Final
Legislative Council Staff Report
on

Public Records, Privacy, and Electronic Access in Vermont

Pursuant to Sec. 5 of No. 158 of the Acts of the 2003 Adj. Sess. (2004)

January 2005

Legislative Council
State House
115 State Street—Drawer 33
Montpelier, VT 05633-5301
(802) 828-2234
www.leg.state.vt.us

Principal author:
Michael J. O'Grady, Legislative Council

Public Records, Privacy, and Electronic Access in Vermont
Legislative Council Staff Report
Table of Contents

Executive Summary

Act 158 of the 2004 session of the General Assembly required Legislative Council to study the public records law of the state of Vermont, the justification for state record requirements, privacy concerns regarding the dissemination of public records containing personal information, and the use of public records. In addition, Act 158 required Legislative Council to recommend to the house and senate committees on local government and government operations potential approaches that the state could adopt to conform the public records law of the state with technological advances and associated privacy concerns.

Staff views the goal of the study, generally, as the production of potential approaches "to conform the public records law of the state with technological advances and associated privacy concerns." In furtherance of this goal, Staff reviewed current Vermont law, examined laws passed by other entities, and interviewed interested parties who were knowledgeable about the public records law of Vermont and who proposed issues that Staff should address in the study. Subsequently, Staff prepared an in depth report on the current public records law in the state and legislative alternatives available to the General Assembly to address mounting privacy concerns associated with evolving technology and access to public records. This abstract summarizes the analysis included in the report and the legislative alternatives proposed by Staff.

I. Summary of Analysis

Part I of the report summarizes the need for adequate public recordkeeping and the facts leading up to the legislative council study. Access and inspection of public records are integral to government accountability. Consequently, Vermont requires public records to be open and available to citizens of the state. Until recently, thorough review of public records could be time consuming due to both poor record keeping and the mechanics of shifting through volumes of paper. Evolving technology and government use of electronic records and the Internet have begun to facilitate access to and use of public records. Electronic records are still subject to poor records management, but computers accelerate the ability to search and discard unnecessary or poorly managed records. However, the use of electronic records and the Internet has led to increased distribution and, some would argue, misuse of public records and the personal information they contain. Public records custodians are sensitive to the potential for misuse of public records and are often reluctant to disclose public records that contain personal information. Such a situation arose in 2003 when the Town of Colchester initially refused to disclose a computer database containing the city's property tax assessment data. The town claimed that the database contained personal information that could be misused if disclosed, while other argued that the town resisted disclosure because of the recording fees it would lose by disclosing one electronic copy of the database versus hundreds of paper pages. Eventually, the city disclosed the database, as required by state law, but the issue was brought to the attention and review of the General Assembly, thereby inspiring Act 158 and this report.

Part II of the report details the public record requirements of the state under statute and case law. The Vermont Constitution provides that all government officers of the state are accountable to the public. This accountability is fulfilled in part through the Public Records Act of Vermont, which declares that public records are subject to inspection and review by citizens

of the state. Inspection and review is not absolute. People retain a right to privacy under the Act, and the General Assembly specifically exempts certain records from disclosure. However, the right to privacy and many of the Public Records Act exemptions are not clearly defined by statute, and, consequently, the Vermont Supreme Court often is called on to interpret the act. Part II examines certain Court interpretations, such as what constitutes the right to privacy and what constitutes "the course of agency business" as referenced in the definition of public record. Part II also discusses criticism of the Public Records act and examines the public records requirements of other jurisdictions, including personal privacy exemptions, Fair Information Practices Acts, and limited access or use of public records.

Part III of the report evaluates the state archival and vital records management programs. The archival records program is administered by the Vermont State Archives and preserves public records that have continuing legal, administrative, or historic value. The archival organization and management requirements of Vermont are similar to the archival management programs of other states, except that most states, unlike Vermont, have an archival management program for electronic records. The vital records program, as administered by the Department of Health regulates the issuance of records that document the births, deaths, marriages, civil unions, divorces, and fetal deaths occurring in the state. The vital records program is also responsible for processing court orders for, among other purposes, name changes, corrections, and foreign born adoptions. Most states regulate vital records through their respective Department of Health, but only Vermont requires documentation of civil unions, divorces, and fetal deaths. In addition, Part III discusses recent federal legislation that will require significant changes in the state vital records program, including use of engraved paper, proof of identity prior to access to vital records, and building security for vital records storage.

Part IV discusses whether a right to privacy in personal information exists under state and federal law. The U.S. Supreme Court has recognized a right to privacy in personal information, but requires that any asserted right to privacy be balanced against the public interest in disclosing the information at interest. However, the Court failed to adequately define the scope and application of the right to privacy under this test. Consequently, the right to privacy in personal information is inconsistently applied and sometimes questioned. Nevertheless, most federal and state courts recognize the right and apply the test set forth by the U.S. Supreme Court, but in doing so, the federal interest in disclosure has always been upheld. Nevertheless, recent U.S. Supreme Court decisions under the federal Freedom of Information Act indicate that the right to privacy is not based solely on the U.S. Constitution and, thus, is more far reaching. Vermont also provides protection of personal privacy through court recognition of the invasion of privacy tort and through recent identity theft legislation that criminalizes the misuse of personal identifying information. Other states utilize additional approaches to protect the privacy of personal information, including codifying a right to privacy or invasion of privacy and criminalizing an invasion of privacy through use of a computer.

Part V describes various issues surrounding the public records management of electronic records, including disclosure of government computer databases, disclosure of government e-mail, and the difficulty of managing electronic records in light of the rapid evolution of computer and digital technology. Under Vermont law and the law of most states, computer databases are public records subject to disclosure. However, several states limit access to or use of databases,

and some states charge an additional fee for access to databases. In at least one state public records stored in a database are subject to inspection in print format only. As with databases, government e-mail is also a public record if produced in the course of agency business. Because the term "in the course of agency business" is not defined sufficiently by statute or case law, some questions remain as to what government e-mail is subject to disclosure. Others states have addressed the disclosure of e-mail clearly through state statute, case law, or advisory opinions. Generally, government e-mail is subject to disclosure when furthering agency or government purposes, but some states provide disclosure exemptions for certain types of government e-mail, such as e-mail correspondence between legislators and their constituents. Other states, unlike Vermont, have also addressed the application of open meeting laws to e-mail correspondence between members of a public body. Some states require such correspondence to be open to the public when discussing the business of the body. Part V also discusses the need for mandatory guidelines for the management of electronic public records, especially in light of the evolving computer and digital technology on which many electronic records programs are based.

Part VI reviews the administration and regulation of records management in Vermont, with a focus on the organizational structure and staff of the state agencies with authority over records management. The majority of the regulatory authority for records management generally lies with the state department of buildings and general services (BGS), specifically the Office of Information Specialist within BGS. The Vermont State Archives and the Department of Health have regulatory authority over the respective management of archival records and vital records. Part VII also discusses criticism of the state records management program and provides examples of other state approaches to records management. Part VII attributes the majority of the problems with the state records management program to a lack of funding, staff, and sufficient storage space. In addition, Part VII describes the need for management of state and local public records forms and how other state programs regulate form creation and distribution.

The report also includes two appendices addressing related public records management issues and requirements. Appendix A examines the issue of posting court records and the personal information contained within them to the Internet. The public has a federal common-law right of access to court records, but in most states the state public records law supersedes the common-law right of access to court records. In Vermont, the right of access to and dissemination of electronic court records is controlled by the Court Rules of the State. These rules attempt to limit the disclosure of sensitive personal information, including exempting from disclosure 33 categories of court records and information. Part VI also discusses approaches used by other states regarding electronic courts records and their dissemination and posting to the Internet.

Appendix B summarizes pending federal legislation and current federal statutes that impact management of public records in the state. Recently, the U.S. Congress enacted law impacting records management in Vermont. The new federal requirements will require birth certificates and drivers licenses to meet minimum standards. The requirements will be set by rule, but the issuance of birth certificates will, at a minimum, be subject to additional security requirements such as required use of engraved paper and proof of identification of the party requesting the record. Drivers' licenses will also need to meet minimum requirements, including a prohibition on the display of Social Security numbers on licenses. Appendix B also discusses

the records management requirements of the Federal Records Act, the Privacy Act of 1974, the Electronic Communications Privacy Act (EPCA), the Freedom of Information Act (FOIA), the Health Insurance Portability and Accountability Act, the Family Educational Right to Privacy Act, and the Patriot Act.

II. Legislative Alternatives

As required by Act 158, this report provides recommendations of potential approaches that the state can take to conform the public records law of the state with technological advances and associated privacy concerns. The recommendations are presented as legislative alternatives available to the General Assembly. Each recommendation discusses the benefits of the legislative alternative and any possible negative impacts or obstacles. The legislative alternatives included in the report are summarized below in the order they appear in the report.

A. Part II: Public Records Act

1. Reorganize Public Records Act and Other Exemptions

The General Assembly could reorganize the Public Records Act. All 160 disclosure exemptions could be listed in one statutory section, and the public records inspection and disclosure requirements of 1 V.S.A. §§ 315 to 320 could be consolidated with the public records management requirements of 22 V.S.A. §§ 451 to 457. Reorganization and consolidation may help to eliminate confusion and allow for improved records management. However, reorganization could be problematic, would require substantial statutory revision, and could create more confusion than it eliminates.

2. Enact a Disclosure Exemption for Disclosures that Constitute an Invasion of Privacy

The General Assembly could enact a disclosure exemption for documents the disclosure of which would constitute an invasion of privacy. Such an exemption could be used to prevent the unwarranted disclosure of personal information in public records. Several states include such an exemption in their public records law. Adding such an exemption would require clarification of what constitutes the right to privacy.

3. Adopt a Fair Information Practices Act

The General Assembly could enact a Fair Information Practices Act. Fair Information Practices Acts provide for public review of personal information in government records and limit the dissemination of personal records and data regarding an individual. A Fair Information Practices Act would supply additional privacy protection while ensuring continued availability of public records. Requiring municipalities to implement a Fair Information Practices Act may be problematic, would require additional municipal staff, and could raise liability issues.

4. Clarify What Constitutes Agency Course of Business

The General Assembly could define what constitutes "the course of agency business" under the definition of "public record" in 1 V.S.A. § 317(b). Defining the term would clarify the types of documents subject to public inspection and review. The clarification would be especially relevant with regard to e-mail, which often is a personal communication unrelated to agency business.

5. Limit Access to Public Records

The General Assembly could restrict or rescind the state open records policy to afford more protection to personal information contained in public records. Limiting access to public records based on legitimate need or authorized use would help prevent unnecessary disclosure of personal information, but likely would be unpopular.

B. Part III: State Archives and Vital Records

1. Implement and Fund an Electronic Archival Records Management Program

The General Assembly could require the Office of State Archives to implement and manage a program for the acquisition and preservation of electronic archival records. With the ubiquity of computers, many public records—especially e-mail correspondence—are created and utilized strictly in electronic form. Without an electronic archival records program, records could be lost and with them a potentially important part of Vermont history. Implementation of an effective electronic archival records program will require long-term funding and commitment to technology upgrades.

2. Require Security Features for the Issuance and Review of Vital Records

Under the recently enacted federal Intelligence Reform and Terrorism Prevention Act, Vermont will need to conform with minimum federal standards set by rule. for the issuance of birth certificates. Compliance with the federal standards will not be required until 2008. However, statute requires the federal regulations to include, at a minimum, requirements for the use of safety paper and proof and verification of identity as a condition of issuance of a birth certificate. The General Assembly could begin the transition to the federal standards by requiring use of safety paper or proof of identity at an earlier date. Implementing the federal requirements could be politically unpopular because it will transform Vermont from an open records state to a closed records state. Requiring implementation of the two minimum standards at an earlier date might ease transition to the more extensive final federal standards.

C. Part IV: Right to Privacy in Personal Information

1. Clarify Right to Privacy in Statute

The Vermont Public Records Act statement of policy provides all people with a right to privacy in their personal and economic pursuits, but the existence, scope, application, and enforcement of the right to privacy are not sufficiently set forth in the statement of policy or the Public Records Act in general. The General Assembly could clarify the application and extent of the right to privacy. Such a clarification would also help resolve questions regarding disclosure exemptions that incorporate an invasion of the right to privacy as part of the standard for withholding documents.

2. Create Statutory Civil Action for the Invasion of Privacy

The General Assembly could create a statutory civil action for invasion of privacy and, in so doing, adopt a standard that would allow individuals to seek damages for the misuse of personal information collected from public records. The General Assembly could codify invasion of privacy as either a tort or as a crime. Vermont courts currently recognize the tort of invasion of privacy. Codifying the standard employed by the courts would likely meet little resistance. It might be argued that recently adopted identity theft legislation sufficiently addresses the misuse of personal information and that codification of an action for invasion of privacy is not necessary.

3. Create Crime of Invasion of Privacy by Computer

The General Assembly could create the crime of invasion of privacy by computer under which an unauthorized person is guilty of a crime if he or she uses a computer to intentionally examine any employment, salary, credit or any other financial or personal information relating to any other person. Such activity is a crime in Virginia. It might be argued that recently enacted identity theft legislation addresses this problem, but the identity theft provisions only prohibit the misuse of personal information, whereas under computer invasion of privacy, mere examination of or unauthorized access to personal information of another via computer would be considered a violation.

D. Part V: Electronic Records and Privacy: Databases, E-Mail, and Evolving Technology

1. Prohibit or Limit Access to Computer Databases

The General Assembly could limit or prohibit access to computer databases that store public records. Prohibiting access to databases would prevent the misuse or commercial use of personal information contained within databases, but such limitation contradicts the state open records policy. Alternatively, the General Assembly could limit access to databases based on the requesting party's intended use of the database. Many states restrict access to public records based on intent or identity of the requesting party. Such a limitation would also violate the state open records policy. The General Assembly also could extend the current temporary restriction on access to databases and permanently provide that records stored in computer databases shall

only be available in print format. Again, such a restriction might be considered in conflict with the state's open records policy and current law.

2. Limit Personal Information Included in Public Records Computer Databases

The General Assembly could require that state and municipal agencies only include necessary personal information in their computer databases. The personal information included in many databases is unnecessary to the government function which they serve. Limiting the use or storage of personal information in databases would address privacy concerns surrounding disclosure of computer databases. Several states already strongly encourage or require the use of necessary information in databases.

3. Authorize an Additional Service Charge for Access to or Disclosure of Databases

The General Assembly could authorize an additional service charge for access to or disclosure of computer databases or other electronic records. Several states currently impose such fees, which attempt to account for the actual cost of database creation and management. Such a fee could be opposed by business interest that frequently access public records and public records databases. However, the General Assembly might deem it appropriate for business interests that frequently use and profit from the service to pay for part of it.

4. Clarify Application of the Public Records Act to E-Mail

The nature of e-mail correspondence and pervasive government use of e-mail have inspired questions regarding whether e-mail is a public record subject to disclosure and, if so, whether certain e-mail is exempt from disclosure. In addressing these questions, the General Assembly has three options. First, it can do nothing. Under the current definition of "public record" and as interpreted by the Vermont Secretary of State, government e-mail sent in the course of agency business is a public record subject to inspection and review and additional records management requirements. Thus, purely personal e-mail apparently would be exempt from disclosure, but e-mail sent in the course of agency business would be subject to disclosure. However, the term "course of agency business" is not defined in statute. Consequently, the no action option leaves the question of what constitutes publicly available government e-mail subject to state agency and court interpretation.

The second option is to amend the definition of "public record" to include e-mail. The General Assembly could clarify whether all e-mail sent from government computers or by government employees qualifies as a public record or whether only e-mail sent in the course of agency business is a public record. The General Assembly could also define what constitutes the course of agency business and add specific exemptions for certain types of e-mail, such as legislative e-mail. In amending the definition of "public record" as it relates to e-mail, the General Assembly should be aware that many state employees currently have an expectation of privacy in e-mail sent from their government computers and might view any legislative efforts subjecting government e-mail to public inspection as a violation of their right to privacy.

As a third option, the Vermont General Assembly could encourage a Vermont state agency, such as the secretary of state or the BGS Office of the Information Specialist, to issue a rule on the use and management of e-mail. The Secretary of State currently provides electronic records management and information tools, which include guidance on e-mail management, but these tools are advisory in nature.

5. Exempt Legislative E-Mail from Disclosure

The General Assembly could enact a disclosure exemption for legislative correspondence with constituents in order to protect the privacy interests of constituents and prevent disclosure of personal information included in such e-mail. At least six states possess similar exemptions. This exemption could be criticized as limiting the transparency and accountability of the General Assembly.

6. Clarify Application of Open Meeting Law to use of E-Mail by Public Bodies

Another issue raised by government use of e-mail is whether the state Open Meeting Law applies to e-mail exchanges among members of a government body. State law does not address this issue. The General Assembly could clarify the application of the Open Meeting Law to e-mail communication between members of a public body by amending the Open Meeting law to provide that e-mail communication between a quorum of the members of a public body is prohibited or authorized under certain limitations. As an alternative, the General Assembly could recommend or require the Office of Attorney General or the Office of the Secretary of State to issue an advisory opinion regarding the application of the state Open Meeting Law to e-mail communication between members of a public body.

7. Require Issuance of a Mandatory Electronic Record Keeping Policy and Manual

The General Assembly could require the Office of the Information Specialist, Secretary of State, or other entity to adopt a mandatory electronic recordkeeping policy and manual for state agencies. The Vermont Secretary of State and Office of the Information Specialist both issue records management manuals that address electronic records management, but these manuals are advisory in nature.

E. Part VI: State Records and Forms Management

1. Increase Public Records Funding, Staff, and Storage Space

The Vermont state agencies with records management authority are underfunded and understaffed. Without increased funding and staff, records management in Vermont likely will not improve and existing records will continue to degrade. Such degradation of records could have significant impacts on the functioning of state government. For example, current legislative records are rapidly degrading. Without funding for restoration, these records will be lost and, consequently, executive agencies and courts could usurp legislative power by interpreting legislation without the aid of records indicating legislative intent. The General Assembly could increase the funding for records management and could require additional staff for the BGS

Office of the Information Specialist, the Vermont State Archives, and the Department of Health vital records program. Increased funding and staff will allow for increased records training and inspection of agency records management. The General Assembly also could plan for or appropriate funding for construction of additional public records storage space.

2. Reorganize Records Management Structure

The General Assembly could require the reorganization of records management authority in the state by consolidating the BGS Office of the Information Specialist records management program and the State Archives. Such a consolidation would focus the state records management program, allow for more effective use of records management resources, combine the state's records management expertise, and increase administrative efficiency. Consolidation might not be politically popular among the state agencies that currently manage public records. Consolidation likely would not need to include the vital records program of the Department of Health.

3. Require State Approval and Review of Government Forms

The General Assembly could delegate to the BGS Office of the Information Specialist (OIS), the Public Records Advisory Board, or the State Archives authority to review and approve state agency and municipal forms. The personal information required by many government forms is unnecessary to the government function to which they serve. An oversight authority could prevent the use and subsequent disclosure of unnecessary information. An oversight authority could also develop form management standards and provide advice on creation of forms, including content and format.

4. Authorize Increased Records Management Enforcement and Penalties

The Vermont state agencies with regulatory authority over records management in the state possess little oversight and penalty authority over state and local records custodians. The Office of the Information Specialist, the State Archives, and the Department of Health vital records program collectively and individually are knowledgeable and conscientious about compliance with the state public records requirements. However, records custodians at other state agencies and at the municipal level have little incentive to comply with records management requirements, and current standards management and personnel practices are not always effective. The General Assembly could grant the OIS oversight authority and could increase the penalties for improper records management. Meaningful administrative penalties could encourage state agency heads and municipalities to devote more funding, staff, and time to proper records management

5. Require Increased Records Management Training

The General Assembly could require the BGS Office of the Information Specialist, State Archives, or other entity to increase the records management training available to state and municipal records custodians. In addition, the General Assembly could require mandatory

training or certification for records custodians. Increased training, however, will require increased funding and staff.

6. Increase Recording Fees and Allocate Fees to Records Management

The General Assembly could address the lack of funding available for records management by increasing recording fees and allocating all fees or a percentage of fees to a fund to be used solely for records management.

The Charge to Staff

Act 158 of the 2003 Adjourned Session (2004) of the General Assembly included a section that read as follows:

> Sec. 5. LEGISLATIVE COUNCIL STUDY
>
> The Legislative Council shall study the public records law of the state of Vermont, the justification for state record requirements, privacy concerns regarding the dissemination of public records containing personal information, and the use of public records and shall recommend to the house and senate committees on local government and government operations potential approaches that the state could adopt to conform the public records law of the state with technological advances and associated privacy concerns.

Staff views the goal of the study, generally, as the production of potential approaches "to conform the public records law of the state with technological advances and associated privacy concerns." In furtherance of this goal, Staff reviewed laws passed by other entities and interviewed interested parties who were knowledgeable about the public records law of Vermont and who proposed issues that Staff should address in the study.

Part I of the report provides an overview of the facts and legislation that required this study. Part II reviews public record requirements under state statute and case law. Part III evaluates the archival and vital records management program in the state. Part IV analyzes whether a right to privacy in personal information exists under state or federal law. Part V examines various issues surrounding the public records management of electronic records, including computer databases, e-mail, and evolving computer technology. Part VI reviews public records management and form creation in Vermont and other states. The report also includes two appendices addressing related public records requirements. Appendix A discusses the issue of posting court records to the Internet and how the issue is addressed by Vermont courts. Appendix B summarizes pending federal legislation, federal statutes, and case law that impact state records management.

Part I. Overview

The American system of government is based on democracy and the concomitant right that all government proceedings shall be open to the public.[1] A necessary function of government is the creation of records to move its various functions and business processes forward.[2] Thus, democracy and the open government it fosters require that records be available to the public so that the public may account for the legal, managerial, or constitutional conduct of government.[3]

Public records serve multiple purposes in ensuring the accountability of government.[4] They document the ownership of state property. They support legislative intent. Public records measure the economic and social health of the state. They evaluate the impact of state programs. They also allow a citizen to document or discover actions taken in his or her name. Public records are a valuable, integral element of an efficient and accountable government.

Failure to maintain accountability subjects government and the society that relies on it to certain risks. Traditional risks of improper public recordkeeping include: failure to locate evidence that government satisfied a legislative mandate; loss of proof of ownership; or inability to find the history of past decisionmaking.[5] Thus, an organized and efficient public records system is an important and necessary tool for a well-run and accountable government. However, public records often contain information that is personal to an individual,[6] and in this age of digital technology, it takes little effort to make such personal information available to anyone with a computer and Internet access.

