use of the information by the government. Second, it would ensure that the state has taken a substantive step in protecting the

privacy of the individual. We believe this consent process will assist records custodians in utilizing the balancing test by maintaining the presumption of openness while protecting privacy rights.

Minnesota shares with Wisconsin a legacy of progressive and open government, yet Wisconsin can benefit by examining Minnesota's policy on open records on the Internet. Minnesota's policy on public records disclosure is similar to federal law, and is found in the Minnesota Government Data Practices Act. Similar to Wisconsin's law, Minnesota's declares an overall presumption to openness to public records and asserts that records deemed public are to be free of charge for "inspection" and copies of public records will be provided for a requester at a "reasonable" cost. Under Minnesota's law, sensitivity to individual privacy is exemplified in the individual rights. Minnesota believes that citizens have the right (1) to know what data the government maintains on them; (2) to inspect such data; (3) to receive copies upon request; (4) for copies to be provided at reasonable cost and; (5) to challenge the accuracy and completeness of the data (Minnesota Department of Administration, 2002).

Minnesota has developed an informed consent form to issue individuals at the time of receiving personal information. This form is called a "Tennessen warning notice" (see Appendix II). The Tennessen warning notice both limits the state's liability and gives the state permission to provide unrestricted access to the information (Minnesota Department of Administration, 2002).

The warning serves to inform the individual of the following:

- Reasons for data collection
- Persons or entities who will be authorized by law to receive the data
- Intended use of data
- Legal obligations to supply data
- Consequences of either supplying or refusing to supply data

In addition to providing notices on government documents and agency Web sites, Wisconsin could benefit from adopting a similar notification system at the time of data collection. This notice would be issued to inform citizens of the reasons their personal information is being collected for use in public domains, including Internet databases.

Conclusion

Although Wisconsin's open records law has retained some of the exceptions developed at common law, it remains one of the broadest in the country (Doeppers, 2003). Based upon the recognition that "a representative government is dependent upon an informed electorate," Wisconsin's open records law presumes that the more open government is, the better (Wis. Stat. § 19.31, 1999–2000). Indeed, by declaring that "all persons are entitled to the greatest possible information regarding affairs of government," the Wisconsin legislature solidified the state's commitment to transparent, open, and accountable government (Wis. Stat. § 19.31, 1999–2000).

Even with the law's strong presumption toward openness, however, Wisconsin's law does not require public record information to be available via the Internet, as long as

records are fully accessible from the records custodian. Yet electronic access to public records makes government more transparent by providing an easy, convenient, and efficient way for citizens to monitor government and its representatives. In Wisconsin, the strong presumption toward openness is steeped in state's legislative and judicial history, and such openness is an underlying characteristic of any representative democracy. We therefore believe that this presumption should prevail, even in today's age of technology. Moreover, Wisconsin is not alone in its philosophy. Whether it is the enactment of the federal Freedom of Information Act, or the fact that all 50 states and the District of Columbia have enacted open records laws similar to Wisconsin's, there is bountiful support for our state's vision of open government (Roang, 1994).

Nevertheless, we are concerned that this increased transparency may result in the unintended consequence of people misusing personally identifiable information that is now widely available to the general public. In the past, the concept of practical obscurity limited malicious uses of such information, but that notion is quickly vanishing.

To address this concern, we set out to ascertain the extent to which improvements in technology and increased access to online data were changing the balance between public access and private harm. Although we did not come across extensive evidence of either identity theft or stalking that resulted from accessing online records, there exists great potential for additional problems to arise as both technology and the sophistication of potential wrongdoers advances.

Therefore, our recommendations focus on preventative measures that attempt to permit the greatest amount of openness while adequately protecting citizens' privacy. To its credit, Wisconsin currently ranks high in privacy protection. In our view, increased electronic access to public records creates the potential for some of these privacy protections to wither. We hope our recommendations will enable officials to apply the balancing test more effectively so that it can withstand the challenges brought forth by new technologies and widespread access to online data.