Before the invention and pervasive use of the Internet, public records were readily available, but they languished in what the U.S. Supreme Court termed "practical obscurity" in the file cabinets and basements of courthouses, town offices, and government agencies.[7] Finding a desired document or record stored in the traditional method could take hours or even days. In contrast, public records stored digitally can be searched in seconds, and the results can be copied electronically, e-mailed to others, posted to the Internet, or compiled by private companies into databases that anyone may search for a nominal fee.[8] In addition, many federal, state, and local government entities currently post public records directly to the Internet. The Internet itself is a computer database that accesses a seemingly continuous stream of information. Anyone with a

---

[1] *See* Will T. DeVries, *Protecting Privacy in the Digital Age*, 18 Berk. Tech. L.J. 283, 300-301 (2003).
[2] Memorandum from Gregory Sanford, State Archivist, to Ben Huffman, Legislative Council, on the Draft Public Records Study of 1995 (Feb. 6, 1995); *see also* DeVries, *supra* note 1, at 301.
[3] *Id.*
[4] As used in this report "accountability" means the ability to provide an explanation or justification, and accept responsibility, for events or transactions and for actions in relation to these events or transactions. With respect to government, accountability relates to the expenditure of money, exercise of power, and performance of duties. Accountability provides evidence that government carried out its responsibilities and that its decisions, actions, and transactions were consistent with and supportive of legislation, regulation, policy, procedure, and best practices.
[5] *See id.*, *citing* David Bearman, Electronic Evidence, Strategies for Managing Records in Contemporary Organizations.
[6] DeVries, *supra* note 1, at 301, discussing examples of personal public records, such as birth certificates, school loans, driving records, divorce proceedings, bankruptcy filings, and collection of social security.
[7] *Id.*, *citing* U.S. Dep't of Justice v. Reporters Committee, 489 U.S. 749, 762 (1989).
[8] *Id.*

computer can access this database and, if so inspired, collect and misuse personal information contained in public records posted thereto.[9]

In Vermont, most municipalities do not store their records digitally and do not post such records to the Internet. In fact, most public records continue to be stored in the traditional paper method that ensures their "practical obscurity." Nevertheless, after recording and storing public records for decades, if not centuries, many municipalities are beginning to run out of the physical space necessary to store public records in the traditional method. The Vermont General Assembly addressed the issue of the diminishing physical space for storage of municipal public records by creating a municipal land records commission to study the significant long-term and systemic managerial issues associated with public records, including whether such records should be stored and available in an electronic format.[10]

Some Vermont municipalities already store public records electronically, and some post public records to the Internet.[11] The Town of Colchester stores records electronically, and in 2003, the city received a public records request that highlighted the potential for confrontation between the state public records law and the right to privacy. Colchester prepares and stores property tax assessment information in a computer database. A company called QueVt requested the database on a compact disc under the Public Records Act. The town refused the request in part because of personal information contained in the database, including home and property descriptions. The town claimed that the database contained personal information that could be misused if disclosed, while other argued that the town resisted disclosure because of the recording fees it would lose by disclosing one electronic copy of the database versus hundreds of paper pages. QueVT sued the town, seeking production of the database. The parties eventually agreed to a settlement, and the town produced a copy of the database on a compact disc.[12]

In response to the questions raised by the QueVT case, the 2004 session of the General Assembly passed Act 158. Act 158 requires completion of this study and for one year exempts from disclosure Social Security numbers and other governmentally assigned personal identification contained in a property tax assessment database, a municipal grand list, or a property transfer tax return.[13] Act 158 provides that until June 30, 2005, the information included within a property tax assessment database is only available in a print format.[14] In addition, the General Assembly enacted Act 155, relating to identity theft, requiring all governmental entities, except town clerks, to redact Social Security numbers from a document before posting a document in a place of general public circulation, including the Internet.

---

[9] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berk. Tech. L.J. 1085, 1107 (2002), *citing* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. Sci. & Tech. L. 288, 293 (2001).

[10] Act 122, § 78a (Adj. Sess. 2004); *see also* Act 66, § 49b (2003) (Creating a study committee to develop guidance for the maintenance of municipal land records). Municipalities have been reluctant to fund adequate, physical vault space for public records. Electronic records have been offered as an alternative to physical storage, but electronic or digital storage may be more expensive than the creation of physical space since electronic records need periodic maintenance and upgrading to new software or technologies.

[11] *See* Vision Appraisal, *Assessor's Online Database for Newport, Vermont*, *at* http://data.visionappraisal.com/newportvt/ (last visited Sept. 14, 2004).

[12] QueVT v. Town of Colchester. No. 384-7-03 (Wash. County Sup. Court Nov. 5, 2003) (stipulated order).

[13] Act 158, § 2 (Adj. Sess. 2004), codified at 1 V.S.A. § 317.

[14] Act 158, § 3 (Adj. Sees. 2004), codified at 1 V.S.A. § 3465..

Part II. Public Records Act Requirements

Public records often include extensive personal information that government uses to facilitate and fulfill its purposes. Federal law exempts from disclosure some personal information in public records. The disclosure of other information usually depends on a state records policy, which is normally set by statute in a Public Records Act. There are three types of state records policies: open, closed, and intermediate. Open records states provide access to most public records with little limitation on inspection or disclosure. Any citizen can request a record or search for a record, and the motive of the individual requesting a record is irrelevant. Closed records states limit access to broad categories of public records. Access may be denied due to the type of record or the requestor's intended use of the record. In addition, records are monitored by staff, and specific procedures control the request and refiling of records. Intermediate states provide significant access to some categories of information but severely limited access to other categories.

State public records policies are motivated by the competing interests of government accountability and protection of personal privacy. Open records states arguably place more importance on the use of public records to ensure government accountability. Closed records states generally restrict access to public records to prevent disclosure of personal information. Intermediate states attempt to balance the competing interests by placing some restrictions on access to public records in order to prevent certain disclosures of private information. This part examines the public records policy and requirements of Vermont as set forth in the Vermont Public Records Act, reviews the public records laws of other states, and discusses several legislative alternatives available to the Vermont General Assembly to address perceived inadequacies in the public records law of the state.

A. Vermont Public Records Requirements

1. Vermont Constitution and Public Records Act

Vermont is one of the 14 states generally considered an "open records" state because it allows any person to inspect any record defined as a public record regardless of the identity or motive of the person inspecting the record. Under the Vermont Constitution, all power is originally inherent in and consequently derived from the people, "therefore, all officers of government, whether legislative or executive, are their trustees and servants; and at all times, in a legal way, accountable to them."[15] In enacting the Vermont Public Records Act, the General Assembly applied the accountability required by the constitution to public records. In so doing, the General Assembly provided that it is the policy of the state to:

> provide free and open examination of records consistent with Chapter I, Article 6 of the Vermont Constitution. Officers of government are trustees and servants of the people and it is in the public interest to enable any person to review and criticize their decision even though such examination may cause inconvenience or embarrassment. *All people, however, have a right to privacy in their personal and economic pursuits, which ought to be protected unless specific information is*

[15] Vt. Const. Ch. 1, Art. 6.

> *needed to review the action of a governmental officer.* Consistent with these principles, the general assembly hereby declares that certain public records shall be made available to any person as hereinafter provided. To that end, the provisions of this subchapter shall be liberally construed with the view toward carrying out the above declaration of public policy. [16]

This policy recognizes that government accountability must be balanced against an individual right to privacy in personal and economic pursuit. However, the Public Records Act does not define the scope or application of the right to privacy. Instead, the Public Records Act focuses on accountability through a general policy of open access to public records.

Although certain state agencies are required by statute to create specific public records, Vermont generally does not mandate that state or municipal agencies generate records to ensure government accountability.[17] Nevertheless, state agencies are required to establish, maintain, and implement an active and continuing program for the management, preservation, and disposition of records in part to "provide citizens a means of monitoring government programs and measuring the performance of public officials."[18] Similarly, although town clerks are required to keep indices of certain transactions and activities,[19] they are not required to produce any public records to ensure government accountability.

The principal requirement of the Public Records Act is that any person is authorized to inspect or copy a public record or document of a public agency.[20] A "public agency" is defined broadly as "any agency, board, department, commission, branch, instrumentality, or authority of the state or any political subdivision of the state."[21] This definition envelops all state agencies and all municipal government. "Public record" is also defined broadly as "all papers, documents, machine readable materials, computer databases, or any other written or recorded matters, regardless of their physical form, that are produced or acquired in the course of agency business."[22] Under this definition, any paper document, e-mail, computer database, or other digital document produced by a state agency or municipality in the course of agency business would likely qualify as a public record subject to public inspection and review.

Exemptions to the state policy of open inspection of public records are set forth at 1 V.S.A. § 317(c). [23] One of the § 317(c) exemptions from public inspection is for records designated by law as confidential.[24] The Vermont Office of State Archives has identified at least 124 public records or public proceedings designated by statute as confidential or otherwise

---

[16] 1 V.S.A. § 315 (emphasis added).
[17] *But see*, 8 V.S.A. § 11(4) requiring BISHCA to create and maintain a record of all department employees holding loans with institutions regulated by BISHCA; *see also*, Vermont Secretary of State, Office of State Archives, *Vermont Public Records and the Right to Know: Is There a Requirement to Create Records?, at* http://vermont-archives.org/records/right-to-know/create.html (last visited Sept. 28, 2004).
[18] 3 V.S.A. § 218.
[19] 24 V.S.A. § 1161 (real estate transactions index); 24 V.S.A. § 1164 (index of attachments); 18 V.S.A. § 5012 (index of marriages and civil unions); 18 V.S.A. § 5013 (index of births).
[20] 1 V.S.A. § 316.
[21] 1 V.S.A. § 317(a).
[22] 1 V.S.A. § 317(b), as amended by Act No. 158, § 2 (2004).
[23] 1 V.S.A. § 317(c) includes 34 other exemptions in addition to the confidential records exemption.
[24] 1 V.S.A. § 317(c)(1).

exempt.[25] In theory, the 1 V.S.A. § 317(c) exemptions and the 124 designated confidential records provide individuals, corporations, associations, and other entities with protection of their right to privacy. However, the right to privacy is not specifically framed by statute. Consequently, the right to privacy remains subject to interpretation. Moreover, the Public Records Act exemptions apply only to the information requested for disclosure. In many cases, exempt information may be redacted from the requested document, but redaction requires agency staff time and expense. In addition, Public Records Act exemptions do not apply to the use or misuse of personal information in public records subject to disclosure.

2. Vermont Case Law

a. Balancing the Public Interest in Disclosure against Harm to the Individual

The Vermont Supreme Court recognizes that the Public Records Act represents and exhibits a strong policy of access to public records, [26] and the Court construes the Act "liberally in favor of disclosure" to effectuate the Act's policy.[27] The Court also construes the exemptions to this policy, as set forth in 1 V.S.A. § 317(c), strictly against the custodians of records and resolves any doubts in favor of disclosure.[28] When interpreting certain § 317(c) exemptions, however, the Court employs a balancing test to determine if the public interest in disclosure is outweighed by potential harm to an individual's privacy interest.

The Court first outlined the balancing test in *Trombley v. Bellows Falls Union High School*[29] when it reviewed a request by two schoolteachers for their school employment records. The school district refused the request and cited the 1 V.S.A. § 317(c)(7)[30] exemption from disclosure for personal documents relating to an individual, including information maintained to hire, evaluate, promote, or discipline an employee of a public agency. The Court held that the § 317(c)(7) exemption applies to the nondisclosure of all "personal documents" and not just employment records or personnel files.[31] Because the term "personal documents" was both undefined and vague, the Court, following a federal model, limited the personal documents exemption "to instances where disclosure would constitute an invasion of personal privacy."[32] In so doing, the Court noted that states employing such a standard "require a balancing of the public interest in disclosure against the harm to the individual."[33] Moreover, due to the absence of a

[25] Vermont Secretary of State, Office of Vermont State Archives, *Vermont Public Records and the Right to Know: What are Examples of Specific Exemptions, at* http://vermont-archives.org/records/right-to-know/exempt.html (last visited Aug. 18, 2004).
[26] Springfield Terminal Ry. Co. v. Agency of Transp., 174 Vt. 341, 345 (Vt. Nov. 1, 2002), *citing* Trombley v. Bellows Falls Union High School, 160 Vt. 101, 106-06 (Vt. Feb. 26, 1993).
[27] Norman v. Vermont Office of Court Adm'r, 844 A.2d 769, 770 (Vt. 2004), *citing* Herald Ass'n v. Dean, 174 Vt. 350, 355 (Vt. 2002); Trombley v. Bellows Falls Union High School, 160 Vt. 101, 106 (Vt. 1993).
[28] *Id*.
[29] 160 Vt. 101 (Vt. 1993).
[30] At the time of the Trombley decision, the exemption for personal documents was codified at 3 V.S.A. § 317(b)(7). The exemption was recodified at 3 V.S.A. § 317(c)(7) in 1995 by Act 159.
[31] *Trombley*, 160 Vt. at 108-109.
[32] *Id*. at 109. Personal privacy does not extend solely to an individual. A "person" is defined by state statute to include "any natural person, corporation, municipality, the state of Vermont or any department, agency or subdivision of the state, and any partnership, unincorporated association or other legal entity." 1 V.S.A. § 128.
[33] *Id*. at 109.

privacy standard in the statute, the Court determined an invasion of personal privacy would occur if disclosure of the personal documents would reveal "intimate details of a person's life, including any information that might subject the person to embarrassment, harassment, disgrace, or loss of employment or friends."[34]

The Court in *Trombley* did not employ the balancing test in resolution of the case, but it employed the balancing test and the standard for invasion of personal privacy in subsequent cases. Most recently, in the 2004 case of *Norman v. Vermont Office of the Court Administrator*, the Court applied *Trombley* in the review of a district court decision that employment records were exempt from disclosure under 1 V.S.A. § 317(c)(7).[35] The Court noted that the public's interest in disclosure in order to oversee "the decisions of its governmental officers must be balanced against the people's right to privacy in their personal and economic pursuits."[36] The *Norman* Court noted that such a balancing test is a fact specific determination, and because the trial court had failed to make the necessary findings to provide for review, the Court remanded the case for further findings and analysis.[37] The Court also employed or cited *Trombley* and its balancing test to analyze other asserted 1 V.S.A. § 317 exemptions from disclosure, including the exemption for student disciplinary records under 1 V.S.A. § 317(c)(11)[38] and the exemption for trade secrets under 1 V.S.A. § 317(c)(9).[39]

b. Course of Agency Business

The public disclosure and inspection requirements of the Vermont Public Records Act apply only if the relevant document or material is "produced or acquired during the course of agency business."[40] The statutes do not define what constitutes "the course of agency business." The Vermont Supreme Court addressed the issue, but in so doing, did not articulate a standard applicable across state and municipal government.

In *Herald Ass'n v. Dean*, the Court held that Governor Howard Dean's schedule was a public record. According to the Court, the governor's schedule was an "integral and essential part of the daily functioning of the governor's office" and its comprehensive design is necessary to the execution of the governor's various duties and to communicate with staff and security personnel.[41] Thus, the Court held that "given the circumstances surrounding [the schedule's] creation and the essential role the calendar plays in the day-to-day functioning of the governor's office, the calendar falls within the definition of a public record because it is produced or acquired in the course of the governor's business."[42] However, the Court did not address the circumstances of the schedule's creation beyond its essential and necessary role in the functioning of the Governor's office. Such an analysis would not encompass many documents

[34] *Id.* at 110.
[35] Norman v. Vermont Office of Court Adm'r, 844 A.2d 769, 770 (Vt. 2004), *citing* Herald Ass'n v. Dean, 174 Vt. 350, 355 (Vt. 2002); Trombley v. Bellows Falls Union High School, 160 Vt. 101, 106 (Vt. 1993).
[36] *Id.*, *citing Trombley*, 160 Vt., at 109-10.
[37] *Id*. at 773.
[38] *See, e.g.*, Caledonian-Record Publishing Co. v. Vermont State College, 833 A.2d 1273, 1277-78 (Vt. 2003).
[39] *See, e.g.*, Springfield Terminal Ry. Co. v. Agency of Transp., 174 Vt. 341, 345-349 (Vt. Nov. 1, 2002).
[40] 1 V.S.A. § 317(b).
[41] Herald Ass'n v. Dean, 174 Vt. 350, 354 (Vt. 2002).
[42] *Id*.

produced by state and municipal agencies where few documents have an essential role in day-to-day operations.

A more generally applicable standard can be found in *Doe v. Salmon*, a 1977 Vermont Supreme Court case addressing public records requests made prior to the July 1, 1976 enactment of the Vermont Public Records Act. In *Doe v. Salmon*, the Court held that records of pardons were public records subject to disclosure because the power to pardon is a state function delegated to the executive and conferred upon the governor. "It is not a personal act of the individual holding that office, but it is an official declaration by the chief executive."[43] Thus, the Court focused on: (1) whether the documents at issue related to a power delegated by statute to the state agency at issue; and (2) whether the document relates to an official act by the state or to a personal act by a state employee. Such a standard could be applied to records produced by all state and municipal agencies. However, because the Court did not interpret the Public Records Act in *Doe v . Salmon* and because it failed to subsequently rely on the case in interpreting the Public Records Act, the standard articulated in *Doe v. Salmon* has little, if any, applicability to current public records statutes.

The Office of the Secretary of State, under its advisory authority for archival records,[44] and the Public Records Advisory Board (PRAB), under its authority to provide advice and guidance concerning the disposal of public records,[45] apparently have issued a non-binding interpretation of what constitutes "the course of agency business" with regard to public records. The Secretary of State advises on its website that many e-mail messages meet the non-record definition of the PRAB.[46] The PRAB, however, does not specifically define "non-record." Instead it characterizes as "non-records" transitory public records that "do not document core functions or activities of an agency or department and do not require an official action."[47] According to the PRAB, such non-records can be destroyed as needed without further action or reference to a record retention schedule.[48] The PRAB purportedly focuses on the "transitory" or temporary nature of a record, but a determination of whether an e-mail documents core functions or activities of an agency and requires official agency action does not address the "transitory" nature of the e-mail. Instead, it addresses the purpose or intent of the agency's production or acquisition of the e-mail and, thus, provides a criterion for what constitutes "the course of agency

[43] Doe v. Salmon, 135 Vt. 443, 445 (Vt. 1977).
[44] There is created within the office of the secretary of state the division of state archives, which administers and implements an archival management program for state government. 1 V.S.A. § 117(b). This program includes the authority to provide advice, assistance, and consultation to state agencies, political subdivisions, historical agencies, libraries and other Vermont organizations on the effective management of archival records. *Id*. § 117(g)(11). The Secretary of State has utilized this authority to provide advice and overviews on all types of public and archival records, including electronic records. *See* Vermont Secretary of State, Electronic Records, *at* http://vermont-archives.org/records/electronic/elec_rec.html (last visited Nov. 29, 2004). Any advice, overview, or interpretation issued by the Secretary of State or any division thereunder is purely advisory and is not binding.
[45] The PRAB is authorized to advise the commissioner of the buildings and general services concerning the preservation and disposal of public records. 22 V.S.A. § 457. This advisory authority is non-binding and should only extend to the commissioner and not to other state or local government or the public.
[46] Vermont Secretary of State, Office of State Archives, *Electronic Records; E-Mail*, *at* http://vermont-archives.org/records/electronic/er_email.html (last visited Oct. 17, 2004).
[47] State of Vermont Department of Buildings and General Services, *Records Management Bulletin V1.0*, *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/bulletin1.htm (last visited Oct. 17, 2004).
[48] *Id*.

business." Such a determination of the purpose or intent of the agency requires review of the content of the e-mail. Thus, according to the advice and interpretations of the Secretary of State and the PRAB, a document is produced in the course of agency business if, based on a review of the content of the e-mail, it documents core functions or activities of an agency *and* requires official agency action.

3. Discovery Rules

It should be noted that the Vermont Public Records Act and any right to privacy afforded to an individual under Vermont statute or common law is of limited applicability to information subject to discovery in litigation. The Vermont Rules of Civil Procedure provide that discovery may be obtained regarding "any matter, not privileged, which is relevant to the subject matter involved in the pending action."[49] Moreover, the Vermont Supreme Court has held that the exemptions to disclosure under 1 V.S.A. § 317(c) of the Public Records Act do not create a privilege that precludes discovery.[50] The Court, however, recognized that at least one of the 124 statutory provisions conferring confidentiality on a document might create an evidentiary privilege, but in so doing allowed limited discovery of the relevant information.[51] Discovery of information does not make such information public. Information disclosed during discovery remains private and protected until filed with the court and made part of the public court record.[52]

4. Criticism of Vermont Public Records Act

Questions repeatedly arise regarding the proper interpretation of the Public Records Act. Resolution of these questions often requires the involvement of state agencies, the General Assembly, or the courts. This section describes those provisions of the Public Records Act that are subject to the most criticism or generally are considered in need of clarification.

The most common criticism of the Public Records Act is that it is outdated and in need of reorganization.[53] As discussed above, the Vermont State Archives recently attempted to compile all of the exemptions to the Public Records Act. The State Archives identified 35 specific exemptions in 1 V.S.A. § 317 and at least 124 other exemptions throughout the statutes.[54] It is important to note that the State Archives list is not comprehensive and does not include exemptions required by administrative or federal law.[55] Thus, proper public records management requires records custodians to be familiar with at least 160 state exemptions and an unknown number of exemptions scattered throughout state and federal statutes and rules.

---

[49] V.R.C.P. Rule 26(b) (1).
[50] Douglas v. Windham Superior Court, 157 Vt. 34, 38 (Vt. 1991).
[51] *See*, *e.g.* In re Danforth, 174 Vt. 231 (Vt. 2002).
[52] *See*, e.g., Herald Ass'n v. Judicial Conduct Bd., 149 Vt. 233, 240 (Vt. 1988).
[53] *See* Report of Interim Legislative Staff Study, Public Records Management in Vermont State Government 2(1995) (App. I: Report of Janice M. Wiggin).
[54] Vermont Secretary of State, Vermont State Archives, *Vermont Public Records and the Right to Know: What are Examples of Specific Exemptions*, *at* http://vermont-archives.org/records/right-to-know/exempt.html (last visited Aug. 18, 2004).
[55] *Id*.

The 1 V.S.A. § 315 statement of policy for the Public Records Act also creates confusion. Section 315 provides that all people have a right to privacy in their personal and economic pursuit. However, this right to privacy is neither defined nor explained in the statutes. Arguably, the 1 V.S.A. § 317(c) exemptions from disclosure give effect to the right to privacy provided for in the statement of policy, but the statutes lack a clear statement supporting this argument. Consequently, the right to privacy provided for in the § 315 statement of policy is subject to interpretation and can lead to arguments by privacy advocates that the right to privacy should prohibit the disclosure of personal information in a public record.

Several of the specific exemptions in 1 V.S.A. § 317(c) also need clarification. The exemption in § 317(c)(7) for "personal documents" is vague and does not address what constitutes a personal document. As a result, the Vermont Supreme Court, as discussed above, held that the exemption applies to instances where disclosure would constitute an invasion of personal privacy.[56] It is unclear whether the General Assembly intended such an interpretation, and if it did, the statutes do not include a standard for an invasion of privacy.[57] In addition, the § 317(c)(7) personal documents exemption appears to be modeled on the federal Freedom of Information Act (FOIA) exemption for "personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[58] However, the Vermont Supreme Court noted that the § 317(c)(7) exemption does not apply to all personnel documents.[59]

Similar confusion can be found in the § 317(c)(10) exemption from disclosure for lists of names compiled or obtained by an agency when disclosure would violate a person's right to privacy or produce public or private gain. The statute does not define the right to privacy or "public gain" and, thus, leaves the exemption open to interpretation. Similarly, § 317(c)(12) exempts from disclosure records concerning the formulation of public policy where disclosure would constitute a clearly unwarranted invasion of personal privacy. As already stated, a standard for the right to privacy and any invasion of it is not set forth in the statute, and the statute does not define what constitutes a record concerning the formulation of policy. The recently added § 317(c)(35) one-year exemption for Social Security numbers found in appraisal databases, the grand list, or property transfer tax returns also has inspired questions as to how such numbers should be exempted, whether redaction is sufficient, and whether appraisal databases, grand lists, or property transfer tax returns should be exempt entirely.

In addition to questions regarding the exemptions in 1 V.S.A. § 317(c), clarification is needed in other sections of the Public Records Act, including the 1 V.S.A. § 316 provisions allowing a public agency to recover costs of document production. Section 316 provides that an agency can charge for the "actual cost" of providing a copy of a public record or charge for the costs associated with mailing or transmitting the record by fax or other electronic means. Section 316(d) provides that the Secretary of State shall establish the actual cost of providing a

[56] Trombley v. Bellows Falls Union High School, 160 Vt. 101, 109 (Vt. 1993).
[57] *See* discussion of right to privacy in Part III.
[58] 5 U.S.C. § 552(b)(6). Many states have a public records exemption modeled on the FOIA § 552(b)(6) exemption. *See, e.g.*, Cal. Gov't Code § 9075(c) (exemption from disclosure for "personnel, medical, or similar files the disclosure of which would constitute an unwarranted invasion of personal privacy").
[59] Trombley v. Bellows Falls Union High School, 160 Vt. 101, 110 (Vt. 1993).

copy of a public records and, in so doing, only shall consider the costs of the paper or electronic media onto which the paper is copied, a prorated amount for maintenance and replacement of the machine of equipment used to copy the records, and any utility charges directly associated with copying a record. However, the statute does not clarify what a utility charge is and how closely it must be associated to copying of the record. Similarly, 1 V.S.A. § 316(c) provides that an agency may charge and collect the cost of staff time associated with complying with a public records request if the time directly involved in the complying with the request exceeds 30 minutes. Questions have been raised regarding what constitutes complying with the request. The statutory limitations on actual cost focus on the expense of the actual duplication or postage of the record by copier or other means, and the Vermont Supreme Court in *Herald Association v. Dean* held that an agency may charge and collect for staff time spent redacting exempt information.[60] Thus, "staff time" at least includes time spent posting, copying, and redacting information, and likely includes additional staff actions. In fact, many public records custodians argue that compliance with a request includes taking the request, processing the request, retrieving the requested record, copying the record, and transmitting the record.