Appendix I: Personal Information Collected and Distributed by Government

1) Name and address (drivers' licenses, and directories)
2) Property description, location, and value (land records and property taxes)
3) Property ownership and mortgage loans (land titles and deeds)
4) Corporate assets, financial abstracts, and executives' background (UCC filing, liens, and judgments)
5) Net income tax paid (tax filing as per Wisconsin law)
6) Home size, price, and physical description (tax assessments)
7) Parents and children (vital statistics)
8) Gender and date of birth (drivers' licenses and voting applications)
9) Occupational status (occupational and professional licensing)
10) Vehicle make and model (vehicle registrations)
11) Accidents and citations (driver records, court records)
12) Boat and airplane ownership (licenses)
13) Political contributions (election board)
14) Hobbies and recreational interests (hunting and fishing licenses and tourism inquiries)
15) Pet ownership (licenses)
16) Criminal history, arrests, and convictions (court records)
17) Divorce, custody proceedings, and wills (court records)
18) Bankruptcies for 50 years (Now Internet access to bankruptcy records)
19) Social Security Numbers (most government forms, marriage and death certificates, custody decrees, bankruptcy records, etc.)

Source: ACLU Data Privacy Project, "Kinds of Personal Information Collected and Often Released by Government."

Appendix II: Minnesota's Tennessen Warning Notice[5]

[IDENTITY OF AGENCY/ENTITY]

CONSENT FOR RELEASE OF INFORMATION

We are asking for your consent (permission) to release information about you to the entities or persons listed on this form. The information can't be released without your consent. This form tells you what information we want to release, or what information we want another entity to release to us. This form tells you the reasons we are asking for your consent. You have the right to look at all the information to be released and have copies of it. You should do this before you give your consent to release the information. If you want to look at the information or have copies of it, you must talk to (NAME AND HOW TO CONTACT).

You may consent to release *all* of the information, *some* of the information or *none* of the information. You may consent to release information to *all*, *some*, or *none* of the entities listed on this form.

If you give us your consent, we can release the information for (TIME PERIOD) or until (EVENT OR CONDITION). You may stop your consent any time before (THIS TIME PERIOD, EVENT, OR CONDITION). If you want to stop your consent, you must write to (NAME AND ADDRESS OF PERSON) and clearly say that you want to stop all or part of your consent. Stopping your consent will not affect information that already has been released because you gave your consent.

You do not have to consent to the release of any information that tells people that you or your child is disabled. If you are asking for help because of a disability, we may need information about the disability in order to help you.

If you have a question about anything on this form, please talk to (NAME) before you sign it.

[A.] I authorize the [entity] to release information about [name of data subject]. I understand:

[B.] The information I agree to let you release is:

[C.] The information will be given to:

[D.] You are asking me to release this information so that:

[E.] If this information is released, what will happen is:

[F.] If this information is *not* released, what will happen is:

[G.] Signature of client_____ Date signed_____

[H.] Signature of parent or guardian_____ Date signed_____

[I.] Signature of person explaining this form _____ Date signed_____
and my rights _____ Date signed_____

[5] State of Minnesota, Department of Administration. Information Policy Analysis Division, "Model Policy Access to Government Data and Rights of Subjects of Data," July 2000.

References

American Civil Liberties Union, " Cyber-Liberties," http://www.aclu.org/Cyber-Liberties/Cyber-LibertiesMain.cfm, accessed February 17, 2003.

American Civil Liberties Union, Data Privacy Project, "Kinds of Personal Information Collected and Often Released by Government," State of Arizona, *Arizona @ your service* - http://www.az.gov/webapp/portal/, accessed February 27, 2003.

American Civil Liberties Union, Wisconsin Data Privacy Project, "Privacy, Open Records, and the Tradeoff of Values," http://www.aclu-wi.org/issues/data-privacy/speech2.html#link, posted July 4, 1998, accessed April 4, 2003.