As a matter of public policy, reasonable "staff time" costs provisions serve an important purpose in helping to defray the very substantial cost of complying with Public Records Act requests. Such requests have become increasingly time-consuming and, thus, are a drain on state agency resources. It is not uncommon for state agencies to receive requests for massive amounts of public records or to receive multiple requests from the same individual. The task of gathering, reviewing, and when appropriate, redacting information in documents is time intensive and costly. The staff time cost provision serves as a reasonable counterweight to the ease with which a massive public records request can be made. The staff time provision is an essential part of the Public Records Act and could be expanded to clearly provide for reimbursement of additional staff tasks.

[60] Herald Ass'n, Inc. v. Dean, 174 Vt. 350, 359 (2002).

B. Public Records Requirements in Other States

1. State Personal Privacy Exemptions to Public Records Disclosure

The majority of states has a public records act that is modeled after the federal Freedom of Information Act.[61] Most state public records acts include designated exemptions from disclosure that are intended to protect the confidentiality or safety of law enforcement officers, public officials and employees, and certain categories of individuals, such as students or medical patients.[62] Some state public records acts include an exemption from disclosure for information that would violate an individual's personal privacy. The state of Michigan exempts from disclosure public records where disclosure "of the information would constitute a clearly unwarranted invasion of an individual's privacy."[63] Similarly, the District of Columbia exempts from disclosure "information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy."[64] Other examples of state privacy standards are discussed in Part IV of this report.

2. Fair Information Practices Acts

In addition to open records laws, many states have additional records management requirements commonly referred to as a Fair Information Practices Act. A Fair Information Practices Act serves to enhance government accountability while protecting an individual's privacy.[65] Generally, a Fair Information Practices Act requires government agencies to: (1) make government records available to the public; (2) conform to certain information management policies; (3) limit the dissemination of personal records and data regarding an individual; and (4) allow individuals to review government records regarding the individual.[66]

The Massachusetts Fair Information Practices Act requires every state and local agency that collects, uses, maintains, or disseminates information that concerns and readily identifies an individual to conform to several requirements.[67] At the request of an individual, an agency must notify the individual whether the agency maintains any records that concern and readily identify the individual.[68] If the agency notifies the individual that it does maintain personal records regarding the individual, the agency must make those records available to the individual for review.[69] The agency also must establish procedures to allow an individual to correct a personal

[61] Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 Minn. L. Rev. 1137, 1164 (2002).
[62] *See* Rita Thaemert, National Conference of State Legislators, State Public Records Privacy, vol. 8, No. 3 (2000), *at* http://www.ncsl.org/legis/LBRIEFS/legis830.htm (last visited Aug. 20, 2004).
[63] Mich. Comp. Laws § 15.243(1)(a).
[64] D.C. Code Ann. § 2-534(a)(2).
[65] *See, e.g.*, National Conference of Commissioners on Uniform State Laws, Uniform Information Practices Code § 1-102 (1980); Federal Trade Commission, *Fair Information Practice Principles*, *at* http://www.ftc.gov/reports/privacy3/fairinfor.htm (last visited Sept. 22, 2004).
[66] *See, id*.; *see, e.g.*, Massachusetts Gen. Laws, tit. X, chapter 66A (Fair Information Practices); *see also*, Robert Ellis Smith, Privacy Journal: Compilation of State and Federal Privacy Laws 29-32 (2002).
[67] Mass. Gen. Laws. Tit. X, Ch. 66A §§ 1, 2.
[68] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(i).
[69] *Id*.

record or contest the accuracy, completeness, or dissemination of the personal data.[70] In addition, the state or local agency must follow certain information management practices, such as designating a responsible person to manage personal information and comply with state law;[71] prohibiting unauthorized access to personal information;[72] and taking reasonable precautions to prevent damage to personal records by fire, flood, natural disaster, or other physical threat.[73] Moreover, and possibly most importantly, the agency must not collect more personal data than are reasonably necessary for performance of the agency's statutory functions.[74]

Several other states, including Alaska, California, Hawaii, Indiana, Kentucky, New York, Ohio, Utah, and Wisconsin, allow an individual to review the contents of any records created or maintained by a state or local agency regarding the individual, and most of these states allow the individual to contest the contents of the record.[75] Other states restrict dissemination of designated confidential or personal records,[76] restrict dissemination of certain types of information,[77] or penalize a state agency or employee for wrongful dissemination of personal information.[78] Virginia requires its state and local subdivisions to adhere to certain principles regarding information practices, including a ban on the collection of secret, inaccurate, or inappropriate personal information.[79]

Minnesota has taken an innovative and complex approach to public records and privacy in its fair information practices act, known as the Minnesota Data Practices Act.[80] The Act attempts to balance privacy interests and government accountability by creating several categories of information that are each subject to specific disclosure requirements or privacy protections. For example, the Data Practices Act categorizes information as government data, data on individuals, data not on individuals, public data, non-public data, confidential data, and private data.[81] An individual can request and review confidential or private data when the individual is the subject of that data.[82] Otherwise, confidential or private data is not considered

---

[70] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(j).
[71] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(a).
[72] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(c).
[73] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(d).
[74] Mass. Gen. Laws. Tit. X, Ch. 66A, § 2(*l*); *see also* Connecticut Personal Data, Conn. Gen. Stat. §§ 4-191 to 4-196. The Connecticut Personal Data statutes are substantially similar to the Fair Information Practices in Massachusetts. As with Massachusetts, Connecticut state and local agencies shall only maintain that information about a person which is relevant and necessary to accomplish the lawful purposes of the agency.
[75] *See*, Alaska Stat. § 44.99.300; Cal. Civil Code §§ 1798-1798.78; Haw. Rev. Stat. § 92F-1; Ind. Code §§ 4-1-6-1 to 4-1-6-9; Ky. Rev. Stat. Ann. § 61.884; N.Y. Pub. Off. Law §§ 93, 94; Ohio Rev. Code § 1347.08; Utah Code Ann. §§ 63-2-201, -202; Wisc. Stat. Ann. §§ 19.365.
[76] *See*, *e.g.*, Colo. Rev. Stat. § 24-72-204(3) (denying public access to mental, medical, psychological, personnel, and other similar personal files).
[77] *See*, *e.g.*, N.J. Rev. Stat. § 39:2-3.3 (Prohibiting the release of personal information connected with a motor vehicle record unless provided for by law).
[78] *See*, *e.g.*, Miss. Code. Ann. § 25-53-59 (Intentional or willful release of confidential information by a state information officer is a misdemeanor subject to a fine of not more than $1,000 or imprisonment of not more than one year.).
[79] Va. Code § 2.2-3800A.
[80] Minn. Stat. ch. 13.
[81] Minn. Stat. § 13.02.
[82] Minn. Stat. § 13.04

government data subject to review by the public.[83] To complicate matters, the Minnesota Legislature reserved to itself the task of classifying each piece of information as public, private, confidential, etc.[84] The state Commissioner of Administration issues opinions regarding access to government data,[85] but the opinions can be inconsistent and the process is often expensive and time consuming.[86] Nevertheless, Minnesota continues to attempt to balance privacy and public records, and the state legislature annually amends the Data Practices Act to classify or reclassify a certain type of government information.

3. Limiting Access to or Use of Public Records

Privacy advocates and some scholars argue that states need to amend their public records policies to restrict access to or use of public records.[87] Many states are posting non-exempt public records to the Internet. Such posting to the Internet obviously facilitates public access to public records. However, Internet access to public records also facilitates access to the personal information contained within records and, consequently, increases the opportunity for misuse of such information. Similarly, open, unsupervised access to traditional paper records allows for the gathering of personal information which quickly can be misused or transferred to another via the Internet. Thus, according to scholars, the accessibility afforded by the Internet and electronic records, and not just misuse of information, threatens an individual's right to privacy in personal information.[88]

To remedy this problem, scholars believe that states should limit the records that are made publicly available or limit the use of personal information gathered from public records. In fact, most states--even those states considered open records states--already restrict access to some public records.[89] For example, Vermont--an open records state--has at least 160 exemptions to the public inspection and review requirements in the Public Records Act.[90] Some states have adopted a limited access policy. Under its Data Practices Act, discussed above, Minnesota restricts public access to broad categories of records.[91] Many states limit access to information if it will be used for commercial purposes or other uses. For example, Colorado prohibits the use of criminal justice records and records of official action for the purpose of soliciting business for pecuniary gain.[92] However, such use restrictions may violate the First Amendment of the U.S. Constitution as prohibited restriction of commercial speech. The

---

[83] Minn. Stat. § 13.03. At times there is overlap of information or tension between the need for government accountability and privacy. *See*, Margaret Westin, *The Minnesota Government Data Practices Act: A Practitioner's Guide and Observations on Access to Government Information*, 22 Wm. Mitchell L. Rev. 839, 843-44 (1996).
[84] *Id.* at 849, *citing* Doe v. State Bd. of Medical Exam'rs, 435 N.W.2d 45, 50 (Minn. 1989) ("The scope of data which can properly be made public is almost always defined by statute.").
[85] Minn. Stat. § 13.072.
[86] *See, e.g.*, Westin, *supra* note 83, at 900-901.
[87] *See, e.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1455-56 (2001).
[88] *Id.*
[89] *Id.*
[90] Vermont Secretary of State, Vermont State Archives, *Vermont Public Records and the Right to Know: What are Examples of Specific Exemptions, at* http://vermont-archives.org/records/right-to-know/exempt.html (last visited Aug. 18, 2004).
[91] Minn. Stat. §§ 13.01 to 13.04.
[92] Colo. Rev. Stat. § 24-72-305.5.

Colorado statute was found to be a permissible regulation of commercial speech,[93] but the Ninth Circuit Court of Appeals struck down a similar California statute prohibiting the release of arrestee information to people who intend to use it for commercial purposes.[94] Nevertheless, use restrictions on voter registration lists, such as Pennsylvania's ban on the use of such lists for commercial purposes, have been upheld as constitutional, and approximately 25 states have adopted such restrictions.[95]

C. Legislative Alternatives

1. Reorganize Public Records Act and Other Exemptions

To address the criticism that the Public Records Act is disorganized, the General Assembly could reorganize the records management requirements of the state. All disclosure exemptions or references to such exemptions could be listed in one statutory section. The public records inspection and disclosure requirements of 1 V.S.A. §§ 315 to 320 could be consolidated with the public records management requirements of 22 V.S.A. §§ 451 to 457. The current disorganization of the public records requirements creates confusion and can lead to diverse interpretations and applications of the Public Records Act and records management requirements. Reorganization and consolidation may help to eliminate such confusion and allow for proper records management.

Nonetheless, reorganization could be problematic. Comprehensive statutory revision would be required to reorganize the state's records management requirements. At least 124 public records inspection and review exemptions are scattered throughout the statutes, and other exemptions exist under federal and administrative law. Moreover, reorganization may not eliminate all uncertainty regarding records management. The current list of 35 exemptions in the Public Records Act is already lengthy and confusing. Adding at least 124 other exemptions to the list will not clarify the list. In addition, a comprehensive reorganization of the Public Records Act likely would require the BGS Office of Information Specialist (OIS) to make extensive changes to the current records management training materials. Because the OIS is currently overburdened and underfunded, a reorganization and subsequent reissuance of training materials would require additional staff and funding for the OIS and the state records management program.

2. Enact a Disclosure Exemption for Disclosures That Constitute an Invasion of Privacy

The General Assembly could enact a new 1 V.S.A. § 317(c) exemption to public inspection or review for documents the disclosure of which would constitute an unwarranted invasion of privacy. The exemption could be used to prevent the unwarranted disclosure of personal information in public records. As discussed above, several states include such an exemption in their public records law. However, adding an exemption would also require

[93] Lanphere & Urbaniak v. Colorado, 21 F.3d 1508 (10th Cir. 1994).
[94] United Reporting Publishing Corp v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998).
[95] Aaron Pressman, *Massive Voter Database Up for Sale*, CNN.com, *at* http://archives.cnn.com/2000/TECH/computing/11/09/aristotle.voters.db.idg/ (last visited Oct. 20, 2004).

clarification of what constitutes the right to privacy. The need for clarification of the right to privacy is discussed in Part IV of this report.

3. Adopt a Fair Information Practices Act

The General Assembly could enact a Fair Information Practices Act. A Fair Information Practices Act would supply additional privacy protection while ensuring continued availability of public records. A Fair Information Practices Act likely would not increase significantly the records management burden on state agencies. State agencies would be required to identify records containing personal information and would need to develop procedures for citizen review of such records. However, much of the burden of preventing the disclosure of personal information shifts from agencies to those individuals with concerns regarding the disclosure of private information. In addition, a Fair Information Practices Act would not require significant reorganization of the Public Records Act or records management requirements for state agencies. Fair Information Practices Acts are generally limited in length and operate in conjunction with existing records inspection and management requirements. A Fair Information Practices Act could be extremely burdensome for some state agencies, such as the Office of State Archives, which would need to review every document it receives for personal information. For example, the Archives handled 600,000 pieces of paper during the media inspection of former Governor Dean's records. Reviewing those records for personal information would have taken months.

Requiring municipalities to implement a Fair Information Practices Act may be more problematic than implementation by state agencies. Many municipal clerks do not have the funding and staff available to review records for personal information or to review citizen complaints regarding personal information contained within a public record. In addition, prohibiting a town clerk from collecting more information than is necessary would require town clerks to review the content of documents submitted as public records. Such content review could raise liability issues and generally is unpopular among town clerks.

4. Clarify What Constitutes Agency Course of Business

The General Assembly could define what constitutes "the course of agency business" under the definition of "public record" in 1 V.S.A. § 317(b). Defining the term may clarify the type of documents subject to public inspection and review. The clarification would be especially relevant with regard to e-mail, which employees often use—properly or improperly--for personal communication unrelated to agency business. A potential definition could be drawn from the Vermont Supreme Court case of *Doe v Salmon*, discussed above, under which a document produced in the course of agency business relates to a power delegated by statute to the state agency at issue and an official act by the state or a state employee. An alternative definition is the Public Records Advisory Boards definition of a "non-record," which focuses on whether a document (1) relates to the core functions or activities of an agency or department, and (2) relates to an official agency action.

5. Limit Access to Public Records

The General Assembly could restrict or rescind the state open records policy to afford more protection to personal information contained in public records. Many scholars argue that evolving electronic and digital technology render current open records laws obsolete. Moreover, with public records custodians providing electronic copies of public records or posting public records to the Internet, opportunities to misuse personal information are increasing. Limiting access to public records based on legitimate need or authorized use would help prevent unnecessary disclosure of personal information.

A policy change likely would be unpopular and some may argue that it is unconstitutional. Under Chapter I, Article 6 of the Vermont Constitution, all government officers are accountable to the people of the state, and the Public Records Act and the Open Meeting Law give effect to Article 6 and its requirement of accountability. Some may argue that limiting access to public records removes an effective tool in ensuring government accountability and, thus, violates Article 6 of the Vermont Constitution. However, Article 6 is a truism and provides no private right of action.[96] Although multiple legislative enactments give effect to Article 6, they are not subject to challenge under the article because the remedy contemplated by Article 6 is that of popular election.[97]

[96] Welch v. Seery, 138 Vt. 126, 128 (1980).
[97] *Id.*

Part III. State Archives and Vital Records

Public records management in Vermont is not limited to the public inspection and review requirements of the Public Records Act. Separate records management requirements exist for the acquisition and preservation of archival records that document the core functions and activities of state government. Additional records management requirements provide for the issuance and preservation of vital records that document the health and well-being of the citizens of the state. This section examines the Vermont archival and vital records management programs, reviews archival and vital records management requirement in other states, analyzes recent federal vital records requirements, and proposes legislative alternatives available to the General Assembly.

A. State Archives

1. Vermont

The Vermont State Archives administers and implements an archival management program that is separate from and in addition to the state Public Records Act and records management requirements. Archival management is defined as the identification and management of archival records to assure their authenticity and accessibility from creation to ultimate disposition.[98] Archives or archival records are public records that have continuing legal, administrative, or historic value.[99] The Archives also develops and establishes standards for creation, preservation, and access to archival records.[100] The State Archives can also identify archival records in state agencies and take custody of archival records.[101] In addition, the State Archives cooperates with heads of state agencies to establish and maintain a program for identification and preservation of archival records.[102] Moreover, the Vermont Secretary of State, in which the State Archives is located, has the authority to approve or disapprove of a state agency's archival records management program.[103] However, the State Archives has little enforcement authority beyond approval of a state agency archival records program.

2. Other State Approaches

Every state maintains an archival management program through either a specific state archives office or a general public records management agency.[104] Generally, the goal of these programs is to acquire and preserve the historical and government records of their respective states. The statutory requirements that enable state archives programs are generally similar to

---

[98] 3 V.S.A. § 117(a)(1).
[99] 3 V.S.A. § 117(a)(2).
[100] 3 V.S.A. § 117(g)(4).
[101] 3 V.S.A. § 117(g)(5), (6).
[102] 3 V.S.A. § 117(g)(3).
[103] 3 V.S.A. § 218(b).
[104] *See*, National Association of Government Archives and Records Administrators, *Member Websites*, *at* http://www.nagara.org/websites.html (last visited Nov. 3, 2004); *see also* Council of State Historical Records Coordinators, *Directory of State Archives and Records Programs*, *at* http://www.coshrc.org/arc/states.htm (last visited Nov. 3, 2004).

the archival management requirements in Vermont.[105] State archives programs also face the same major problems: lack of space, lack of funding, lack of sufficient training, disaster planning, and electronic records management.[106]

Many states archives offices accept, manage, and store electronic records under an active program for the acquisition and preservation of such records.[107] States without electronic archival records programs claim a lack of resources and trained staff necessary for implementation and management of the program.[108] States with electronic archival programs have similar concerns because implementing and maintaining electronic archival systems require investment in regular technology upgrades and informed and trained staff. Consequently, implementation of an electronic archival program must be made with the knowledge and commitment to continuing, long-term funding. Additional challenges of electronic records management are discussed in Part V of this report.

B. Vital Records

1. Vermont

Vital records document events such as births, deaths, and marriages.[109] Vermont statute governs the issuance and recording of vital records. Vermont uses vital records to help document the health of the state, and, correspondingly, the Vermont Department of Health (DH) regulates the issuance and recording of vital records. Vermont's vital records program and requirements are similar to the requirements of other states,[110] and most states manage vital records through their respective departments of health.[111] Vermont's vital records program differs from other states by requiring the documentation of divorces, fetal deaths, and the establishment and dissolution of civil unions and reciprocal beneficiary relationships.[112] These additional reporting requirements increase the workload of and funding needed by the DH vital records program.[113] Moreover, the Vermont vital records program is also responsible for processing court orders for, among other purposes, name changes, corrections, and foreign-born adoptions. The DH processes an average of 75-100 court orders a month, with the number steadily growing.

---

[105] *See*, *e.g.*, R.I. Gen. Laws ch. 42-8.1 (state archives).
[106] Council of State Historical Records Coordinators, Historical Records Repository Survey (1998).
[107] National Association of Government Archives and Records Administrators, Committee on Electronic Records and Information Systems, Status of the Preservation of Electronic Records by State Archives (2004), *at* http://www.nagara.org/news/ceris_report.pdf (last visited Nov. 3, 2004).
[108] *Id*.
[109] Vermont Department of Health, *Vermont Vital Records: An Overview*, *at* http://www.healthyvermonters.info/hs/vital/vitalhome.shtml#Anchor-Vermon-17189 (last visited Oct. 20, 2004).
[110] VitalRec.com, United States Vital Records Information, *United States Map*, *at* http://www.vitalrec.com/usmap.html (last visited Oct. 20, 2004).
[111] *See*, *e.g.*, Connecticut Department of Health, *Vital Records Section*, *at* http://www.dph.state.ct.us/OPPE/hpvital.htm (last visited Oct. 20, 2004). Some states manage vital records through the office of the secretary of state. *See*, *e.g.*, New Hampshire Department of State, Division of Vital Records Administration, *Vital Records*, *at* http://www.sos.nh.gov/vitalrecords/index.html.
[112] *Id.; see also* 18 V.S.A. § 5004 (divorces); 18 V.S.A. § 5008 (preservation of data); 18 V.S.A. § 5160 (civil unions); 18 V.S.A. 5222 (fetal deaths).
[113] For example, the Department of Health receives approximately 1,500 to 1,600 reports of abortions annually.

The DH prescribes the forms towns use when issuing certificates of birth, marriage, civil union, divorce, death, and fetal death.[114] Town clerks are required to receive, number, and file certificates of births, marriages, civil unions, and deaths.[115] Town clerks must also send a certified copy of the certificate to the DH.[116] The DH uses the copies sent by towns to prepare annual tables of the births, deaths, marriages, and civil unions in the state.[117] Town clerks that fail to transmit copies of certificates to the DH may be fined up to $100.00.[118] Town clerks are also required to prepare general indices to the marriage, civil union, birth, and death records recorded in the town.[119]

As an open records state, Vermont does not require a person requesting a vital record to produce proof of identity or to show a need for the vital record. Thus, any person can request and receive the vital record of another person. The Vermont General Assembly criminalized the improper use of personal identifying information in Act No. 155 of the 2004 session,[120] but Act 155 exempts town clerks from the requirement that Social Security numbers be redacted from a document before posting in a place of general public circulation, including the Internet.[121] Although clerks do not have to redact Social Security numbers, misuse of those numbers is still prohibited by Act 155. Moreover, although the Vermont DH recommends that towns use safety paper when issuing vital records, safety paper is not required. Safety paper is a unique paper with multiple antifraud and counterfeiting features that help prevent the misuse of public or vital records. Because the Vermont DH does not require safety paper, many towns do not use it because they believe it is too expensive or the recordkeeping requirements accompanying it are too time-consuming.[122]

2. Other State Approaches

The proper management of vital records is important in preventing their fraudulent use. The fraudulent use of vital records is often a key component in identity theft and other crimes.[123] For example, a vital record, such as a birth certificate, can be used fraudulently to obtain a Social Security number, a driver's license, and credit cards. A national association for vital records custodians warns that unfettered access to records in open records states, such as Vermont, facilitates fraudulent use of vital records.[124] Moreover, birth certificate fraud is hard to determine due to the use of 14,000 different types of birth certificates nationwide and the fact

[114] 18 V.S.A. § 5001.
[115] 18 V.S.A. § 5007.
[116] 10 V.S.A. § 5010; *see also* Vermont Department of Health, *Vermont Vital Records: An Overview*, *at* http://www.healthyvermonters.info/hs/vital/vitalhome.shtml#Anchor-Vermon-17189 (last visited Oct. 20, 2004).
[117] 18 V.S.A. § 5002.
[118] 10 V.S.A. § 5011.
[119] 10 V.S.A. § 5012 (marriage and civil union index); 10 V.S.A. § 5013 (birth and death index).
[120] Act No. 155 § 4 (2004).
[121] Act 155, § 3 (Adj. Sess.).
[122] Vermont Department of Health Survey of Why Town Clerks Do Not Use Engraved Paper (on file with staff).
[123] National Association for Public Health Statistics and Inspection, *NAPHSIS Standard: Limited Access to Vital Records*, *at* http://www.naphsis.org/NAPHSIS/files/ccPageContentDOCFILENAME000435705546Limited_Access_to_Records.doc (last visited Oct. 25, 2004).
[124] *Id*.

that many birth certificates are not issued on safety paper.[125] To combat identity theft, the U.S. Department of Health and Human Services (HHS) recommends that states standardize the processes and paper used to issue birth certificates.[126] HHS also recommends that states improve the security of their vital records programs by requiring people requesting birth certificates and other vital records to prove their identity in order to be eligible for vital records services.[127] Vermont has not implemented these security features largely because of the state open records policy and cost.