State of Arkansas *accessArkansas.org – The Official Website for the State of Arkansas* http://www.accessarkansas.org, Accessed February 28, 2003.

Arkansas Office of Information Technology, "Standard Statement – Security SS-70-55," http://www.techarch.state.ar.us/domains/security/standards/pki_standard_statement.doc accessed February 27, 2003.

Bergquist, Lee, *Milwaukee Journal-Sentinel*, "Study Faults State on Accessibility of DNR Records," http://www.jsonline.com/news/state/apr03/130684.asp, Milwaukee: *Milwaukee Journal-Sentinel*, last updated April 2, 2003, accessed April 10, 2003.

Burnett III, James H., "Man gets 3 years in prison for identity theft; College graduate lived off fraudulent credit cards," *Milwaukee Journal – Sentinel*, Section: News P. 03B, August 30, 2002.

State of California, "My California website," http://www.ca.gov/state/ Viewed February 28, 2003.

Center for Democracy and Technology, "A Quiet Revolution in the Courts: Electronic Access to State Court Records: A CDT Survey of State Activity and Comments on Privacy, Cost, Equity and Accountability," http://www.cdt.org/publications/020821courtrecords.shtml, accessed February 20, 2003.

Chaptman, Dennis, "Year Long Study Brings Proposals to Toughen State Identity Theft Law," *Milwaukee Journal - Sentinel*, Section: News, Pg. 01B, April 8, 2003.

City of Wichita, Kansas, "A Guide to Open Records: Exemptions: K.S.A. 45-221," http://www.wichita.gov/gov/manager/exemptions.asp, copyright 2000, accessed February 17, 2003.

Competitive Enterprise Institute (authored by Solveig Singleton, Senior Analyst), *Arizona Issue Analysis 171*, "The Freedom of Information Versus the Right to Privacy: A Pro-Market Framework for Arizona," The Goldwater Institute, May 24, 2002.

Doeppers, Carole, *Personal interview with authors,* Madison, WI: March 3, 2003.

Doeppers, Carole, Issues of Public Records on the Internet: Discussion Notes, undated.

Electronic Government Task Force: Strategic Issues Subcommittee, prepared by the Department of Information Resources, Austin, Texas, "Privacy Issues Involved in Electronic Government," http://www.dir.state.tx.us/egov/report/privacy.html, August 2000.

Enterprise Information Architecture Working Group, "Practical Approaches to Electronic Records Management and Preservation (Draft)," August 2001 http://www.techarch.state.ar.us/domains/information/resources/RecordMgtGuideline_v2.pdf Accessed February 27, 2003

Erpenbach, Jon, Wisconsin State Senator. *Personal interview with authors*, Madison: February 26, 2003.

Federal Trade Commission, "Identity Theft Complaint Data Figures and Trends on Identity Theft January 2000 through December 2001," Federal Trade Commission, http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf, 2002.

Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, Washington D.C.: Division of Financial Practices, Bureau of Consumer Protection, May 2000.

Freedom Forum, "Kansas Governor Puts Teeth into Open Records Law," Arlington: Freedom Forum, http://www.freedomforum.org/templates/document.asp?documentID=12474, accessed February 17, 2003.

Givens, Beth, *Public Records on the Internet: The Privacy Dilemma,* San Diego: Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/onlinepubrecs.htm, accessed March 8, 2003, pp. 2-3.

The Goldwater Institute, "Arizona Issue Analysis 171: The Freedom of Information versus the Right to Privacy: A Pro-Market Framework for Arizona," The Goldwater Institute, http://www.goldwaterinstitute.org/article.php/35.html, May 24, 2002.

Government Accounting Office, "Identity Theft: Prevalence and Cost Appear to be Growing," http://www.consumer.gov/idtheft/reports/gao-d02363.pdf, March, 2002.

Government Records Council, http://www.nj.gov/grc/, accessed March 2003.

Lee, Allan, State of Wisconsin Assistant Attorney General, *Personal interview with authors*, Madison: February 28, 2003.