Only 14 states are open records states. The other 36 states require some form of identification before granting access to vital records.[128] In addition, many states use specific security features including watermarks, intaglio, engraved paper, ultraviolet ink, or security threads.[129] In addition, many states centralize the custody and issuance of vital records. For example, one centralized state agency issues birth certificates in North Dakota, a state of similar population but far greater geographic size than Vermont.[130]

3. Pending Federal Birth Certificate Standard

As discussed in Appendix B of this report, the U.S. Congress recently passed legislation requiring national standards for the issuance of birth certificates. The Intelligence Reform and Terrorism Prevention Act of 2004 directs the U.S. Secretary of Health and Human Services to establish by rule within one year of enactment minimum standards for birth certificates used by federal agencies.[131] The standards shall require certification of a birth certificate by a state, use of safety paper or other secure measure, and other features to prevent tampering or otherwise duplicating the certificate.[132] The standards shall also establish requirements for proof and verification of identity as a condition of issuance of a birth certificate, with additional security measures for the issuance of a birth certificate for a person who is not an applicant.[133] The act further requires standards for the processing of birth certificate applications to prevent fraud.[134] Within two years of establishment of the Department of Health rule, no federal agency shall accept a birth certificate for any official purpose unless it conforms to the minimum federal standards.[135]

---

[125] Department of Health and Human Services, Office of the Inspector General, Birth Certificate Fraud (2000), *at* http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf (last visited Oct. 25, 2004). Safety paper is a unique paper with multiple antifraud and counterfeiting features that help prevent the misuse of public or vital records.
[126] *Id*. at iv.
[127] *Id*.
[128] National Association for Public Health Statistics and Inspection, *NAPHSIS Standard: Limited Access to Vital Records*, *at* http://www.naphsis.org/NAPHSIS/files/ccPageContentDOCFILENAME000435705546Limited_Access_to_Records.doc (last visited Oct. 25, 2004).
[129] Department of Health and Human Services, Office of the Inspector General, Birth Certificate Fraud 25 app. B (2000), *at* http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf (last visited Oct. 25, 2004).
[130] *Id*. at 24.
[131] S.2845, Conf. Comm. Rep. § 7211, 108th Cong. (2004).
[132] *Id*.
[133] *Id*.
[134] *Id*.
[135] *Id*.

Compliance with the birth certificate standards of the Intelligence Reform and Terrorism Prevention Act will alter Vermont's open records policy. Currently, proof of identification or additional security measures are not necessary for the access to and copying of a Vermont-issued birth certificate. Vermont could ignore the access and identification requirements of the federal act, but in so doing would put the citizens of the state at risk of losing federal services because the federal act prohibits federal agencies from accepting birth certificates that do not conform to the federal requirements.

C. Legislative Alternatives

1. Implement and Fund an Electronic Archival Management Program

The General Assembly could require the Office of State Archives to implement and manage a state program for the acquisition and preservation of electronic records. With the ubiquity of computers and e-mail, many public records—especially correspondence—are created and utilized strictly in electronic form. Without an electronic records archival program, records could be lost and with them a potentially important part of Vermont history. However, implementation of an effective archival program for electronic records will require the long-term continued funding of the program with a commitment to technology and staffing upgrades.

2. Require Security Features for the Issuance and Review of Vital Records

Under the recently enacted federal Intelligence Reform and Terrorism Prevention Act discussed above and in Appendix B, Vermont will need to conform with minimum federal standards for the issuance of birth certificates. The standards will not be set until 2006, and the Intelligence Reform and Terrorism Prevention Act provides states two years from the final date of the regulations to comply. Thus, compliance with the federal standards will not be required until 2008 at the earliest. However, the Intelligence Reform and Terrorism Prevention Act requires the federal standards to include, at a minimum, the use of safety paper and proof and verification of identity as a condition of issuance of a birth certificate. The General Assembly could begin the transition to the federal standards by requiring use of safety paper or proof of identity at an earlier date. Implementing the federal requirements will transform Vermont from an open records state to a closed records state. Such a change in policy could be politically unpopular,[136] but will be necessary to maintain federal services in the state. Requiring implementation of the two minimum standards at an earlier, accelerated date might ease transition to the more detailed and potentially cumbersome final federal standards.

[136] Some may argue that the federal standards are unconstitutional under the Vermont Constitution. In this instance, however, express federal law would likely preempt the state constitution, and limiting access to vital records likely does not violate the state constitution. Chapter I, Article 6 of the Vermont constitution provides that government officers are to be accountable to the public, and the Public Records Act gives effect to this policy, but Article 6 is a truism and provides no private right of action. Moreover, vital records document the health of the state and not the functioning of government and thus have little connection to government accountability.

Part IV. The Right to Privacy in Personal Information

The U.S. Supreme Court Justice Potter Stewart wrote that the Fourth Amendment secures to the citizens of the United States personal rights, and at the very core of the Fourth Amendment is "the right of a man to retreat into his own home and there be free from unreasonable government intrusion."[137] Privacy advocates argue that this right to be free from government intrusion extends to personal information and the right of the individual to control or limit the disclosure of such information. However, others argue that in this age of rapidly developing technology, any right to informational privacy is obsolete, especially when personal information is included in public records and, therefore, subject to public inspection under state public records law.[138] This section first examines whether a right to informational privacy exists under federal and state law, with specific emphasis on privacy protection afforded by state public records law. The section then summarizes several legislative alternatives the Vermont General Assembly could enact to address the informational right to privacy.

A. Federal Right to Privacy in Personal Information

In 1977, the U.S. Supreme Court addressed whether the constitutional right to privacy established in a series of Court cases[139] extended to information regarding an individual rather than the actions or decisions of the individual. In *Whalen v. Roe*, the Court held that the privacy cases involve two different interests. "One is the individual interest in *avoiding the disclosure of personal matters*, and another is the interest in independence in making certain kinds of important decisions."[140] Although the decision in *Whalen v. Roe* did not turn on the existence or violation of an informational right to privacy,[141] the Court addressed the existence of the right by stating:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has roots in the Constitution. . . .

Thus, according to the *Whalen* Court, when a government agency collects an individual's personal information in public records, the individual continues to have a protected right in that

---

[137] Silverman v. United States, 365 U.S. 505, 511 (1961).
[138] Solove, *supra* note 61, at 1177-1179.
[139] *See*, *e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965); Eisenstadt v. Baird, 410 U.S. 113 (1973); and Roe v. Wade, 429 U.S. 589 (1977); *see also* Solove, *supra* note 61, at 1205.
[140] 429 U.S. 589, 598-99 (1977).
[141] The Court held that the New York State Controlled Substances Act and the records the state retained under that act for certain addictive medications did not constitute an invasion of any right or liberty protected by the Fourteenth Amendment. *Whalen v. Roe*, 429 U.S. at 604.

information, and the government has the corresponding duty to avoid its unwarranted or embarrassing disclosure.

Following *Whalen*, the U.S. Supreme Court, in *Nixon v. Administrator of General Services*,[142] reviewed a claim by President Richard M. Nixon that the Presidential Recordings and Materials Preservation Act and the public disclosure provision under that Act violated his right to privacy. The Court held that public officials, including the President, have a constitutional right to privacy "in matters of personal life unrelated to any acts done by them in their public capacity."[143] However, the Court found that the right to personal privacy cannot be considered in the abstract and must be weighed against the public interest in subjecting the materials to screening.[144] Applying this balancing test, the Court found that the public interest in screening President Nixon's presidential materials outweighed any personal right to privacy against disclosure.[145]

Since *Whalen* and *Nixon*, the Supreme Court has failed to revisit the right to privacy in personal information in order to define its scope and limits. Consequently, although the majority of federal courts recognizes the right,[146] it has been inconsistently applied and occasionally questioned.[147] In fact, the D.C. Circuit expressed its "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information."[148] Ultimately, the D.C. Circuit recognized the right to privacy in personal information, but held that "the individual interest in protecting the privacy of information sought by the government is significantly less important when the information is collected by the government, but not disseminated publicly."[149] Further, the D.C. Circuit noted that the unsubstantiated fear of public disclosure is insufficient to invalidate a statute requiring the collection of personal information.[150]

The Second Circuit Court of Appeals also "recognize[s] a constitutionally protected interest in the confidentiality of personal information."[151] "[T]his confidentiality interest is not absolute, however, and can be overcome by a sufficiently weighty government purpose."[152] In weighing the government purpose, the Second Circuit employs intermediate scrutiny by upholding a state regulation that requires disclosure of personal information if the regulation furthers a substantial government interest and "does not land very wide of any reasonable mark in making its classifications."[153] Many of the other federal Circuit Courts of Appeal employ a

---

[142] 433 U.S. 425 (1977).
[143] *Id*. at 457.
[144] *Id*. at 458.
[145] *Id.*
[146] *See* Solove, *supra* note 61, at 1205, n.413, *citing* In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978).
[147] Solove, *supra* note 61, at 1205, n.413.
[148] Am. Fed'n of Gov't Employees v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997).
[149] *Id*. at 793.
[150] *Id.*
[151] Statharos v. New York City Taxi & Limousine Comm'n, 198 F.3d 317, 322-23 (2d Cir. 1999).
[152] *Id*. at 323.
[153] *Id*., *citing* Eisenbud v. Suffolk County, 841 F.2d 42, 46 (2d Cir. 1988).

similar test, under which the government regulation is usually upheld.[154] Since the majority of the federal Circuit Courts of Appeal uphold the government interest in disclosure of public records that contain personal information, the constitutional right to privacy in personal information is of little consequence to those seeking to prevent or remedy the disclosure of personal information. Until the U.S. Supreme Court clarifies the scope and application of the constitutional right to privacy in personal information, the right cannot be relied upon as adequate protection from disclosure of personal information.

Although the U.S. Supreme Court has failed to revisit the constitutional right to privacy in personal information, it has recently addressed the right to privacy in personal information under the federal Freedom of Information Act (FOIA). In *United States Department of Justice v. Reporters Committee for Freedom of the Press,* the U.S. Supreme Court held that the FBI's release of criminal records--referred to as rap sheets--organized and stored in computer databases constituted an invasion of privacy under the FOIA § 552(b)(7)(C) exemption for law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[155] Reporters seeking the rap sheets argued that there was no privacy interest preventing disclosure because the rap sheets had already been disclosed to the public. The Court rejected this argument and held that "the fact that an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[156] The substantial privacy interest in a rap sheet is augmented by the compilation of the information in a computer where it can be organized and retained beyond the normal human memory.[157] In addition, the public interest in disclosure of information under FOIA is low when the requested information is sought to gather information regarding an individual rather than a public understanding of the operations and activities of government.[158] Thus, *Reporters Committee* stands for two important tenets under FOIA and, by analogy, those state public records laws based on FOIA. First, an individual retains a right to privacy in personal information under FOIA when information in a record has already been disclosed. Second, there is a strong privacy interest in the nondisclosure of compiled computerized information.

The U.S. Supreme Court returned to the right to privacy under FOIA § 552(b)(7)(C) in the recent case of *National Archives and Records Administration v. Favish* in which it held that FOIA recognizes surviving family members' right to personal privacy with respect to the disclosure of death-scene images of a close relative.[159] In so doing, the Court held that the right to privacy afforded under FOIA § 552(b)(7)(C) is not afforded solely to the individual to which the requested material pertains. Individuals whose personal data are not contained in the requested material, in this case the relatives of the deceased, also have a privacy interest.[160] Moreover, the Court found that in enacting § 552(b)(7)(C), Congress intended to permit family members a right to privacy that had been afforded them under common law and cultural traditions.

---

[154] *See* Will Thomas De Vries, Protecting Privacy in the Digital Age, 18 Berk. Tech. L.J. 283, 288 (2003).
[155] 489 U.S. 749 (1989); *see also* 5 U.S.C. 551(b)(7)(C).
[156] *Id*. at 770-771.
[157] *Id*.
[158] *Id*. at 776, 780.
[159] National Archives & Records Administration v. Favish, 124 S.Ct. 1570, 1579 (2004).
[160] *Id*. at 1579.

The *Favish* decision could stand for a broader application this statutory right to privacy goes beyond the common law and the Constitution. The decision in *Favish* was limited to the privacy rights of the family members of a deceased individual, but it could stand for a broader application. The Court in *Favish* recognized a statutory right to privacy in personal information that extends beyond the right of the individual to which the information pertains. Thus, the right to privacy afforded by FOIA is one of general application that conceivably could be asserted with regard to other documents or public records.

B. Informational Right to Privacy in Vermont

1. Right to Privacy

As discussed above, the statement of policy for the Vermont Public Records Act provides that "All people, however, have a right to privacy in their personal and economic pursuits, which ought to be protected unless specific information is needed to review the action of a governmental officer."[161] Although the Public Records Act provides numerous exemptions from public disclosure that, in theory, account for the right to privacy provided for in the statement of policy, the Public Records Act goes no further in defining the existence, scope, application, or enforcement of a right to privacy in information collected within the public records. Consequently, when an individual claims a violation of the right to privacy under the Public Records Act, it is left to the discretion and authority of state courts to recognize the right and apply it to the facts.

2. Invasion of Privacy Tort

The Vermont Supreme Court, through recognition of the tort of invasion of privacy, acknowledged a right to privacy separate from the Public Records Act and statute. In *Hodgdon v. Mt. Mansfield Co.*, the Court, citing the Restatement of Torts 2d,[162] recognized a right to privacy as the "right to be left alone."[163] In defining an invasion of the right to privacy, the Court relied on the Restatement and noted:

> [t]he Restatement of Torts 2d identifies four forms of invasion of privacy. Only one, the intrusion upon seclusion does not require publicity of a person's private interests or affairs. To state a cause of action for intrusion upon seclusion, the plaintiff must allege 'an intentional interference with [her] interest in solitude or seclusion, either as to [her] person or as to [her] private affairs or concerns, of a

[161] 1 V.S.A. § 315.

[162] The Restatement (Second) of Torts reads as follows:

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

(2) The right to privacy is invaded by:

(a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or

(b) appropriation of the other's name or likeness, as stated in § 652C; or

(c) unreasonable publicity given to the other's private life, as stated in § 652D; or

(d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.

[163] 160 Vt. 150, 162 (Vt. Nov. 6, 1992).

> kind that would be highly offensive to a reasonable [person]. Moreover, the intrusion must be substantial.[164]

The *Hodgdon* Court did not find an invasion of the right to privacy,[165] but in *Pion v. Bean*, the Court determined that false accusations made by a landowner against his neighbor constituted an invasion of privacy. [166] At the time of this report, the Court has not addressed a claim for invasion of the right to privacy involving the publication or disclosure of accurate personal information--such as that gathered from inspection and review of public records--which substantially interferes with the solitude or seclusion of another to the degree of being highly offensive.

3. Identity Theft; Protection of Personal Information

The 2004 session of the General Assembly addressed the misuse of personal information in Act No. 155, An Act Relating to Identity Theft. Among other provisions, Act 155 creates the crime of identity theft under 13 V.S.A. § 2030.[167] Under § 2030, the crime of identity theft consists of two parts. First, no person shall possess, use, or transfer personal identifying information belonging or pertaining to another person with the intent to use the information to commit a misdemeanor or a felony.[168] Second, no person shall knowingly or recklessly possess, use, or transfer personal identifying information belonging or pertaining to another person without the consent of the other person or knowingly or recklessly facilitate the use of the information by a third person to commit a misdemeanor or a felony.[169] "Personal identifying information" is defined to include such information as name, address, birth date, Social Security number, motor vehicle identification number, and telephone number.[170] A violator of the crime of identity theft faces up to three years in prison and a fine of $5,000.00 for a first offense and up to 10 years in prison and a fine of $10,000.00 for subsequent violations.[171] In addition, all governmental entities, except town clerks, are required to redact Social Security numbers from a document before posting or requiring the posting of a document in a place of general public circulation, including the Internet.[172]

---

[164] *Id*., *citing* Restatement (Second) of Torts § 652A (1977).
[165] *Id*. The alleged invasion of privacy in *Hodgdon* was a letter sent by the employer of a toothless hotel maid informing the maid that she could not return to work without wearing dentures. The single letter was not sufficient to constitute an invasion of privacy and was not "a substantial intrusion." *Id. See also* Denton v. Chittenden Bank, 163 Vt. 62, 69 (Vt. 1994) (supervisor's uninvited visit to employee's house and questioning of employee in front of the employee's guests did not constitute an invasion of privacy).
[166] 833 A.2d 1248, 1256 (Vt. 2003).
[167] 13 V.S.A. § 2030.
[168] *Id*. § 2030(a).
[169] *Id*. § 2030(b).
[170] *Id*. § 2030(c) (Personal identifying information includes "name, address, birth date, Social Security number, motor vehicle personal identification number, telephone number, financial services account number, savings account number, checking account number, credit card number, debit card number, picture, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-mail address, computer system password, mother's maiden name, or similar personal number, record, or information.").
[171] *Id.* § 2030(f).
[172] 9 V.S.A. § 2480m.

C. Other State Approaches to Privacy Law

1. Privacy Protection

Many states recognize a right to privacy either by statute or in their constitution. The constitution of Florida defines the right to privacy in relation to public records by providing that the constitutional right to privacy does not limit the public's right of access to public records.[173] Other state constitutions address the right to privacy in one of three ways: (1) the right to privacy is recognized generally with little discussion of its scope or application;[174] (2) the state recognizes the right to privacy, prohibits its infringement in the absence of a compelling state interest, and requires the state legislature to implement the right;[175] or (3) the state constitution does not address the right to privacy.[176] Under the first and third approaches, either the state legislature or the state courts can define the scope and application of the right, but under the second approach, the state legislature is expressly charged with defining the scope and application of the right to privacy.

Some state legislatures have defined what constitutes a violation of the right to privacy in relation to the disclosure of information and specifically public records. For example, Washington state statute provides that a person's right to privacy, right of privacy, privacy, or personal privacy is invaded or violated only if the disclosure of information about a person "would be (1) highly offensive to a reasonable person, and (2) is not of legitimate concern to the public."[177] However, Washington statute also states that any provision dealing with the right to privacy in certain public records does not create a right of privacy beyond those rights that are specified as express exemptions from the public's right to inspect or copy public records.[178] Thus, the exemptions from disclosure of public records in Washington effectuate the right to privacy afforded to citizens by the state's public records act.

[173] Florida Const. Art. I, § 12.
[174] *See, e.g.*, Ariz. Const. Art II, § 8 (No person shall be disturbed in his private affairs, or his home invaded without authority of law.); Wash. Const. Art I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); S.C. Const. Art. 1, § 10 (The right of the people to be secure . . . against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.).
[175] *See, e.g.*, Mont. Const. Art. II, § 10 ("[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest); Haw. Const. Art. 1, § 6 ("[t]he right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."); Alaska Const. Art. 1, § 22 (The right of the privacy is recognized and shall not be infringed. The legislature shall implement this section.).
[176] *See, e.g.* Vermont, Rhode Island, Massachusetts, New Hampshire, and Maine.
[177] Wash. Rev. Code § 42.17.255.
[178] *Id.*

2. Invasion of Privacy

State legislatures defining the right to privacy generally have adopted some form of the standard set forth in the Restatement (Second) of Torts for the tort of invasion of privacy, namely: (1) unreasonable intrusion upon seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; or (4) publicity that unreasonably places the other in a false light before the public. [179] State legislatures have defined the scope of the right further by establishing the defenses or penalties for a violation of the right to privacy. [180]

At least one legislature stepped away from the traditional standard of invasion of privacy to specifically address the potential impact of computers and electronic access on personal privacy. In Virginia, the invasion of privacy has been extended to the criminal use of computers. Under the Virginia Computer Crimes Act:

> A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.[181]

Violation of the crime of computer invasion of privacy is a misdemeanor,[182] and a person injured by a violation may seek civil damages, including loss of profits.[183] In addition, one Virginia court extended liability for a computer invasion of privacy to the employer of an individual that used a computer network to examine the personal documents of another.[184] Thus, the traditional standard of invasion of privacy is not an absolute confine, and state legislatures can redefine the standard specifically to apply to computer access to and disclosure of personal information.

---

[179] *See* note 162, *supra*; Nebraska recognizes three actions for invasion of privacy that correspond with three of the traditional actions set forth in the Restatement: highly offensive or unreasonable intrusion on a person or their seclusion; publicity that unreasonably places another person in a false light; and exploitation or appropriation of another's name or likeness for commercial purposes. Neb. Rev. Stat. §§20-202 to 20-204. California code recognizes a cause of action for misappropriation of a likeness or name. Cal. Civ. Code §§ 990, 3344. Under the Massachusetts general laws, a person shall have a right against unreasonable, substantial, or serious interference with privacy and state law recognizes a cause of action for misappropriation of a name or likeness. Mass. Gen. Laws Ann. Ch. 214, §§ 1B, 3A. An Oklahoma statute also recognizes the misappropriation cause of action. Okla. Stat. Ann. Title 21, § 839.1.

[180] *See, e.g.*, Neb. Rev. Stat. §§ 20-206 (defenses and privileges to invasion of privacy), 20-205 (intrusion on privacy not actionable); Me. Rev. Stat. Ann. tit. 17-A, § 511(1-A) (defense to video surveillance); Mass. Gen. Laws ch. 214 § 3A (defense to misappropriation). *See, also* Del. Code tit. 11 § 1335 (Certain violations of privacy are criminal acts subject to the penalties for misdemeanors and felonies.).

[181] Va. Code § 18.2-152.5(A); *see also* Raymond L. Hogge, *Computer Invasion of Privacy Under the Virginia Computer Crimes Act* (Jan. 2001), *at* http://www.virginialaborlaw.com/library/e-law/outline-vccacomputerinvasionofprivacy2001-01-24.pdf (last visited Aug. 31, 2004).

[182] Va. Code § 18.2-152.5(B).

[183] Va. Code § 18.2-152.12(A).

[184] *See*, S.R. v. Inova Healthcare Services, 49 Va. Cir. 119, 1999 WL 797192 (Va. Cir. Ct. June 1, 1999).

Where a state does not recognize a right to privacy in statute, state courts have defined the scope and application of the right. Many of the state courts that have addressed the right to privacy have also adopted the standard set forth in the Restatement (Second) of Torts § 652.[185] In addition, state courts have recognized the traditional defenses to a violation of the right privacy.[186] Some state courts recognize a common law right to collect damages for a violation of a right to privacy,[187] but other courts reject the right to recover damages under the common law[188] and only allow recovery of damages when the invasion of privacy is statutorily recognized as a cause of action.

D. Legislative Alternatives

1. Clarify Right to Privacy in Statute

Under 1 V.S.A. § 315, the Vermont Public Records Act statement of policy provides all people with a right to privacy in their personal and economic pursuit, but the existence, scope, application, and enforcement of the right to privacy are not clearly set forth in the statement of policy or the Public Records Act in general. As discussed above, the right to privacy is arguably protected through the numerous exemptions to public inspection and review of records. However, any legislative intent to effectuate the right to privacy through the exemptions is not clearly expressed in the statutes. Because legislative intent is not clearly set forth in the statutes, it falls to executive agencies and courts to interpret the Public Records Act in a piecemeal fashion to determine how and if a right to privacy exists or applies. The General Assembly could clarify the application and extent of the right to privacy policy. Such a clarification would also help resolve questions regarding the disclosure exemptions in 1 V.S.A. §317(c) that incorporate an invasion of the right to privacy as part of the standard for withholding documents.[189]

2. Codify an Action for the Invasion of Privacy

The General Assembly could create a statutory civil action for invasion of privacy and, in so doing, adopt a standard that would allow individuals to seek damages for the misuse of personal information collected from public records. The General Assembly could codify invasion of privacy as either a tort or a crime. As discussed above, other states have employed both approaches. In addition, in codifying an invasion of privacy, the General Assembly could define the penalties for and defenses to an alleged invasion of privacy. Vermont courts currently recognize the tort of invasion of privacy. Codifying the standard employed by the courts would likely meet little resistance. Criminalizing an invasion of privacy or adopting a standard substantially different from the current standard used in the courts would generate more opposition. In addition, it might be argued that the recently adopted identity theft prohibitions in

[185] *See, e.g.*, Beane v. McMullen, 291 A.2d 37, 44-46 (Md. 1972); DeAngelo v. Fortney, 515 A.2d 594, 594-596 (Pa. Super. Ct. 1986).
[186] *See, e.g.*, Lloyd v. Quorum Health Resources, 77 P.3d 993, 954 (Kan. App. 2003); Furman v. Sheppard, 744 A.2d 583, 587-88 (Md. Spec. App. 2000); Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 84 (W.Va. 1984).
[187] *See, e.g.* Givens v. Mulliken, ex rel Estate of McElwaney, 75 S.W.3d 383, 411-412 (Tenn. 2002).
[188] *See, e.g.*, Topor v. State, 671 N.Y.S.2d 584, 587-88 (N.Y. Ct. Cl. 1997).
[189] *See*, 1 V.S.A. §§ 317(c)(10) (lists of person's names the disclosure of which would violate a person's right to privacy), and (c)(12) (records concerning the formulation of policy where disclosure would constitute a clearly unwarranted invasion of personal privacy).

Act 155 of 2004 sufficiently address the misuse of personal information and that codification of an action for invasion of privacy is not necessary.

3. Enact a Computer Invasion of Privacy Statute

The General Assembly could enact a computer invasion of privacy act under which an unauthorized person is guilty of a crime if he or she uses a computer to intentionally examine any employment, salary, credit or any other financial or personal information relating to any other person. As discussed above, such activity is a crime in Virginia. Some might argue that such a standard is not necessary because of the recently enacted identity theft provisions in Act 155 of the 2004 session. However, the identity theft provisions prohibit the misuse of personal information. In Virginia, mere examination of or unauthorized access to the personal information of another via computer is considered misuse and a violation of personal privacy.

Part V. Electronic Records: Databases, E-Mail, and Evolving Technology

The rapid evolution of digital and electronic technology has outgrown the legal requirements for public records and privacy protection. Many public records requirements are incomplete as applied to electronic and digital communications or records. Similarly, digital and electronic communications or records have rendered many of the privacy protections afforded by law obsolete or inapplicable. Nevertheless, state legislatures continue to amend public records and privacy laws to address the issues and dilemmas created by technology. This section reviews the law of Vermont and other states regarding several legal issues created by the evolution of technology, including computer databases, e-mail, and records management systems. In addition, the section provides several legislative alternatives through which the Vermont General Assembly could address public records and privacy issues created by evolving technology.[190]

A. Computer Databases

Many public records are created or reproduced in an electronic or digital format, and it is often easier to store such documents in a computer database rather than the traditional paper method. In addition, federal and state agencies intentionally compile public records for a governmental purpose or to facilitate government services. The federal government and its agencies maintain over 2,000 computer databases, and many of these databases contain personal information compiled from public records. For example, in order to locate parents who fail to pay child support, the federal government operates a database of people who obtain new employment in the United States, including their Social Security numbers, addresses, and wages.[191]

State governments also maintain or create public records databases. Many states, including Vermont, maintain criminal history databases. In addition, the QueVT public records request that inspired this report involved a property tax assessment database, which many municipalities use. In fact, the Town of Newport posted its property tax assessment database to the Internet where it is accessible to the public.[192] The Newport database is very easy to use and amazingly informative, allowing review of the assessment information for any town property, including the name of the owner, the address, a picture of the property, property characteristics, and assessed property value.

The posting of the Newport database to the Internet created little controversy. Nevertheless, many people in Vermont and around the country are concerned that the disclosure of entire databases, either voluntarily, such as with Newport, or as required by a public records law, such as with the QueVT request, violates personal privacy interests and facilitates misuse of personal information. The following subsections review the current Vermont law regarding

---

[190] DeVries, *supra* note 1, at 283.
[191] Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1403 (2001), *citing* Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996).
[192] *See* Vision Appraisal, *Assessor's Online Database for Newport, Vermont, at* http://data.visionappraisal.com/newportvt/ (last visited Sept. 14, 2004).

databases and public disclosure and describe approaches other states have adopted in response to records requests for public databases.

1. Vermont

During the 2004 legislative session, the General Assembly clarified the question of database disclosure by amending the 1 V.S.A. § 317(b) definition of "public record" explicitly to include "computer databases."[193] To account for potential privacy concerns, the General Assembly imposed a one-year exemption on the disclosure of Social Security numbers or other identification numbers included in computerized assessment databases, town grand lists, or property transfer tax returns. Therefore, computer databases are subject to public disclosure, but certain personal information within assessment databases is exempt from disclosure until June 30, 2005.[194] However, the non-exempt information in assessment databases is only available in paper format until June 30, 2005.[195]

Even without specific inclusion in the definition of "public record," state and municipal government databases are public records subject to disclosure. Under the definition of "public record," all "machine readable materials or any other written or recorded matters, regardless of their physical form or characteristics" are public records subject to disclosure.[196] The information included in computer databases is a machine readable material regardless of physical form or characteristic. Thus, computer databases have been and continue to be subject to disclosure under the Public Records Act.

2. Other State Approaches

a. Disclosure of Databases

Several states possess specific statutes addressing the disclosure of computer databases. In Ohio, records contained within electronic databases must be available to the public upon request.[197] To assist state agencies, the Ohio Electronic Records Committee (ERC) issued guidelines for responding to public records requests involving databases.[198] The ERC Guidelines recommend that state and local agencies attempt to narrow requests for electronic records to allow disclosure of specific documents instead of the entire database.[199] When a request cannot

[193] Act No. 158, § 2 (2004).
[194] *Id*.
[195] Act No. 158, §4 (2004).
[196] 1 V.S.A. § 317(b).
[197] Ohio Electronic Records Committee, Subcommittee on Databases as Public Records, Databases as Public Records Guidelines (2002), *at* http://www.ohiojunction.net/erc/databases/databasesguidelines.html (last visited Sept. 15, 2004). In Ohio, government "records" include electronic records, and electronic records" are records "created, generated, sent, communicated, received, or stored by electronic means." Ohio Rev. Code §§ 149.011(G), 1306.01(G).
[198] *Id*. The Ohio Electronic Records Committee is a joint effort between the Ohio Office of State Archives and the Ohio Office of Policy and Planning; *see*, Ohio Electronic Records Committee, *About ERC, at* http://www.ohiojunction.net/erc/abouterc.html (last visited Sept. 15, 2004). Prior to inclusion of electronic records in the definition of "records," Ohio courts interpreted the law to require disclosure of databases that included public records. State ex rel. Beacon Journal Publishing Co. v. Bodiker, 134 Ohio App. 3d 415, 442 (Ohio App. Dist 1999).
[199] *Id*.

be narrowed and an entire database must be disclosed, the agency must accommodate the request and export the data in a standardized computer format. However, agencies must not disclose exempt, confidential information when disclosing databases. To avoid disclosure of confidential information, the ERC recommends that Ohio agencies design their databases and records forms to avoid the collection of exempt records or other sensitive information.[200]

In New Mexico, every person has the right to inspect any public record in the state except those specifically exempted.[201] Non-exempt information that qualifies as a public record and that is stored on a state or local government database is open to inspection under New Mexico law.[202] However, public records contained in databases are subject to unrestricted inspection only in a printed format.[203] A state agency may disclose information in a database in a computer format only if the person requesting the information agrees: (1) not to make unauthorized copies of the database; (2) not to use the database for a commercial or political purpose unless so approved by the state; (3) not to use the database for solicitation or advertisement unless authorized by law; (4) not to allow access to the database by any other person unless approved by the state; and (5) to pay royalty to the state agency that created the database.[204] Despite these restrictions, a person requesting disclosure of a database is not required to state a reason for inspecting the records,[205] but the state may require the person requesting the database to sign a sworn statement that he or she will not use the database improperly.[206] Moreover, the unauthorized disclosure of, use of, or access to a database is a misdemeanor subject to imprisonment and a fine.[207]

Although most state public records statutes do not specifically address the disclosure of government databases, disclosure is usually required under the state's definition of public records, and many states adopt an approach similar to Vermont. For example, Illinois defines "public records" as "all records, reports . . . electronic data processing records, *recorded information and all other documentary materials, regardless of physical form or characteristics*, having been prepared, or having been or being used, received, possessed or under the control of any public body."[208] Recorded information and all other documentary information, regardless of physical form or characteristics, would include computer databases and other electronic records.

---

[200] *Id*.
[201] N.M. Stat. § 14-2-1(A).
[202] *See*, New Mexico Attorney General Patricia Madrid, The Inspection of Public Records Act: A Compliance Guide for New Mexico Public Officials and Citizens (2004), *at* http://www.ago.state.nm.us/divs/civil/IPRAFourthEdition2003.pdf (last visited Sept. 15, 2004). New Mexico defines "public records" as "books, papers, maps, photographs or other documentary materials regardless of physical form or characteristics, made or received by any agency in pursuance of law or in connection with the transaction of public business" N.M. Stat. § 14-3-2(C).
[203] N.M. Stat. § 14-3-15.1(A).
[204] N.M. Stat. § 14-3-15.1(C).
[205] N.M. Stat. § 14-2-8(C).
[206] *See*, New Mexico Attorney General Patricia Madrid, The Inspection of Public Records Act: A Compliance Guide for New Mexico Public Officials and Citizens 36 (2004), *at* http://www.ago.state.nm.us/divs/civil/IPRAFourthEdition2003.pdf (last visited Sept. 15, 2004).
[207] N.M. Stat. § 14-3-15.1(G).
[208] 5 I.L.C.S. § 140/2(c) (emphasis added); *see also* University of Florida College of Journalism and Communications, Brechner Center for Freedom of Information, *Citizen Access Project*, *Computer Documents as Public Records (Public Records)*, *at* http://www.citizenaccess.org (last visited Sept. 15, 2004) (The approaches the 50 states take regarding computer documents as public records). *See also* Georgia's definition of "public records" as "all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or

b. Database Access Fees

An additional issue is the fee charged by a state or local agency meeting a public record request for a computer database or other electronic record. For traditional paper records, most states require that the public agency providing the record charge only the actual cost of making the copy and any postage delivery costs.[209] However, it is difficult to quantify the "actual cost" of saving a computer database to a disc or e-mailing an electronic document. In addition, fees received for meeting records requests are often an important source of revenue at the municipal level, and electronic records arguably eliminate this revenue. At least two states have specifically addressed the issue.

A Montana statute attempts to quantify the cost of providing public access to electronic information.[210] Public agencies may charge: (1) the actual cost of purchasing the electronic media used to transfer data (i.e., a computer disc) if media is not provided; (2) the expenses incurred as a result of mainframe or midtier processing charges; (3) expenses for providing online computer access; (4) other out-of-pocket expenses directly associated with the information request, including retrieval or production of electronic mail; and (5) the hourly rate for a state employee."[211] In addition, the Montana department of revenue may charge an additional fee to any person who requests information from a property assessment database.[212] The additional fee serves as reimbursement for a municipality's cost of developing and maintaining the database.[213]

Similarly, North Carolina authorizes a special service charge when meeting a public records request that requires "extensive use of informational technology resources."[214] A service charge also may be assessed if the request requires extensive clerical or supervisory assistance or results in a greater use of information technology resources than established by the agency for reproduction.[215] The special service charge must be reasonable and based on the actual cost of the extensive use of the informational technology resources or the labor costs of the personnel providing the services.[216]

---

similar material prepared and maintained or received in the course of the operation of a public office or agency." Ga. Code Ann. § 50-18-70(a).

[209] *See*, *e.g.* 1 V.S.A. § 316(b); N.C. Gen. Stat. § 132-6.2(b).

[210] Mont. Code. Ann. § 2-6-110.

[211] Mont. Code. Ann. § 2-6-110(2).

[212] *Id*. § 2-6-110(3).

[213] *Id*.

[214] N.C. Gen. Stat. § 132-6.2(b).

[215] *Id*.

[216] *Id*.

B. E-Mail as Public Record

E-mail and the near instantaneous communication and document transfer it provides is undeniably useful to government. Government use of e-mail, however, has inspired several questions regarding whether government e-mail is a public record and, if so, whether it qualifies for disclosure exemptions or confidentiality under state public records laws. In addition, the transitory nature of e-mail and the ability of government employees to send e-mail from government and non-government computers may make it difficult to determine if a particular e-mail qualifies for an exemption to disclosure.

Many states have addressed these and other similar questions. The majority of states concludes that e-mail is a public record subject to disclosure under open records law, but the approaches used to implement this solution differ greatly. Some states acted through legislation, other states adopted administrative policy, and still other states rely on court precedent. These three approaches, the federal law, and current Vermont law are described below.

1. Vermont

The Vermont statutes do not expressly address whether e-mail is a public record. Similarly, at the time of this writing, the Vermont Supreme Court has not addressed whether government e-mail is a public record under 1 V.S.A. § 317. Under its advisory authority over the management of archival records,[217] the Vermont Secretary of State addressed the issue and advised in a nonbinding interpretation that e-mail is a public record subject to the inspection and disclosure requirements of the Public Records Act and the state records management requirements.[218] The 1 V.S.A. § 317(b) definition of "public record" supports the Secretary of State's interpretation. "Public record" is defined to include all "papers, documents, machine readable materials, computer databases, or any other written or recorded matters, regardless of their physical form or characteristics, that are produced or acquired in the course of agency business."[219] E-mail is a machine readable material, and when produced or acquired in the course of agency business, it is a public record subject to the inspection and disclosure requirements of the Public Records Act unless exempt under 1 V.S.A. § 317(c) or other disclosure exemptions.

A key to determining whether an e-mail or any other document is a public record is whether it was produced in the course of agency business. As discussed in Part II of this report, the Public Records Act does not define or address what constitutes agency business. However, the Office of the Secretary of State and the Public Records Advisory Board (PRAB) in their respective advisory authorities over archival and public records addressed the issue with regard

[217] The office of the secretary includes the state archives, which administers an archival management program for state government. This program includes the authority to provide advice, assistance, and consultation to state agencies, political subdivisions, and other Vermont organizations on the management of archival records. The Secretary of State has utilized this authority to provide advice and overviews on all types of public and archival records, including electronic records. Any advice, overview, or interpretation issued by the Secretary of State or any division thereunder is purely advisory and is not binding. *See* 1 V.S.A. § 117.

[218] Vermont Secretary of State, Office of State Archives, *Electronic Records; E-Mail, at* http://vermont-archives.org/records/electronic/er_email.html (last visited Oct. 17, 2004).

[219] 1 V.S.A. § 317(b), as amended by Act No. 158, § 2 (2004).

to e-mail. The Secretary of State advised on its website that many e-mail messages meet the non-record definition of the PRAB.[220] The PRAB, however, did not specifically define "non-record." Instead, PRAB recommended in a records management bulletin the type of records that must be retained and stored and the type of records that could be destroyed immediately because of their specifically transitory or temporary nature.[221] According to the PRAB, a record can be destroyed immediately and, thus, is "non-record material" if it does "not document core functions or activities of an agency or department and [does] not require an official action."[222]

Although the PRAB purportedly focuses on the "transitory" or temporary nature of a record, its reference to a non-record actually addresses whether a document is produced or acquired in the course of agency business. A determination of whether an e-mail documents core functions or activities of an agency and requires official agency action addresses the purpose or intent of the agency's production or acquisition of the e-mail and, thus, provides criteria for what constitutes "the course of agency business." Such a determination of agency purpose or intent requires review of the content of the e-mail. Thus, according to the advice and interpretations of the Secretary of State and the PRAB, a document is produced in the course of agency business if, based on a review of the content of the e-mail, it documents core functions or activities of an agency *and* requires official agency action. This standard could be interpreted very narrowly because it apparently requires both documentation of core agency functions or activities *and* official agency action. Consequently, using the PRAB standard for the course of agency business, many government e-mails or other records would fall outside the definition of public records.[223] For example, the Agency of Natural Resources (ANR) may receive a complaint via e-mail from a citizen alleging that a business is polluting. Under the standard recommended by the Secretary of State and the PRAB such an e-mail is not a public record. The regulation of pollution and the receipt of complaints regarding pollution are core ANR functions, but no official agency action is required because ANR is under no obligation to act based on receipt of the e-mail. Thus, under the interpretation offered by the Secretary of State and the PRAB, such a record could be destroyed. However, such a record could be instrumental in a citizen suit action under federal environmental statute, and its destruction could be costly to the state and agency.

In addition, if government e-mail is a public record, a broad category of it may be exempt from disclosure under the Public Records Act. Under 1 V.S.A. § 317(c)(17), a record of an interdepartmental and intradepartmental communication in any political subdivision of the state is exempt from disclosure to the extent that the communication addresses other than primarily factual materials and is preliminary to a determination of policy or action or precedes a budget presentation.[224] The § 317(c)(17) exemption is a form of executive privilege or deliberative

---

[220] Vermont Secretary of State, Office of State Archives, *Electronic Records; E-Mail*, *at* http://vermont-archives.org/records/electronic/er_email.html (last visited Oct. 17, 2004).

[221] State of Vermont Department of Buildings and General Services, *Records Management Bulletin V1.0*, *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/bulletin1.htm (last visited Oct. 17, 2004). The PRAB is authorized to advise the commissioner of buildings and general services concerning the preservation and disposal of public records. 22 V.S.A. § 457. This advisory authority is nonbinding and should only extend to the commissioner and not to other state or local government or the public.

[222] *Id*.

[223] *See* discussion in Part II regarding the need to clarify what constitutes the course of agency business.

[224] 1 V.S.A. § 317(c)(17).

process privilege that has long been recognized under federal and state public records law.[225] Thus, because E-mail between or within state and municipal government agencies obviously is communication, government e-mail addressing key factual materials preliminary to policy, action, or a budget is exempt from disclosure when sent between or within a government agency or political subdivision. Theoretically, an agency could claim this exemption for a large percentage of agency e-mail.

2. Federal Law

The Federal Records Act requires federal agency heads to "preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[226] "Records" are defined as "[a]ll books, papers, maps, photographs, machine readable materials, or other documental materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency."[227] In *Armstrong v. Executive Office of the President*, the D.C. Circuit Court held that e-mail communication made or received by a U.S. agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation are federal records subject to the requirements of the Federal Records Act.[228] Moreover, the D.C. Circuit held that paper printouts of e-mails do not necessarily meet the requirements of the Federal Records Act since the paper printout could omit fundamental pieces of information in the electronic message.[229] Consequently, e-mail that qualifies as a federal record must be recorded and managed in its electronic form.[230]

3. Other State Approaches

a. State Legislatures

California statute explicitly provides that e-mail can constitute a public record. In California, "public records" are defined as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[231] A "writing" is defined as "any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile . . . ."[232] Thus, any government e-mail sent or received by a California state or local agency relating to the conduct of the public's business is a public record subject to disclosure. Similarly, Colorado includes e-mail in the definition of a "writing" that qualifies as a public record.[233] Colorado statute, however, also includes an exemption from disclosure for a

[225] *See* Killington, Ltd. V. Lash, 153 Vt. 628, 632 n.3 (citing federal cases).
[226] 44 U.S.C. § 3101.
[227] 44 U.S.C. § 3301.
[228] 1 F.3d 1274, 1282-83 (D.C. Cir. 1993).
[229] *Id.* 1283-1287 (In *Armstrong*, the text of the e-mail was provided, but not the recipients, sender, or dates.).
[230] *Id*.
[231] Cal. Gov't Code § 6252(e).
[232] Cal. Gov't Code §6252(f).
[233] Colo. Rev. Stat. § 24-72-202(6)(a)(I) defines "public records" to mean and include "all writings made, maintained, or kept by the state, any agency, institution, a nonprofit corporation incorporated pursuant to section 23-

correspondence of an elected official that has no "demonstrable connection to the exercise of functions required by law or the expenditure of public funds."[234] At least one Colorado court held that certain personal e-mail is exempt from disclosure under this exemption.[235]

In Montana, all government e-mail is deemed to be a public record regardless of whether it concerns public government business or a private communication. Montana statute provides that state citizens are entitled to inspect and copy any public writing of the state unless the record is exempt or constitutionally protected.[236] A "public writing" is defined to include electronic mail except for confidential library records, records of confidential cultural burial sites, and "records that are constitutionally protected from disclosure."[237] Therefore, almost all government e-mail in Montana is subject to public inspection.

The Tennessee legislature adopted a slightly different approach to government e-mail in contrast to California, Colorado, and Montana. Tennessee required any state agency that operates or maintains an e-mail system to adopt a written policy on the monitoring of e-mail by July 1, 2000.[238] Any policy must provide that e-mail correspondence from a government computer "may be a public record under the public records law and may be subject to inspection."[239] This approach avoids legislative action while recognizing the issue of the privacy of government e-mail. In addition, it places all Tennessee state employees on notice that their e-mail is not entirely private. However, this approach does not answer the question of whether or not government e-mail is a public record, and either the Tennessee legislature or courts will need to revisit the issue.

In addition, although most states do not specifically reference e-mail in their definition of "public records," many state public records acts can be interpreted to include e-mail.[240] For example, Georgia defines the term "public record" to include computer-based or -generated information prepared and maintained or received in the course of the operation of a public office or agency.[241] E-mail falls under such a definition.

b. State Advisory Opinions

In several states, administrative agencies, such as the office of the state attorney general or the office of secretary of state, have addressed the question of e-mail as public record by

---

5-121 (2), C.R.S., or political subdivision of the state, or that are described in section 29-1-902, C.R.S., and held by any local government-financed entity for use in the exercise of functions required or authorized by law or administrative rule or involving the receipt or expenditure of public funds." "Writings" are defined by Colo. Rev. Stat. § 24-72-202(6)(a)(I) to mean and include all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials, regardless of physical form or characteristics. 'Writings' includes digitally stored data, *including without limitation electronic mail messages*, but does not include computer software." (emphasis added).

[234] Colo. Rev. Stat. §24-72-202(6)(a).

[235] In re Bd. of County Comm'rs of the County of Arapahoe, 2002 WL 21664844 (Colo. Ct. App. July 17, 2003).

[236] Mont. Code Ann. § 2-6-102.

[237] Mont. Code Ann. § 2-6-101(b).

[238] Tenn. Code Ann. § 10-7-512.

[239] *Id*.

[240] University of Florida College of Journalism and Communications, Brechner Center for Freedom of Information, *Citizen Access Project, E-Mail (Public Records), at* http://www.citizenaccess.org (last visited Sept. 15, 2004).

[241] Ga. Code Ann. § 50-18-70(a).

issuing opinions interpreting state statute. For example, the definition of "public record" under Arkansas statute includes "electronic or computer based information," and the state attorney general interpreted the definition to include e-mail.[242] Similarly, the Massachusetts Secretary of State issued a policy stating that "all e-mail created or received by an employee of a government unit is a public record."[243] In New York, the Committee on Open Government within the New York Department of State issued an advisory opinion concluding that e-mail communications between government officials are public records.[244] In Connecticut, the state Public Records Administrator issued a public records retention guide which provides that e-mail sent or received in the conduct of public business is a public record.[245] The Maryland state attorney general issued an opinion that state agency e-mail is a public record.[246] Many other states have issued similar opinions or adopted similar policies.[247]

c. State Courts

Several state courts have addressed whether e-mail qualifies as a public record. In *State v. City of Clearwater*,[248] the Florida Supreme Court held that e-mail produced or received in the course of official agency business is a public record, but personal e-mail sent between two city employees is not a public record. Under Florida statute, a public record must be "made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."[249] According to the Florida Supreme Court, a personal e-mail is not made or received pursuant to law or ordinance and is not created or received in connection with official business.[250] The court rejected the argument that the mere placement of an e-mail on a government computer makes it a public record. The court stated that an e-mail is not a "public record" unless it is prepared in connection with government business and "intended to perpetuate, communicate, or formalize knowledge of some type."[251] Moreover, the court held that a city policy that users of city computers have no expectation of privacy is inapplicable and does not supersede the definition of public record.[252] Therefore, in Florida, the content and

---

[242] Ark. Code Ann. § 25-19-103(5)(A); *see also* Jean Maneke & Dan Curry, *Public Scrutiny of Missouri E-Mail under the Sunshine Law*, 60 J. Mo. Bar. (Apr. 2004).
[243] Office of the Massachusetts Secretary of State, Office of State Archives, *SPR Bulletin No. 1-99* (Feb. 16, 1999, revised May 21, 2003), *at* http://www.sec.state.ma.us/arc/arcrmu/rmubul/bul199.htm (last visited Aug. 23, 2004).
[244] New York Department of State, Committee on Open Government, Freedom of Information Law Advisory Opinion 12348 (Oct. 19, 2000), *at* http://www.dos.state.ny.us/coog/ftext/f12348.htm (last visited Aug. 24 2004).
[245] Connecticut Office of Public Records Administrator, A Management and Retention Guide for State and Municipal Government Agencies (June 1, 1998), *at* http://wwwcslib.org/e-mail.htm (last visited Aug. 24, 2004).
[246] Office of the Attorney General, State of Maryland, Open Meetings Act: Public Information Act—Status of Electronic Mail, 81 Op. Atty. 140 (May 22, 1996).
[247] *See, e.g.*, Council of State Historical Records Coordinators, *Information Resources on Archives and Records Administration for State and Local Government: E-Mail Policies and Management*, *at* http://www.coshrc.org/arc/states/res_emai.htm (last updated April 3, 2004).
[248] 863 So.2d 149 (Fla. Sept. 11, 2003); *see also* Penelope Thurmon Bryan, *Agency E-Mail and the Public Records Laws—Is the Fox Now Guarding the Henhouse*, 33 Stetson L. Rev. 649 (2004).
[249] A public record is "all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material regardless of the physical form, characteristics, or means for transmission, *made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency*." Fla. Stat. §119.011(1) (emphasis added).
[250] *City of Clearwater*, 863 So.2d at 153, 155.
[251] *Id*. at 154.
[252] *Id*.

intent of the e-mail message controls whether it is a public record, and any agency computer policy regarding privacy or computer usage is irrelevant.