State of Minnesota, *Minnesota north star: home,* http://www.state.mn.us, accessed February 27, 2003.

State of Minnesota Department of Administration, Information Policy Analysis Division *Information Policy Analysis Division Web Site* http://www.ipad.state.mn.us/ Accessed 28, 2003.

State of Minnesota, Department of Administration, Information Policy Analysis Division, "Preserving and Disposing Government records," http://www.ipad.state.mn.us/docs/p_d.pdf, July 2000.

State of Minnesota, Department of Administration, Information Policy Analysis Division, "Model policy public access to government data and rights of subjects of data," http://www.ipad.state.mn.us/docs/model_policyw.doc, July 2000.

Minnesota State Statutes, ss. 13.03, subd 3(c).

National Council of State Legislatures, PowerPoint Presentation by Adam White Scoville, "Effective Open Government in the Electronic Age," http://www.ncsl.org/programs/lis/cip/PPT/ascoville, presented at the 2002 NCSL Annual Meeting, Friday, July 26, 2002.

National Council of State Legislatures, "DRAFT: 2002 Information Technology & Internet Laws," http://www.ncsl.org/programs/lis/legislation/itech02.htm#_Toc30920536, accessed February 20, 2003.

New Jersey Supreme Court, *Higg-A-Rella, Inc. v. County of Essex,* 141 N.J. 35, 48-49, 660 A.2d 1163 (1995).

Pennsylvania Supreme Court, *Hoffman Pennsylvania v. Game Commission,* 455 A.2d 7321 734, PA Commonwealth, 1983.

Preston, Ethan, *Journal of Technology Law and Policy*, "Finding Fences in Cyberspace: Privacy and Open Access on the Internet," http://grove.ufl.edu/~techlaw/vol6/Preston.html, University of Florida, Levin School of Law: 2000.

Privacy Journal. "Ranking of States in Privacy Protection," http://www.privacyjournal.net/events.htm, accessed April 28, 2003.

The Reporters Committee for Freedom of the Press, *Tapping Officials' Secrets: Fourth Edition,* Arlington, VA: The Reporters Committee for Freedom of the Press, also available at http://www.rcfp.org.tapping/index.cgi, 2001.

Roang, Sverre David, "Toward a More Open and Accountable Government: A Call for Optimal Disclosure under the Wisconsin Open Records Law," 1994 Wisconsin Law Review 719.

Shelleby, J. B., "Online Court Records Raise Privacy Issues," Ipswich Chronicle, February 19, 2003, http://www.townonline.com/ipswich/news.html, accessed March 2003.

State Bar of Wisconsin, prepared by the Government Lawyers Division, Standing Committee on Public Records and Open Meetings, *Understanding the Wisconsin Open Records and Open Meetings Laws,* Madison: State Bar Association, current as of December 1999, p. 4, p. 51.

Study Committee on Public Records, *Examination of the Effects of Advanced Technologies on Privacy and Public Access to Court Records and Official Records: Final Report,* Florida: Study Committee on Public Records, created by the Florida Legislature, February 15, 2003, pp. 6-8.

Wisconsin Department of Administration, *Wisconsin Administrative Code, Chapter Adm 12,* "Electronic Records Management – Standards and Requirements," Madison: Department of Administration, Register February 2002, No. 554, pp. 26-27.

Wisconsin Department of Justice, "Public Records/Open Meetings Information," http://www.doj.state.wi.us/dls/spar.asp#pubrec, accessed February 4, 2003.

Wisconsin Professional Police Association-Working to Protect and to Serve Wisconsin's Finest, Gordon McQuillen Cullen, Weston, Pines & Bach "A Brief History Of The Open Records Law In Wisconsin," http://wppa.com/Oldarticles/openreco.htm, accessed February 17, 2003.

Witynski, Curt, Assistant Director of the League of Wisconsin Municipalities, *Personal interview with authors*, Madison: March 3, 2003.