In *Tiberino v. Spokane County*,[253] a Washington state court of appeals held that the personal e-mails of government employee are public records, but the e-mails were exempt under a specific exemption from disclosure. Washington state statute defines a "public record" as "any writing, containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[254] The court held that a county's printing and compilation of the employee's e-mails in preparation for litigation over her termination constituted a proprietary function and, therefore, a public record.[255] However, the employee's e-mails were exempt from disclosure under the exemption for personal information the disclosure of which would violate the individual's right to privacy.[256] The court held that disclosure of the e-mail violated the state standard for invasion of privacy because it would be highly offensive to the employee and served no legitimate public concern.[257] If disclosure of the e-mail had not been highly offensive or had related to a legitimate public concern, such as the use of public funds,[258] the e-mail would have been disclosed.

In *State v. Lake County Sherriff's Department*,[259] the Ohio Supreme Court held that a government employee's e-mail that contained racist slurs about another employee did not qualify as a public record. The Ohio definition of "public record" requires the record to be created or received by any public office of the state or its political subdivisions "to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office."[260] The Court held that the e-mails containing racist slurs did not serve to document the organization, functions, etc., of the government office, and thus, were not public records subject to disclosure.[261]

C. Legislative E-Mail

A subset of the question of whether government e-mail is a public record is the issue of legislative e-mail. E-mail correspondence between legislators and legislative staff or between legislators and constituents in the course of legislative business may involve confidential or personal information not intended for public disclosure. Consequently, a blanket state e-mail policy that all government e-mail sent in the course of agency business is a public record would subject legislative e-mail to public disclosure. Several states have acknowledged this problem by

[253] 13 P.3d 1104 (Wash. Ct. App. Dec. 14, 2000).
[254] Wash. Rev. Code § 42.17.020(36).
[255] *Tiberino*, 13 P.3d. at 1108.
[256] *Id*.; *see also* Wash. Rev. Code § 42.17.310.
[257] *Id*. at 1109-1110; *see also* Wash. Rev. Code § 42.17.255 (standard for invasion or violation of right to privacy).
[258] *Id*. at 1109.
[259] 693 N.E.2d 789 (Ohio 1998).
[260] Ohio Rev. Code § 149.011(G).
[261] *Lake County Sheriff's Department*, 693 N.E.2d at 793-793.

exempting legislative e-mail from disclosure.[262] A summary of these exemptions and current Vermont law follows.

1. Vermont

The Vermont Statutes do not specifically address e-mail communications by members of the General Assembly or other elected officials. As discussed in Part II, any person is authorized to inspect or copy a public record or document of a public agency, and the definition of "public agency" includes any branch of the state.[263] The General Assembly is a government branch of the state and, consequently, e-mail sent or acquired by the General Assembly in the course of legislative business is subject to disclosure unless exempt from disclosure.[264]

No blanket exemption exists for legislative e-mail, but all requests received by legislative council from members of the General Assembly for legal assistance, information, and advice and all information received in connection with research or drafting is confidential unless the party requesting or giving the information waives confidentiality.[265] Thus, any e-mail from a legislator requesting information or legal assistance or received in connection with the request would be confidential and exempt from disclosure. E-mail from a legislator to a party other than legislative council regarding legislative business would be subject to disclosure as a public record unless it fell under a specific exemption from disclosure. Arguably, the 1 V.S.A. § 317(c)(12) disclosure exemption for records concerning the formulation of policy where disclosure would constitute an unwarranted invasion of personal privacy could be claimed to prevent disclosure of personal information contained in a legislative correspondence with a constituent. However, as discussed in Part IV, the statutes do not define what constitutes an invasion of privacy. The standard is relatively high and would, as the Vermont Supreme Court held in *Trombley v. Bellows Falls Union High School*, require a balancing of the public interest in disclosure against the embarrassment, harassment, or disgrace to the legislator or constituent caused by the disclosure.[266] Such a determination would likely require the decision of a court.

[262] *See* Pam Greenberg, The Public Life of E-Mail, State Legislature Magazine (Sept. 2002), *at* http://www.ncsl.org/programs/pubs/902email.htm (last visited Oct. 15, 2004). *See also*, National Conference of State Legislatures, Electronic Communications: Are They Public Record? (Oct. 2004) (five states specifically exempt certain categories of legislative e-mail: Colorado, New Jersey, Rhode Island, Missouri, and Texas).
[263] *See* 1 V.S.A. §§ 316, 317(a).
[264] *See* 1 V.S.A. § 317(b).
[265] 2 V.S.A. § 404(c).
[266] *See* Trombley v. Bellows Falls Union High School, 160 Vt. 101, 109-110 (Vt. 1993).

2. Other State Approaches

Colorado includes e-mail messages within its definition of "public record," but exempts from disclosure both a communication from a constituent to an elected official that clearly implies by nature or content that the constituent expects the communication to be confidential and the elected official's response to such a communication.[267] Texas statute also exempts from public disclosure legislative communication from a state citizen to a legislator unless the citizen authorizes disclosure, the e-mail is of a type that the statute expressly authorizes to be disclosed, or the legislator determines that disclosure is not an unwarranted invasion of personal privacy.[268] In Florida, the records of the legislature are public, but certain designated records are exempt from inspection and copying, including portions of correspondence held by the legislative branch which, if disclosed, would reveal information otherwise exempt from disclosure by law, such as an individual's medical condition or information regarding physical or child abuse.[269] Thus, Colorado, Texas, and Florida protect the privacy interests of legislative constituents, but do not exempt all legislative e-mail from disclosure.

Rhode Island does extend protection to all legislative e-mails. Specifically, Rhode Island defines "public record" to include electronic e-mail messages made or received in the course of official agency business, but exempts from disclosure any e-mail messages "of or to elected officials with or relating to those they represent and correspondence of or to elected officials in their official capacities."[270] Therefore, all legislative e-mails and constituent correspondence are exempt from disclosure, and any personal, non-official e-mail also would be protected because it is not made or received in the course of official agency business. Similarly, the California Legislative Open Records Act exempts from public inspection and disclosure correspondence of and to individual members of the legislature and their staff and communications from private citizens to the legislature.[271] Although the exemption does not specifically reference e-mail, e-mail is a correspondence or communication. Thus, a large percentage of legislative e-mail in California is exempt from disclosure. However, disclosure exemptions do not apply if the correspondence or communication is included in an official committee file of a bill, resolution, or proposed constitutional amendment.[272] In addition, California exempts from disclosure "personnel, medical, or similar files the disclosure of which would constitute an unwarranted invasion of personal privacy."[273]

Ohio does not specifically exempt e-mail between legislators and citizens from disclosure, but does protect any communication, correspondence, or work product between a legislator and legislative staff.[274] Legislative staff must maintain a confidential relationship with

[267] Colo. Rev. Stat. §§ 24-72-202 (1.2), (6), (7).
[268] Tex. Gov't Code § 306.004; *see also* Tex Gov't Code § 306.003 ("Records of a member of the legislature or lieutenant governor that are composed entirely of memoranda or communications with residents of this state and or personal information concerning the person communicating with the member or lieutenant governor are confidential.").
[269] Fla. Stat. § 11.0431(2)(i).
[270] R.I. Stat. § 38-2-2(4).
[271] Cal. Gov't Code § 9075(h), (j).
[272] Cal. Gov't Code §§ 9075(h), (j), 9080.
[273] Cal. Gov't Code § 9075(c).
[274] Ohio Rev. Code § 101.30.

individual legislators, and any legislative documents arising out of this relationship are not a public record.[275] However, the document may become a public record if it is required to be prepared by law or if the legislator for whom the document was prepared makes it public.[276]

D. E-Mail and Open Meeting Laws

Another issue raised by government use of e-mail is whether a state open meeting applies to e-mail exchanges among members of a government body. Although this issue does not specifically address personal privacy, e-mail exchanges among members of public bodies can circumvent a state requirement that public meetings shall be open to the public and recorded. To assure government accountability and preserve citizen review of government decision-making, several states specifically addressed the issue through legislation, litigation, or agency interpretation. A summary of these approaches and current Vermont law follows.

1. Vermont

In Vermont "all meetings of a public body are declared to be open to the public at all times" except when an executive session is authorized by statute.[277] A "meeting" is defined as "a gathering of a quorum of the members of a public body for the purpose of discussing the business of the public body or for the purpose of taking action."[278] Currently, no statute, case law, or advisory opinion speaks to the issue of whether e-mail between members of a Vermont public body constitutes a public meeting subject to the state's Open Meeting Law. Any court or agency opinion on this issue likely will focus on what constitutes a gathering of a quorum of the public body.

2. Other State Approaches

a. State Legislation

Virginia, like many states, requires all meetings of public bodies to be open to the public.[279] In addition, Virginia statute provides that "no meeting shall be conducted through telephonic, video, electronic, or other communication means where the members are not physically assembled to discuss or transact public business."[280] The statute does permit public meetings to be held by telephone or video conferencing, but only if a quorum of the public body is physically assembled at one location for the purpose of conducting the meeting.[281] Thus, government bodies in Virginia cannot conduct public meetings through the exchange of e-mail.

[275] Ohio Rev. Code § 101.30(B). A legislative document includes work product, correspondences, draft requests, legislative drafts, bills, amendments, and bill summaries prepared before bill introduction. Ohio Rev. Code § 101.30.
[276] Ohio Rev. Code § 101.30(C).
[277] 1 V.S.A. § 312(a).
[278] 1 V.S.A. § 310(2).
[279] Va. Code § 2.2-3707(A).
[280] Va. Code § 2.2-3707(B).
[281] Va. Code § 2.2-3708.

b. State Case Law

In *Wood v. Battle Ground School District*,[282] a Washington state court of appeals held that under the state's open meeting law, the successive exchange of e-mails among members of a public body can constitute a "meeting" subject to the state's open meeting law, but only if a quorum of the public body exchanges e-mail and through such exchange deliberates or discusses the business of the body.[283] The court based its decision in part on the state open meeting law and its definitions of "meeting" and "action." Washington statute defines "meeting" broadly as "meetings at which action is taken."[284] "Action," also is defined broadly as "the transaction of the official business . . . by a governing body including but not limited to receipt of public testimony, deliberations, discussions, considerations, reviews, evaluations, and final actions."[285] The court noted that under these definitions, a meeting could encompass various means of communication, including serial e-mail communications not occurring in real time.[286] However, the passive receipt of e-mail does not automatically constitute a "meeting," and the open meeting law is "not implicated when members receive information about upcoming issues or communicate amongst themselves about matters unrelated to the governing body's business via e-mail."[287] The participants in the e-mail exchange must intend to transact the body's official business, and the body must take action by communicating about issues that may come before the board for a vote.[288] In such instances, the public meeting laws of the state would apply.[289]

c. State Advisory Opinions

Several state attorney generals have issued advisory opinions regarding whether the use of e-mail by a public body violates open meeting laws. The Florida state attorney general advised that e-mail communication that does not result in the exchange of comments or responses on subjects requiring action by the public body does not constitute a public meeting subject to the open meeting law.[290] Factual background information sent from one member of a

[282] 27 P.3d 1208 (Wash. Ct. App. July 27, 2001).
[283] *Id*. at 1217-1218; *see also* Stephen Schaeffer, *Sunshine in Cyberspace? Electronic Deliberation and the Reach of Open Meeting Law*, 28 St. Louis U. L.J. 755, 765-777 (2004).
[284] *Id*. at 1216, *citing* Wash. Rev. Code § 54952.2(a), (b).
[285] Wash. Rev. Code § 42.30.020(3).
[286] *Wood*, 27 P.3d at 1216.
[287] *Id*. at 1217.
[288] *Id*. The court relied on a California Supreme Court decision due to the fact that the Washington open meeting law had been modeled, in part, on the California open meeting law. The California decision involved the circulation of a letter, not an e-mail, among the members of a city council. Although the California court found that the letter did not violate the state open meeting law, it did state that the open meeting law "…cannot be avoided by subterfuge; a concerted plan to engage in collective deliberation on public business through a series of letters or telephone calls passing from one member of the governing body to the next would violate the open meeting requirements." Roberts v. City of Palmdale, 5 Cal.4th 363, 376 (Cal. June 23, 1993).
[289] *See also* Del Papa v. Board of Regents of the University and Community College System of Nevada, 114 Nev. 388 (Nev. 1998) (serial e-mail communication and deliberation on issue before board constitutes a public meeting). *But see* Claxton Enterprises v. Evans County Bd. of Com'rs, 549 S.E.2d 830 (Ga. Ct. App. 2001) (series of telephone calls does not constitute a meeting).
[290] Florida Attorney General Advisory Legal Opinion, E-Mail as a Public Record and as a Meeting, AGO 2001-20 (Mar. 20, 2001); *see also* Schaeffer, *supra* note 283, at 772-774.

public body to other members is not subject to the state open meeting law if it does not result in discussion or deliberation by the body on a decision under its jurisdiction.[291]

Similarly, the Kansas attorney general issued an advisory opinion that a serial communication, such as e-mail, from one member of a public body to another constitutes a public meeting subject to the state's open meeting law if, as required by the state definition of "public meeting,"[292] the communication involves a quorum of the members of the body and the communication discusses the business or affairs of the body.[293] Real time communication is not a necessary condition for e-mail communication to constitute a meeting.[294] The e-mail exchange allows each member of a public body to hear and comment on another member's opinions and thoughts.[295] When this reciprocal sharing of thoughts involves discussion of government business, it must be open to the public.[296]

In contrast to the Florida and Kansas advisory opinions, the Maryland office of the attorney general issued an opinion that the state open meeting law does not apply to e-mail communications among members of a public body, unless a quorum of the public body is engaged in a *simultaneous* exchange of e-mail on a matter of public business.[297] The attorney general focused on the fact that the state's open meeting law does not apply until a quorum of the body is convened. The open meetings law "does not apply to forms of interchange among members of a public body that do not amount to a convening—the assembly that characterizes the quorum."[298] The sequential exchange of e-mail is not equivalent to the simultaneous, real-time discussion at the convening of a quorum.[299] Thus, in Maryland, a quorum of the members of a public body must physically meet in one place in order to trigger the requirements of the state open meeting law.

E. Guidelines for Electronic Records Management

Under its advisory authority over the management of archival records, the Vermont Secretary of State's office has issued two electronic records management guides,[300] but the

---

[291] *Id*.

[292] K.S.A. § 75-4317a. In Kansas a meeting is defined as "any gathering, assembly, telephone call, or any other means of interactive communication by a majority of a quorum of the membership of a body or agency subject to [the open meeting act] for the purpose of discussing the business or affairs of the body or agency." *Id.*

[293] Office of the Attorney General, State of Kansas, Opinion No. 98-26, 1998 WL 190416 (Apr. 20, 1998)

[294] *Id*.; *see also* Schaeffer, *supra* note 283, at 776-777.

[295] *Id*.

[296] *Id*.

[297] Office of the Attorney General, State of Maryland, Open Meetings Act: Public Information Act--Status of Electronic Mail, 81 Op. Atty. 140 (May 22, 1996) (emphasis added); *see also* Schaeffer, *supra* note 283, at 775.

[298] *Id*.

[299] *Id*. The attorney general's opinion noted that exchange of e-mail among members of a public body after a quorum is convened would be subject to the state open meeting law because it would allow for real-time, simultaneous exchange.

[300] Vermont Secretary of State, Limiting Liability in the Digital Age: Electronic Records Guidelines for Business and Government (2003), *at* http://vermont-archives.org/records/electronic/liability.doc (last visited Oct. 17, 2004); Vermont Secretary of State, Vermont Trustworthy Information Systems (2002), *at* http://vermont-archives.org/records/electronic/er_downloads.html (last visited Oct. 17, 2004). The state archives administers the archival management program for state government. The program includes the authority to provide advice, assistance, and consultation to state agencies, political subdivisions, and other Vermont organizations on the

guides are not mandatory and only provide guidance for agency management of electronic records. In contrast, many states possess mandatory requirements for electronic records management. The Wisconsin legislature adopted an administrative rule establishing requirements and standards to ensure that electronic public records "are preserved and maintained and remain accessible" to the public.[301] In Mississippi, state statute requires all public bodies to ensure that any information technology, equipment, or software that the body uses does not hinder the right of the public to inspect and copy public records.[302] Similarly, Michigan requires all information systems used by the state to ensure continued access to public records.[303] Ohio adopted electronic records guidelines, including an e-mail policy and management and retention policies.[304]

F. Public Records and the Evolution of Technology

A key component of electronic recordkeeping is understanding the realities and limitations of electronic data and technology. "Electronic data, unlike paper data, may be incomprehensible when separated from its environment."[305] It is therefore necessary to maintain the proper software or other electronic platform in order to ensure access to the electronic data. However, as technology rapidly evolves, a public records custodian may be unable to locate the technical infrastructure and personnel needed to maintain an electronic recordkeeping system.[306] Consequently, when a public records custodian initiates an electronic recordkeeping system, the custodian must be committed to maintaining that system or a similar system in perpetuity.

To make an informed commitment to an electronic recordkeeping system, a custodian must assess the legal requirements for record retention and destruction.[307] Custodians also must assess the needs of an electronic recordkeeping system, such as the system's operating costs, and

---

management of archival records. Any advice, overview, or interpretation issued by the Secretary of State or any division thereunder is purely advisory and is not binding. *See* 1 V.S.A. § 117; *see also* note 44 *supra*.

[301] Wisconsin Administrative Rules, Electronic Records Management—Standards and Requirements Ch. ADM 12 (2000); *see also* Wisconsin Department of Administration, Electronic Records Management: Guidance on ADM 12 (Nov. 19, 2001), *at* http://enterprise.state.wi.us/home/erecords/Primer.htm (last visited Sept. 15, 2004); *see also* Indiana Commission on Public Records, *Records Management: Electronic Records*, *at* http://www.in.gov/icpr/records_management/rch_sec7.html (last visited Sept. 15, 2004); North Carolina Office of Archives and History, North Carolina Guidelines for Managing Public Records Produced by Information Technology Systems (2000), *at* http://www.ah.dcr.state.nc.us/e-records/manrecrd/manrecrd.htm (last visited Sept. 15, 2004). *See also* Council of State Historical Records Coordinators, *Information Resources on Archives and Records Administration for State and Local Government: E-mail Policies and Management*, *at* http://www.coshrc.org/arc/states/res_emai.htm (last updated April 3, 2004).

[302] Miss. Code Ann. § 25-61-10.

[303] M.C.L. § 24.402(2).

[304] Ohio Electronic Records Guidelines, *at* http://www.ohiojunction.net/erc/RMGuide/ERGuidelines.htm (last visited Sept. 16, 2003).

[305] Sedona Conferences Working Group on Electronic Document Retention and Production, *The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production*, 5 Sedona Conf. J. 151, 157 (2004).

[306] *Id*.

[307] The Sedona Conference Working Group on Best Practices for Electronic Document Retention and Production, Draft: The Sedona Guidelines: Best Practices Guidelines and Commentary for Managing Information and Records in the Electronic Age (Sept. 2004) (public comment draft), *at* http://www.thesedonaconference.org/miscFiles/RetGuide200409 (last visited Oct. 8, 2004).

must realize that a commitment to a system includes budgeting for new equipment, new software, and trained maintenance personnel or subcontractors. If a custodian is unwilling or unable to budget for such necessities, the electronic recordkeeping system will likely fail, and the custodian will likely violate the legal requirements for record retention due to the loss of existing public records or the inability to store new, electronic records. Therefore, any electronic recordkeeping system should be realistic, practical, and tailored to the circumstances of the relevant public records custodian.[308]

G. Legislative Alternatives

1. Prohibit or Limit Access to Computer Databases

The General Assembly could limit or prohibit access to computer databases. Prohibiting access to computer databases would prevent the misuse or commercial use of personal information contained within such databases, but such limitation would contradict the open records policy of the state. Alternatively, the General Assembly could limit access to databases based on the requesting party's intended use of the database. Many states—albeit closed records states—restrict access to public records based on the intent or identity of the requesting party. Such a limitation would also violate the state open records policy. The General Assembly also could extend the current temporary restriction on access to databases and permanently provide that records stored in computer databases shall only be available in print format. The current requirement that databases are available only in print format expires June 30, 2005. At least one state restricts the disclosure of database records in this manner. However, such a restriction might be considered in conflict with the state's open records policy and current law. Current statute provides that the standard format for copies of electronic records is the format in which the record is maintained. Computer databases, obviously, are not maintained in a print format.

2. Limit Personal Information Included in Public Records Computer Databases

The General Assembly also could require that state and municipal agencies only include necessary information in their computer databases. The personal information included in many databases is unnecessary to the government function which they serve. Limiting the use or storage of personal information in databases would address privacy concerns surrounding disclosure of computer databases. Several states already strongly encourage or require the use of "necessary" information. However, it might be difficult to enact legislation defining "necessary" information. Thus, the General Assembly would need to delegate oversight authority over database creation and "necessary" information to the OIS, State Archives, or other records management authority.

[308] *Id*.

3. Authorize an Additional Service Charge for Access to or Disclosure of Databases

The General Assembly could authorize an additional service charge for access to computer databases or other electronic records. Several states currently impose such fees, which attempt to account for the actual cost of database creation. Calculating an appropriate fee in legislation might be problematic and could be opposed by business interests that frequently access public records. However, the General Assembly might deem it appropriate for business interests that frequently use and profit from a service to pay for part of it.

4. Clarify Application of the Public Records Act to E-Mail

The nature of e-mail correspondence and pervasive government use of e-mail have inspired questions regarding whether e-mail is a public record subject to disclosure under the Public Records Act and, if so, whether certain e-mail is exempt from disclosure. In addressing these questions, the General Assembly has three options. First, it can do nothing. Under the current definition of "public record" and as interpreted by the Vermont Secretary of State, government e-mail sent in the course of agency business is a public record subject to inspection and review and additional records management requirements. "Public record" is defined in 1 V.S.A. § 317(b) to include "any machine readable materials or any other written or recorded matters, regardless of their physical form or characteristics." E-mail is a machine readable material. The definition of public record also requires that the e-mail be produced in the course of agency business and the Public Records Act does not clarify what constitutes agency business. If the standards employed in the court decisions in Florida, Washington, and Ohio were employed in Vermont, personal e-mail sent from government computers in Vermont likely would be exempt from disclosure. The Florida, Washington, and Ohio courts focused on the content of the e-mail to determine whether or not it fell under the state statute at issue. If a Vermont court were to address the question of government e-mail as a public record, it would likely review the content of the e-mail and the purpose it serves for agency business. Under such review, e-mail of a truly personal nature with no relation to agency business would not qualify as a public record. Such a review, however, would be conducted by a court. Thus, the no action option leaves the question of what constitutes publicly available government e-mail to the courts.

The second option available to the General Assembly is to amend the definition of "public record" to include the term "e-mail." Currently, the definition of "public records" includes "all papers, documents, machine readable materials or any other written or recorded matters." Most consider e-mail to fall within the term "machine readable materials." Including the term "e-mail" in the definition would eliminate any possible alternative interpretations inspired by current or evolving technologies. The General Assembly could clarify whether all e-mail sent from government computers or by government employees qualifies as a public record or whether only e-mail sent in the course of agency business qualifies as a public record. The General Assembly could also define what constitutes the course of agency business and add specific exemptions for certain types of e-mail, such as legislative e-mail. In amending the definition of "public record" as it relates to e-mail, the General Assembly should be aware that many state employees currently have an expectation of privacy in e-mail sent from their government computers and might view any legislative efforts subjecting government e-mail to public inspection as a violation of their right to privacy.

As a third option, the Vermont General Assembly could encourage a Vermont state agency, such as the secretary of state or OIS, to issue a rule on the use and management of e-mail. The Secretary of State currently provides electronic records management and information tools, which include guidance on e-mail management, but these tools are advisory in nature. Many states currently have a mandatory e-mail or electronic records management policy. However, any agency effort should take care not to create further confusion.[309]

5. Exempt Legislative E-Mail from Disclosure

The General Assembly could enact a disclosure exemption for legislative correspondence with constituents in order to protect the privacy interest of constituents and prevent disclosure of personal information included in such e-mail. Currently, legislative drafting requests are confidential, but not correspondence between legislators and constituents. It could be argued that such correspondence are exempt as records concerning the formulation of policy under 1 V.S.A. § 317, but it may be difficult to determine if e-mail correspondence are records concerning policy. Moreover, determining if the policy exemption applied to legislative e-mail would be a question for the courts. At least six states possess similar exemptions.[310] The exemption could be criticized as limiting the transparency and accountability of the General Assembly.

6. Clarify Application of Open Meeting Law to use of E-Mail by Public Bodies

Another issue raised by government use of e-mail is whether the state Open Meeting Law applies to e-mail exchanges among members of a government body. Currently, state law does not address this issue. The Vermont General Assembly could clarify the application of the state Open Meeting Law to e-mail communication between members of a public body. As discussed above, Vermont law defines a meeting as a "gathering of a quorum of the members of a public body for the purpose of discussing the business of the public body or for the purpose of taking action."[311] When interpreting what constitutes a public meeting under its advisory authority, the Secretary of State has focused on "the gathering" of the members of the public body. In a Quick Guide to Open Meeting Law, the Secretary of State advises that "if a majority of a board finds themselves together at a social function they must take care not to discuss the business of the board."[312] Under this rationale, a public meeting does not occur unless a quorum of a public body *physically gathers* together in one meeting place to discuss business of the body or to take action. Therefore, the public meeting law does not apply to e-mail communication between the members of a public body, because the members have not physically gathered in one place to discuss business of the body or to take action. Thus, members of a public body could circumvent

[309] Attempts to clarify the use of e-mail in other states have been of little help or have created additional confusion. For example, the Oregon Office of State Archives addresses the question of e-mail as a public record on its website by stating "most of the time e-mail is a public record. If you have any doubts, you should assume that it is a public record." Oregon Office of State Archives, *E-Mail Frequently Asked Questions*, *at* http://arcweb.sos.state.or.us/recmgmt/emailfaq.html (last visited Aug. 24, 2004).

[310] *See* Pam Greenberg, The Public Life of E-Mail, State Legislature Magazine (Sept. 2002), *at* http://www.ncsl.org/programs/pubs/902email.htm (last visited Oct. 15, 2004).

[311] 1 V.S.A. § 310(2).

[312] Vermont Secretary of State, *A Quick Guide to Open Meeting Law*, Opinions, vol. 5, p. 9 (May 2003).

the requirements of the Open Meeting Law by conducting business via e-mail. To avoid this result, the General Assembly could (1) amend the definition of a public meeting to delete the requirement of a "gathering"; (2) define what constitutes a "gathering"; or (3) provide that e-mail communication among a quorum of the members of a public body is prohibited or authorized under certain limitations. As an alternative, the General Assembly could recommend or require the Office of Attorney General or the Office of the Secretary of State to issue an advisory opinion regarding the application of the state Open Meeting Law to e-mail communication between members of a public body.

7. Require Issuance of a Mandatory Electronic Record Keeping Policy and Manual

The General Assembly could require OIS, the Secretary of State, or another entity to adopt a mandatory electronic record keeping policy and manual for state agencies. Most states currently have such a policy. In addition, most states have an electronic records management manual for use by state agencies. The Vermont Office of the Secretary of State and the OIS both issue records management manuals that specifically or partially address electronic records management, but these manuals are advisory in nature.

VI. State Records and Forms Management

The management of public records from creation of a record through its use by a government entity until its placement in a storage and retrieval system can play a vital role in the operation of government. A well-run records management program enhances the efficacy of a government agency by increasing efficiency, improving productivity, and reducing costs. A well-run records management program also protects the privacy interests of individuals by ensuring that personal information in public records is not lost or disclosed inappropriately. Improper management of records risks the loss of necessary information and increases the time and expense required to locate information or requested documents. This section reviews the current records retention and management policy in Vermont, discusses criticism of that system, and examines how other states address records and forms management.

A. Vermont Records Management

1. Vermont Records Retention and Management Policy

State and local government agencies in Vermont must manage the creation and retention of public records to ensure their availability to the public.[313] State agency heads are required by statute to establish and maintain a record management program for their agencies.[314] Each agency program for public records must be approved by the commissioner of buildings and general services (BGS).[315] For an agency records program to be approved by the commissioner, the head of each agency must meet certain statutory requirements such as establishing an inventory of all records, developing justifiable retention records for all records, and efficiently and economically processing and storing agency records.[316] An agency archival records program

---

[313] The state policy on public records management is set forth in statute:

> (a) The general assembly finds that public records are essential to the administration of state and local government. Public records contain information which allows government programs to function, provides officials with a basis for making decisions, and ensures continuity with past operations. Public records document the legal responsibilities of government, help protect the rights of citizens, and provide citizens a means of monitoring government programs and measuring the performance of public officials. Public records provide documentation for the functioning of government and for the retrospective analysis of the development of Vermont government and the impact of programs on citizens. Public records in general and archival records in particular need to be systematically managed to preserve their legal, historic, and informational value, to provide ready access to vital information, and to promote the efficient and economical operation of government. 3 V.S.A. § 218(a).

[314] 3 V.S.A. § 218(b).

[315] *Id*. Each agency program for archival records must be approved by the Secretary of State. *Id*.

[316] Each agency department head is required to:

> (1) establish and maintain an accurate inventory of all records;
> (2) develop justifiable retention periods for all records;
> (3) dispose promptly of those records authorized for destruction by the department of buildings and general services of the agency of administration;
> (4) establish and maintain accurate records indicating the identity and quantity of all records destroyed, the savings in space and equipment, and any money savings resulting from the disposal of such records;
> (5) establish and maintain other records related to management of the agency's or department's records as required by the director of public records or the state archivist;

must also be approved by the Secretary of State, but the Secretary of State has no enforcement authority beyond this approval.[317] In addition, a custodian of public records shall not destroy, give away, sell, or dispose of a record without first receiving approval from BGS.[318] BGS authorizes disposal through its record retention schedules, which set a retention period for records common to all agencies. When a record is unique to an agency, the agency is required to seek BGS approval. However, the statutes provide little enforcement authority after an agency records program is approved, and it is difficult for BGS to determine when or if a record has been disposed of without its approval. BGS may fine a person who willfully destroys, gives away, sells, or disposes of a public record without BGS approval,[319] but BGS issues few fines because of the difficulty in determining when or if a record has been improperly destroyed. The commissioner of BGS also may refuse to provide an agency with file cabinets, open shelving, or other equipment if that agency is not making sufficient effort to improve records management, but unlike individual records custodians, the agency is not subject to monetary penalty for substandard records management and need not comply with the BGS advice or order.

In addition to the statutory requirements, the BGS Office of the Information Specialist (OIS) provides records management advice and information to custodians of public records at the state agency and municipal level.[320] The aid provided includes visiting municipal records custodians, inspecting public records vaults, providing vault design standards, and interpreting the statutory record management requirements. [321] The OIS also provides training or educational materials regarding records management.[322]

The Vermont State Archives also provides guidance and establishes standards for the identification and management of archival records.[323] Similarly, the Vermont Department of Health regulates the issuance and recording of vital records, including the forms used by the towns when issuing certificates of birth, marriage, civil union, divorce, death, and fetal death.[324] However, statute requires town clerks to use the recording method specified by BGS when recording or indexing vital records.[325]

---

(6) provide for furnishing to the division of public records and state archives, such special reports regarding the records of the agency or department as the department of buildings and general services or the secretary of state may deem necessary;
(7) process, store and preserve records kept by the agency or department in an efficient and economical manner;
(8) where practicable, consolidate or eliminate existing records of the agency or department and control the creation of new records; and
(9) maintain the records of the agency or department in a manner that permits the prompt and orderly removal of records authorized for destruction. 3 V.S.A. § 218(c).

[317] 3 V.S.A. § 218(b).
[318] 22 V.S.A. § 454.
[319] 22 V.S.A. § 456.
[320] 22 V.S.A. § 453(a)(1).
[321] Vermont Department of Buildings and General Services, Office of the Information Specialist, *Our Mission, at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/index.html (last visited Sept. 28, 2004).
[322] *Id*.
[323] 3 V.S.A. § 117.
[324] 18 V.S.A. § 5001.
[325] 18 V.S.A. § 5008.

The educational publications produced by BGS and the OIS focus on how to inventory, store, and dispose of public records, rather than their creation or public inspection. The BGS publications include record retention schedules for state and municipal records[326] and a records management manual[327] that is intended to assist state agencies in the establishment and maintenance of a comprehensive records disposition program.[328] The manual is a "paperwork management technique aimed at the systematic, timely, and effective destruction or removal of obsolete or inactive records from expensive office space and the effective but economical preservation of records."[329] However, the manual is not mandatory, and state agencies inevitably develop a records management program that is specific to the agency and independent from other agencies.

The OIS provides records management training classes to state agencies generally once a year. In addition, the OIS meets individually with the records management officer of each agency for one-on-one instruction. The OIS also provides training to municipal clerks twice a year and one-on-one instruction when visiting municipal offices.

2. Criticism of the State Records Management Program

Several sources have criticized state and municipal records management in Vermont as outdated, understaffed, unorganized, and in violation of the state statutory requirements. A 1995 legislative staff study of public records management in Vermont conducted by a private records management consultant concluded that Vermont's record retention and management policy and program required revision.[330] According to the study, the current records management statutes, which have not substantially changed since 1995, reflect outdated records management principles, policies, methods, and accountabilities. Moreover, the study stated that the statutes do not accommodate the highly specialized nature and requirement of modern records and information management. The study also concluded that there is an immediate and critical need for a comprehensive, statewide records retention program which includes staff support and training. In addition, the 1995 study noted a lack of records management knowledge, training, and organization at the individual agency level. The study further noted that the reliance on individual agency management of records made records searches difficult and expensive and led to inconsistent storage methods and labeling.[331]

---

[326] Vermont Department of Buildings and General Services, Office of the Information Specialist, State of Vermont Retention Schedule for State Agencies (2002), *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/schedules/stateretention.pdf (last visited Sept. 30, 2004); *see also* State of Vermont Retention Time Table for Municipal Records (2001), *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/schedules/municipal.pdf

[327] Vermont Department of Buildings and General Services, General Services Center, Public Records Division, Records Officer Procedure Manual for All State Agencies (2002), *at* http://www.bgs.state.vt.us/gsc/pubrec/recctr/manual.pdf (last visited Sept. 28, 2004).

[328] *Id*. at 3.

[329] *Id*.

[330] Report of Interim Legislative Staff Study, Public Records Management in Vermont State Government 2(1995) (Appendix I: Report of Janice M. Wiggin, CRM, Joint Fiscal Committee Staff, "Public Records Study; Summer Fall 1994).

[331] *Id*. at app. 2, pp. 2-10 (The study noted that several records types which had historical value were being destroyed at the agency level because of a lack of knowledge of their importance or due to a lack of sufficient analysis of the record.).

Since the 1995 report, OIS has issued a public records management manual and updated state and municipal retention schedules. The manual and the retention schedules focus on the inventory, storage, and disposal of public records. The manual includes the compilation and analysis of records called for in the 1995 study. The manual, however, is not a comprehensive statewide records retention and management program that addresses the specialized nature and requirements of modern records and information management. Consequently, many of the problems that existed in 1995 exist today.

A 2000 legislative staff study of the administrative rule-making process also criticized the public records management in the state, with specific emphasis on legislative records.[332] According to the study, the state faces a crisis in that it risks the loss of legislative history gathered through the years in the form of tape recordings of committee hearings. The analog audiotape used for the recordings is deteriorating and may, over time, be permanently lost.[333] To ensure the preservation of these recordings, the analog tapes must be converted to a compact disc format. Moreover, the 2000 study called for a long-term record-keeping approach for legislative records.[334] Since 2000, the state has failed to convert the analog tapes or adopt a comprehensive legislative records policy. Consequently, legislative intent may be lost as state legislation is subject to interpretation by executive agencies and the courts without the aid of sufficient legislative history.

Much of the criticism of the state records management program from the 1995 report can be traced to three major factors: lack of staff, lack of funds, and lack of space. The OIS, which is responsible for the majority of BGS' records management responsibilities, is staffed by one person,[335] who coordinates most of the records management training provided by the state, inspects municipal records vaults, and produces or provides input on the BGS records management publications. Similarly, the State Archives is staffed by two people, and the Department of Health vital records division is staffed by five people. Moreover, staffing or budget cuts often target records management staff. For instance, the Department of Health vital records staff is funded from the state general fund and has experienced staff cuts.

The lack of records management staff is directly connected to the lack of funds available to records management in the state. All Vermont agencies are suffering budget cutbacks, but continued budget cuts for state records management programs would be difficult to absorb. For example, the vital records division of the Department of Health recently lost one full-time employee position due to budget cuts. The vital records division does produce its own revenue of approximately $150,000 a year in fees, but the money is allocated to the general fund and not specifically to vital records management. In addition, the recent federal vital records requirements and the investment they will require in technology, security, and oversight will compel serious reconsideration of the vital records budget. In fact, the cost of the federal requirements may force Vermont and many other states to make the difficult decision to not comply with the federal law.

---

[332] Legislative Council Report on the Administrative Rulemaking Process (2000).
[333] *Id*. at 13.
[334] *Id*. at 18.
[335] The OIS consists of one employee, Mark Reaves, the State Information Specialist. *Id.*

The lack of staffing and funding has a ripple effect on records management in the state. The 1995 report and other observers have noted the need for more extensive records management training. These observers believe training is needed at each level of state agency records management--from agency heads to records management officers to administrative staff that handle records. Agency heads need to be informed of the statutory record management requirements and convinced to assign adequate employee time and money to records management.[336] At the municipal level, town clerks are not required to follow any records management guidelines. Each town office has its own individual and independent method of records management and storage.[337]

Comprehensive and continued records management training could help eliminate current problems in the state records management program. However, the OIS, State Archives, and the Department of Health do not have the time or funding to provide adequate training. The OIS does provide limited records management training to state agencies, but generally in a one-on-one forum, and only when the OIS has the time to visit state agencies. Since agency records management duties are often transferred among agency administrative staff, such one-on-one training is of limited use. Moreover, OIS provides records training to town clerks twice a year, but clerks are not required to attend, and each town clerk is generally free to manage records as he or she wishes. Similarly, the vital records division of the Department of Health is supposed to provide training on the management of vital records to towns, but has been unable to do so due to staff limitations. The OIS temporarily and voluntarily provided vital records training to towns, but because of its own staffing limitations, OIS no longer provides such training.

Due to the lack of comprehensive and requisite training caused by lack of staff and funds, the records management methods used by towns range from good to bad. Bad records management can have significant repercussions on a community. For example, improperly recorded or stored land records make title searches difficult and, consequently, may make it difficult to acquire title insurance on a property.[338] Moreover, many records custodians probably are violating current records management requirements. The independence and autonomy of records custodians, the lack of records analysis, and the difficulty and expense of record keeping

---

[336] In many agencies, the task of records management officer is often deemed an administrative task that is assigned to the newest administrative employee. Consequently, there is no continuity in records management at the agency level as "new" records managers educate themselves regarding the records management requirements. The agency records management officer needs to be permanently assigned to an employee and that employee must be instructed regarding proper records retention and disposal requirements and on other important issues such as privacy and forms management. In addition, administrative staff must be instructed regarding proper filing practices and the need to consult with an agency records management officer before destruction or disposal of a record.

[337] Peter Crabtree, *Selectboard Grills Longtime Town Clerk*, Rutland Herald, Sept. 24, 2004 (quoting Mark Reaves, the state Information Specialist: "Every office has its own idiosyncratic methods.").

[338] *See, id. But see*, Brent Curtis, *Road Issue May Threaten Title Insurance Coverage*, Rutland Herald, July 13, 2004. The state Department of Banking, Insurance, Securities and Health Care Administration (BISHCA) might construe a company's failure to provide title insurance to a town as a discriminatory insurance practice. Recently, BISHCA warned the Vermont Attorneys Title Insurance Company that failure to provide title insurance in three towns planning to resurrect old roads would be a discriminatory business practice. *Id.* An argument could be made that failure to provide title insurance based on poor records management is also discriminatory. However, a title insurance company likely would argue that failure to provide insurance in a town with poor records management is based on the inability to prove effective title and not discrimination.

likely lead to the destruction or mismanagement of records that are required by statute to be available for public review and inspection. However, it is difficult to determine when violations occur because they usually become known only when requested records are destroyed or lost. Similarly, improper records management is not remedied until a violation receives public attention. Although courts can penalize the improper withholding, disclosure, or damage of public or confidential records,[339] penalties are rare and do not discourage agencies from violating record keeping requirements.[340]

Even when state agencies and municipalities properly manage public records, a lack of adequate storage space may lead to the loss or improper storage of valuable records. For example, the vital records vault at the Department of Health is at or near capacity. The Office of State Archives has the smallest archival space of any state and cannot accept many archival records. Consequently, the archives spends significant time and money on reformatting records from paper to microfilm in order to create physical shelf space. The BGS public records center is operating with one month of available capacity. Although the BGS public records center is constantly receiving records, it creates capacity through the destruction of documents scheduled for disposal. An unexpected spike in public document creation quickly could reduce available capacity. BGS also faces space limitations for the storage of legislative documents, which are retained indefinitely in a climate-controlled vault.[341] In addition, state agencies and towns are running out of satisfactory storage space for public records and are forced to improvise storage as vault space or other acceptable storage options fill up.

3. Other State Approaches

Every state regulates the management and disposal of public records.[342] In many states, record conservation and management is regulated by the Office of the State Archives within the Office of the Secretary of State.[343] For example, the State Archives Office within the Office of the Secretary of the Commonwealth of Massachusetts regulates both the management of public records and their long-term conservation. Some states have created a stand alone department or agency that regulates both the conservation and management of public records.[344] For example, the state of New Mexico created a Commission of Public Records, which has separate archives

[339] 1 V.S.A. § 320; 22 V.S.A. § 455; *see also* Vermont Office of the Secretary of State, Vermont State Archives, *Vermont Public Records and the Right-to-Know: What are the Penalties for Violating Public Records Laws*, *at* http://vermont-archives.org/records/right-to-know/penalties.html (last visited Oct. 5, 2004).
[340] No case imposing penalties is digested in the Vermont reports, and the cases cited as annotations in the Vermont Statutes Annotated only refer the authority to impose penalties, not to any actual imposition.
[341] *See*, *e.g.* Legislative Council Report on the Administrative Rulemaking Process (2000).
[342] Council of State Historical Records Coordinators, Directory of State Archives and Records Programs, at http://www.coshrc.org/arc/states.htm (last visited Sept. 29, 2004).
[343] *See*, *e.g.*, Massachusetts Secretary of the Commonwealth, *Massachusetts Archives*, *at* http://www.sec.state.ma.us/arc/arcidx.htm (last visited Oct. 1, 2004); Rhode Island Secretary of State, *State Archives and Public Records*, *at* http://www.state.ri.us/archives/ (last visited Oct. 2, 2004); Washington Secretary of State, *State Archives*, *at* http://www.secstate.wa.gov/archives/ (last visited Oct. 1, 2004).
[344] *See*, *e.g.*, Pennsylvania Historical and Museum Commission, *at* http://www.phmc.state.pa.us/overview.asp (last visited Oct. 1, 2004); New Mexico Commission of Public Records, *State Records Center and Archives*, *at* http://www.nmcpr.state.nm.us/commiss/commission_hm.htm (last visited Oct. 1, 2004); State of New Hampshire, *Division of Archives and Records Management*, *at* http://www.sos.nh.gov/archives/index.html (last visited Oct. 1, 2004*).*

and records management divisions. Still other states, such as Vermont, divide records conservation responsibilities and records management duties between two separate state agencies often within separate state departments. For example, Maryland regulates records conservation through a state archives office, but the Department of General Services has responsibility over records management.[345]

Regardless of the organizational structure maintained by a state for records management, most state records management requirements are similar to the Vermont program.[346] As with Vermont, most states require state agencies to operate a records management program in coordination with the state archives or state records management program.[347] Most state archives or state records programs are required to advise agencies on records management, and such advice generally takes the form of training and advisory publications such as a records management manual.[348] The records management manuals and publications issued by other states are similar to the Vermont records management manual and address the same general subject areas—records analysis, retention, storage, and disposal.[349] In addition, as with Vermont, the records management manuals of most states are not mandatory,[350] but some states have mandatory records management requirements. For example, Wisconsin has mandatory electronic record keeping requirements.[351]

---

[345] *Maryland State Archives*, *at* http://www.mdarchives.state.md.us/ (last visited Oct. 1, 2004); Maryland Department of General Services, *Records Management Division*, *at* http://www.dgs.maryland.gov/overview/logistics.htm#Link3 (last visited Oct. 1, 2004).

[346] *See, e.g.*, Council of State Historical Records Coordinators, Directory of State Archives and Records Programs, *at* http://www.coshrc.org/arc/states.htm (last visited Sept. 29, 2004).

[347] *See, e.g.*, *id.*; *see also* Commonwealth of Pennsylvania, Office of the Governor, Management Directive 210.5 (2002) (containing policy, responsibilities, and procedures for records management).

[348] *See, e.g.*, *id*; *see also* Commonwealth of Pennsylvania Historical and Museum Commission, State Records Management Manual (2004), *at* http://www.oa.state.pa.us/oac/lib/oac/manuals/m210-7.pdf (last visited Oct. 5, 2004).

[349] California Department of General Services, Records and Information Management Program, *Records Retention Handbook*, *at* http://www.pd.dgs.ca.gov/recs/rrhtoc.htm (last visited Sept. 29, 2004) (guidelines for record management); Kansas State Historical Society, Kansas State Records Management Manual (1995), *at* http://www.kshs.org/government/records/stategovt/staterecordsmanual.pdf (last visited Sept. 29, 2004) (non-mandatory encouragement for state agencies); Kansas State Historical Society, Kansas State Records Management Manual (1997), *a*t http://www.kshs.org/government/records/localgovt/localrecordsmanual.pdf (last visited Sept. 29, 2004) (non-mandatory help for local officials to fulfill recordkeeping requirements); Illinois Secretary of State, State Archives, State Records Management Manual for Illinois State Agencies, at http://www.sos.state.il.us/publications/pdf_publications/ard_pub52.pdf (last visited Sept. 29, 2004) (providing record management assistance to state agencies); Commonwealth of Pennsylvania, Historical and Museum Commission, State Records Management Manual, *at* http://sites.state.pa.us/oa/manuals/m210-7.pdf (last visited Sept. 29, 2004). *See also* Council of State Historical Records Coordinators, Directory of State Archives and Records Programs, at http://www.coshrc.org/arc/states.htm (last visited Sept. 29, 2004).

[350] *See, e.g.*, Kansas State Historical Society, State Records Management Manual (1995), *at* http://www.kshs.org/government/records/stategovt/staterecordsmanual.htm ("to encourage effective and efficient management of state government records"). *See also*, Maine State Archives, Division of Records Management Services, Guidelines for Your Records Management Program (2003); Missouri Secretary of State, Record Management Division, Missouri Records Management Program Manual, *at* http://www.sos.mo.gov/records/recmgmt/rmpm/ (last visited Oct. 3, 2004).

[351] Wisconsin Administrative Rules, Electronic Records Management—Standards and Requirements Ch. ADM 12 (2000); *see also* Wisconsin Department of Administration, Electronic Records Management: Guidance on ADM 12 (Nov. 19, 2001), *at* http://enterprise.state.wi.us/home/erecords/Primer.htm (last visited Sept. 15, 2004).

Unlike Vermont, most state archives or state records management programs have sufficient staff and funding to fulfill their statutory responsibilities and aid state and local agencies in compliance with records management requirements. For example, in Delaware, a state of similar population to Vermont, the Office of State Archives maintains a staff of forty, fourteen of which are assigned to a records management program. [352] Most states also provide extensive records management training at both the state and local level. For example, Pennsylvania offers eight different records management courses free of charge to state agency personnel.[353] Each of the classes is available at least three times a year, depending on demand.[354] Similarly, the records fees in most states exceed those charged in Vermont. For example, most states charge between $10.00 and $15.00 for copies of vital records.[355] Moreover, in many states, the record fees generated by records custodians are used exclusively for records management activities. For example, the Oregon Department of Human Services' Center for Health Statistics covers 80% of the cost of its staff and functions through the use of records fees.[356] In the 2004 session, the Vermont vital records program requested an increase in fees from $7.00 to $10.00 for copies of vital records obtained from the DH and town clerks. The General Assembly increased the fee for the DH from $7.00 to $9.50, but refused the increase for town clerks.

Although most state archives or state records management programs only serve an advisory role for state agencies, some state records management programs have significant enforcement authority over records management. For example, the Delaware Public Records Law, like Vermont law, requires all public officials and public employees to document adequately the transaction of public business, retain and protect all public records, and cooperate with the Delaware Public Archives.[357] Also like Vermont, all custodians of public records in Delaware must use material or methods approved by the Delaware Public Archives, and the archives must approve the destruction or disposal of any public records.[358] However, unlike Vermont, the records management requirements in Delaware are given teeth by a penalty provision making any violation of records management law a misdemeanor subject to fine or imprisonment.[359]

---

[352] *Delaware Public Archives, at* http://www.state.de.us/sos/dpa/contact_info.shtml (last visited Oct. 4, 2004).
[353] Pennsylvania Historical and Museum Commission, *Records Management: Courses, at* http://www.phmc.state.pa.us/bah/RecordsMgnt/TrainingSchedule.asp?secid=43 (last visited Oct. 4, 2004).
[354] Pennsylvania Historical and Museum Commission, *State Government Records Management Training Schedule, at* http://www.phmc.state.pa.us/bah/RecordsMgnt/StateGovForms/Training-04-fall.pdf (last visited Oct. 4, 2004).
[355] Memorandum from Bill Apao and Richard McCoy to Commissioner of Health Paul Jarris, regarding Legislative Changes to Title 32 (Fees for Vital Registration) attachment B (current vital records fees of the 50 states).
[356] Oregon Department of Human Services, Health Data and Vital Records, *Frequently Asked Questions About Vital Records, at* http://www.dhs.state.or.us/publichealth/chs/certif/certfaqs.cfm (last visited Cot. 26, 2004).
[357] 29 Del. Code § 504.
[358] 29 Del. Code §§ 504, 517.
[359] 29 Del. Code § 526. *See also* Cal. Gov't Code §§ 14750, 14755 (the California Records Management Act requires state agency heads to establish a records management program that complies "with the rules, regulations, standards and procedures issued by the director" of the state records management program, and the California Records Management Act prohibits a state agency from destroying or disposing of a record unless the director of the state records management program determines that the record "has no further administrative, legal, or fiscal value.).

B. Forms Management

Many commentators blame the increasing unauthorized use of personal information on the information collection practices of government and business.[360] The public generally relies on business and government to supply goods and services, and to receive these goods and services, it is often necessary to provide personal information. Businesses collect personal information for marketing purposes or for resale to other businesses. Government collects personal information for identification purposes and to provide government services. However, an individual is usually under no obligation to provide information requested by a business. In contracts, an individual often has no choice but to provide the information requested by government. Moreover, government often gives little thought to the need for the specific information collected or how such information ultimately will be used, stored, or made public.

Since state law often requires disclosure of government records to the public, government has little opportunity to prevent disclosure or misuse of personal information contained in government records. Limiting or reviewing the information solicited on government forms and applications to ensure that only necessary data is collected could help protect privacy interest while reducing the disclosure and subsequent misuse of personal information. To this end, several states have incorporated forms management into their records management programs. These programs and the forms management practices of Vermont are discussed below.

1. Vermont

BGS and the public records program do not have oversight authority over the forms or applications produced by state agencies. BGS may "devise and advise as to the use of standard books or forms for the keeping of records,"[361] and the agency does provide records management forms to state agencies and local government.[362] However, the BGS forms management authority applies only to the forms used for managing public records, not the establishment, design, and content of forms that are public records themselves. In addition, the state public records advisory board (PRAB) has the authority to advise the commissioner of BGS concerning the preservation and disposal of public records.[363] Although the PRAB does not have specific authority to conduct forms management, it has provided forms management advice on an ad hoc basis. If the PRAB sees a problem with a form that it reviews, the board may advise the relevant agency to amend the form. Nevertheless, PRAB only reviews records when requested by a state agency or the BGS. Thus, the PRAB reviews relatively few forms produced by Vermont state agencies and no municipal forms.

---

[360] *See*, *e.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1428-1430 (2001).
[361] 22 VSA § 453(6).
[362] Department of Buildings and General Services, *State Publications and Forms*, *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/forms_state.htm (last visited Oct. 5, 2004); Department of Buildings and General Service, *Municipal Publications and Forms*, *at* http://www.bgs.state.vt.us/gsc/pubrec/infospec/forms_muni.htm (last visited Oct. 5, 2004).
[363] 22 V.S.A. §§ 456, 457.

2. Other State Approaches

Several states actively manage the forms, applications, and other documents produced by state and local agencies.[364] For example, the Ohio legislature created a forms management program within its state department of administrative services.[365] The program is "designed to simplify, consolidate, or eliminate, when expedient, forms, surveys, and other documents used by state agencies."[366] The program is also required to place specific emphasis on determining the actual need for any information sought by state agencies from private business, agriculture, and local governments.[367] In furtherance of this requirement, the Ohio state forms management program aids agencies in the design of forms and the information selected for forms.[368] The state forms program also is required to establish basic design and specification criteria to standardize state forms, and all state agency forms must be registered with the program.[369] In addition, the Ohio state forms program conducts a periodic review of state agency forms to determine if they should be consolidated, eliminated, or standardized.[370]

C. Legislative Alternatives

1. Increase Public Records Funding, Staff, and Space

The Vermont state agencies with records management authority are underfunded and understaffed. Without increased funding and staff, records management in Vermont likely will not improve and existing records will continue to degrade. Such degradation of records could have significant impacts on the functioning of state government. For example, current legislative records are rapidly degrading and the General Assembly has failed to provide the necessary funding to improve and restore these records. Consequently, executive agencies and courts usurp legislative power by interpreting legislation without the aid of legislative records indicating legislative intent. The General Assembly could increase the funding for records management and could require the hiring of additional staff for the BGS Office of the Information Specialist, the Vermont State Archives, and the Department of Health vital records program. As discussed above, the OIS is staffed by one, overburdened person. Most other states have records management staff well in excess of the OIS. Increased funding and staff will allow for increased records management training and inspection of agency records management. In

[364] *See, e.g.*, California Department of General Services, *Statutory Information: Forms Management Center*, *at* http://www.osp.dgs.ca.gov/StandardForms/statinfo.htm (last visited Oct. 5, 2004); Louisiana Office of State Printing and Forms Management, *Overview*, *at* http://www.state.la.us/ospfm/ (last visited Oct. 5, 2004); Indiana Commission on Public Records, *Forms Management Division*, *at* http://www.state.in.us/icpr/webfile/formsdiv/ (last visited Oct. 5, 2004); Michigan Department of Management and Budget, *Forms Management Programs*, *at* http://www.michigan.gov/dmb/0,1607,7-150-9131_9347-27974--,00.html (last visited Oct. 5, 2004); *Missouri State Forms Management Act*, *at* http://www.oa.mo.gov/gs/form/pdfs/fm_act.pdf (last visited Oct. 5, 2004).
[365] Ohio Rev. Code § 125.92.
[366] *Id*.
[367] *Id*.
[368] Ohio Department of Administrative Services, General Services Division, State Forms Management, *Forms Analysis Series: Selecting Information Elements for a Forms*, *at* http://www.gsd.das.state.oh.us/forms/elements.pdf (last visited Oct. 13, 2004).
[369] Ohio Rev. Code § 125.93.
[370] Ohio General Services, State Forms Management Center, *State Forms Management*, *at* http://www.gsd.das.state.oh.us/forms/forms.html (last visited Oct. 5, 2004).

addition, the General Assembly could plan for or appropriate funding for the construction of additional public records storage space.

2. Reorganize Records Management Structure

The General Assembly could require the reorganization of records management authority in the state. Many states consolidate records management and historic records preservation in one agency, either an office of state archives or a stand alone records management agency. A similar consolidation in Vermont would focus the state records management program, allow for more effective use of records management resources, combine the state's records management expertise, and increase administrative efficiency. Consolidation might not be politically popular among the state agencies that currently manage public records. Consolidation likely would not need to include the vital records program of the Department of Health. The main purpose of the vital records program is to document the health of the state through the recording of births, deaths, and other vital statistics. Consequently, it is a key component of the Department of Health.

3. Require State Approval and Review of Government Forms

The General Assembly could delegate to the OIS, the PRAB, or the State Archives authority to review and approve state agency and municipal forms. The personal information required by many government forms is unnecessary to the government function which they serve. An oversight authority could prevent the use of unnecessary information. In addition, an oversight authority could develop form management standards and provide advice on creation of forms, including content and format. Delegation of this authority to OIS or the State Archives likely would require increased funding and staff. In addition, PRAB serves in an advisory function. Any delegation to PRAB would require redefinition of the board's functions and authority.

4. Authorize Increased Records Management Enforcement and Penalties

The Vermont state agencies with regulatory authority over records management in the state possess little oversight and penalty authority over state and local records custodians. The BGS OIS, the Office of State Archives, and the Department of Health vital records program collectively and individually are knowledgeable and conscientious about compliance with the state public records management requirements. However, records custodians at other state agencies and at the town level have little incentive to comply with state records management requirements. Current standards management and personnel practices are not always effective. OIS possesses some oversight authority over state and municipal records management, but the OIS is overburdened and lacks the time and staff to police agency and municipal records management adequately. As a result, most records management violations only become known when a requested record is lost or improperly disclosed. Moreover, the OIS has no enforcement or penalty authority, and only individual records custodians are subject to court-imposed penalty. BGS may withhold file cabinets and other resources if an agency is not making efforts to improve records management, but this penalty is largely symbolic and may, in fact, be counterproductive. The General Assembly could increase the penalties for improper records

management. Meaningful administrative penalties could encourage state agency heads and municipalities to devote more funding, staff, and time to proper records management. Without additional enforcement authority, records management in Vermont is unlikely to improve.

5. Require Increased Records Management Training

The General Assembly could require the OIS, State Archives, or other entity to increase the records management training available to state and municipal records custodians. In addition, the General Assembly could require mandatory training or certification for records custodians. Increased training, however, likely will require increased funding and staff.

6. Increase Recording Fees and Allocate Fees to Records Management

The General Assembly could address the lack of funding available for records management by increasing recording fees and allocating all fees or a percentage of fees to a fund to be used solely for records management. Vital records fees in Vermont currently are below those charged in other states. In addition, the $7.00 vital records fee charged by towns is less than the $9.50 fee charged by BGS and the Department of Health for vital records. Most states charge between $10.00 and $15.00 for vital records, with some states charging as high as $20.00.[371]

[371] Memorandum from Bill Apao and Richard McCoy to Commissioner of Health Paul Jarris, regarding Legislative Changes to Title 32 (Fees for Vital Registration) attachment B (current vital records fees of the 50 states); *see also* Oregon Department of Human Services, Health Data and Vital Records, *Frequently Asked Questions About Vital Records*, *at* http://www.dhs.state.or.us/publichealth/chs/certif/certfaqs.cfm (last visited Cot. 26, 2004).

Appendix A. Internet Access to Court Records

Note: The Vermont Supreme Court Advisory Committee on Public Access is currently studying public access to court records. This appendix provides a brief overview of the issue and possible legislative alternatives available to the General Assembly. This appendix and the report itself do not substitute for the findings of the Supreme Court Advisory Committee on Public Access.

Many federal and state courts recently have begun to post or consider posting court records to the Internet. Many privacy advocates, however, argue against the posting of court records because of the sensitive personal information that they contain.[1] For example, a family court record can include Social Security numbers, bank account numbers, credit card numbers, home addresses, place of employment, children's names, and dates of birth.[2] However, under federal and state law, the public generally has a right of access to court records unless the court record is sealed by the court or otherwise exempt from disclosure by state or federal law. Nevertheless, some states have adopted or are considering measures to prevent the dissemination and misuse of personal information within court records posted to the Internet.

A. Federal Right to Access Court Records

The public has a common-law right of access to court proceedings,[3] and the U.S. Supreme Court and many lower courts have extended this right of access to court records.[4] However, the common-law right of access to court records is not absolute, and access to records may be denied when the records are to be used for improper purposes, such as to promote scandal, facilitate libel, or harm a business litigant's competitive standing.[5] The decision on the right to access to court records is left to the discretion of the trial court in light of the relevant facts and circumstances.[6] In addition, as discussed in Appendix I of this report, several federal courts have interpreted U.S. Supreme Court precedent to provide for a right to inspect court records under the First Amendment to the U.S. Constitution. Again, the right of access is not

---

[1] *See*, Melissa F. Brown, *Family Court Files: A Treasure Trove for Identity Thieves?*, 55 S.C. L. Rev. 777 (2004); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1157 (2002).

[2] Melissa F. Brown, *Family Court Files: A Treasure Trove for Identity Thieves?*, 55 S.C. L. Rev. 777 (2004).

[3] Globe Newspaper Co. v. Superior Court, 448 U.S. 555, 605-606 (1980).

[4] Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978) ("It is clear that the courts of this country recognize a general right to inspect and copy public records and documents"); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1157 (2002); Kelli L. Sager, Memorandum: Leading Authority on Public/Press Right of Access (2002), *at* http://www.courtaccess.org/legalwritings/sager2002.pdf (last visited Oct. 18, 2004).

[5] *Id*. ("It is uncontested, however, that the right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes. For example, the common-law right of inspection has bowed before the power of a court to insure that its records are not used to gratify private spite or promote public scandal through the publication of the painful and sometimes disgusting details of a divorce case. Similarly, courts have refused to permit their files to serve as reservoirs of libelous statements for press consumption, or as a source of business information that might harm a litigant's competitive standing." (citations omitted)); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1156 (2002).

[6] *Id.* at 599.

absolute, and a state may limit access to a court record if it has a compelling government interest and the denial of access is narrowly tailored to meet that government interest.[7]

B. Access to Court Records Under State Law

In most states, the state public records law supersedes the federal common law right to access court records.[8] The statutory right of access to court records is narrower than the federal common-law right of access. However, court records generally are available to the public and may be posted to the Internet, albeit with some restrictions.

1. Vermont

In Vermont, the public shall have access to all case records, except for records specifically exempt from disclosure.[9] A case record is defined as any judicial branch record pertaining to a particular case or controversy.[10] In addition, some public records subject to disclosure under 1 V.S.A. §§ 316-317 become court records upon inspection and review by a court and, thus, subject to disclosure under 4 V.S.A. § 693 and court rules.[11] Thirty-three categories of court records are exempt from disclosure, including probate records, family court juvenile proceedings, discovery records, records containing the Social Security number of an individual until that number is redacted, and records with respect to jurors. [12] The court rules also provide an exemption from disclosure for any other record to which public access is prohibited,[13] including the records exempt from disclosure under the Public Records Act. In addition, a court may seal from public access a record to which the public otherwise has access or may redact information from a record to which the public has access.[14] The court must seal a record or redact information by court order, and the order shall be issued only upon a finding of good cause.[15]

The Vermont Court Rules provide for the dissemination of electronic case records. The Court defines "electronic case records" as "an electronic record pertaining to one case or controversy or to cases which have been joined by the court."[16] The public has access to electronic case records, but only to notices, decisions, and orders of the court and not to electronic filings or scanned images of court records.[17] Moreover, access is provided by the Court Administrator only on a case-by-case basis and subject to limitations on access to personal

[7] *Id*. at 607; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1202 (2002).
[8] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1156 (2002).
[9] 4 V.S.A. § 693; Vt. Ct. Rules, Rules for Public Access to Court Records, Rule 6. See also Herald Ass'n v. Judicial Conduct Board, 149 Vt. 233, 241 n.7 (questioning whether the Public Records Act applies to court or judicial records.)
[10] Vt. Ct. Rules, Rules for Public Access to Court Records, Rule 3.
[11] *See* State v. Tallman, 148 Vt. 465, 472 (1987).
[12] Vt. Ct. Rules, Rules for Public Access to Court Records, Rule 6.
[13] *Id*.
[14] Vt. Ct. Rules. Rules for Public Access to Court Records, Rule 7.
[15] *Id*.
[16] Vt. Ct. Rules, Rules Governing the Dissemination of Electronic Case Records, Rule 1.
[17] Vt. Ct. Rules, Rules Governing the Dissemination of Electronic Case Records, Rule 3.

information contained in the record.[18] The public does not have access to Social Security numbers, street addresses, telephone numbers, and any personal identification numbers, including driver's license numbers and account numbers.[19] The rules also provide that court records may be made available online.[20] In addition, under the Vermont Rules of Civil Procedure, Criminal Procedure, and Probate Procedure, Social Security numbers must be redacted from any documents filed with a court unless the court specifically requests the Social Security number.[21]

The court may disclose court records not available to the public to state or local government or nonprofit agencies, known as public purpose agencies, whose principal function is to do research or provide services to the public.[22] A public purpose agency's access to otherwise exempt information and case records is contingent on a data dissemination contract under which the public purpose agency must agree to use the information only for specified purposes and to maintain the confidentiality of third parties. However, beyond requiring termination of a data dissemination contract, neither the rules for access to court records nor the rules for the dissemination of electronic records address the misuse of otherwise exempt information or the improper dissemination of court records by a public purpose agency or other entity.

2. Other State Approaches

Many states have adopted policies or rules similar to the Vermont Court Rules governing dissemination of electronic case records.[23] Each state generally provides that court records are open records subject to disclosure unless otherwise sealed or exempt. In addition, most states attempt to prevent unnecessary disclosure of personal information, but the approaches used to protect personal information vary.

A recent Washington state court rule provides that the public shall have access to all court records except those restricted by federal law, state law, court rule, or court order.[24] The Washington rule provides approximately 70 exemptions from disclosure, and the Washington courts can seal records for cause.[25] To prevent disclosure of personal information, the rule requires parties to a proceeding or their attorney to redact from court records Social Security numbers, names of minor children, financial account numbers, and driver's license numbers.[26]

---

[18] *Id.*
[19] *Id.*
[20] Vt. Ct. Rules, Rules Governing the Dissemination of Electronic Case Records, Rule 3.
[21] Vermont Rule of Civil Procedure 5(g); Vermont Rules of Criminal Procedure 49(c); Vermont Rules of Probate Procedure 5(h).
[22] Vt. Ct. Rules, Rules Governing the Dissemination of Electronic Case Records, Rules 6, 1.
[23] Administrative Office of the Illinois Courts, Electronic Access Policy for Circuit Court Records of the Illinois Courts (2003); Iowa Judicial Branch, *Frequently Asked Questions: Open Records*, *at* http://www.judicial.state.ia.us/faq/open.asp (last visited Oct. 20, 2004). *See also* Electronic Privacy Information Center, *Privacy and Public Records*, *at* http://www.epic.org/privacy/publicrecords/ (last visited Oct. 20, 2004); First Amendment Center, *Electronic Access to Public Records*, *at* http://www.firstamendmentcenter.org/analysis.aspx?id=6563 (last visited Oct. 20, 2004).
[24] Washington Court Rules, GR 31 Access to Court Records (Oct. 2004).
[25] Wash. Rev. Code § 42.17.310.
[26] Washington Court Rules, GR 31 Access to Court Records (Oct. 2004).

The onus is specifically on the party to redact the information, but the court may allow redaction after filing.[27]

In California, all court records must be made available to the public in some form, whether electronic or paper, except if they are sealed by the court or made confidential by law.[28] However, electronic access to a court record is a case-by-case determination by the relevant court,[29] and a court may condition access to electronic records on the user's consent to court instructions and monitoring.[30] Moreover, court records of juvenile, guardianship, mental health, or civil harassment proceedings are only available electronically at a courthouse and not through the Internet.[31] Generally, electronic records of criminal proceedings are only available at a courthouse, but if the demand for an individual criminal case record is high, a court can make an electronic record available remotely after the redaction of personal information.[32]

In Maryland, court records are presumed to be open to the public unless otherwise exempted or sealed.[33] The Maryland court rules, however, include several provisions restricting access to court records or to specific information within court records.[34] Among these many exemptions is one prohibiting the disclosure of any part of a Social Security number other than the last four digits.[35] In addition, a court record available in an electronic format must be open to the public to the same extent that the record would be available in paper form.[36] The rules do provide the information officer of each court some discretion in determining if, how, and when electronic access shall be available.[37]

In some states, little restriction is placed on electronic access to court records. For example, Iowa provides free Internet access to all "public access records" subject to disclosure[38] with limited exemptions for certain court records, including juvenile proceedings, domestic abuse cases, divorce proceedings, and cases involving sensitive medical or substance abuse information.[39] All non-exempt records are available over the Internet free of charge and do not require redaction of personal information.

---

[27] *Id.*
[28] Cal. Rules of Court Rule 2073.
[29] *Id.*
[30] Cal. Rules of Court Rule 2074.
[31] *Id.*
[32] Cal. Rules of Court Rule 2073.5.
[33] Md. Court Rules, Rule 16-1002(general policy).
[34] Md. Court Rules, Rules 16-1005 to 16-1007.
[35] Md. Court Rules, Rule 16-1007.
[36] Md. Court Rules, Rule 16-1008.
[37] *Id.*
[38] Iowa Court Information Systems, *Iowa Courts Online*, *at* http://www.judicial.state.ia.us/online_records/ (last visited Oct. 20, 2004).
[39] Iowa Judicial Branch, *Frequently Asked Questions: Open Records*, *at* http://www.judicial.state.ia.us/faq/open.asp (last visited Oct. 20, 2004).

C. Legislative Alternatives

1. Exempt Additional Court Records from Electronic Disclosure

The current Vermont Court Rules on electronic access to court records and the privacy protection they offer compare favorably to similar rules in other states. The General Assembly could extend the privacy protection offered by the rules by exempting from disclosure other subsets of information such as divorce proceedings or additional family court proceedings. Currently, only family court proceedings involving a juvenile or a DNA analysis are exempt.

2. Require Determination by Courts For Dissemination of Court Records

Currently, the Vermont rules provide that the Court Administrator shall make case-by-case determinations regarding the dissemination of electronic court records. To protect privacy further, the General Assembly could require provisions similar to those used in California where a court and not a court administrator must make a case-by-case determination regarding the dissemination of a court record and may impose restrictions on the use of any disclosed court records. Such a provision may not be necessary in Vermont, considering the significant number of exemptions and privacy protections afforded by Vermont Court rules. A case-by-case determination could also increase the burden on courts and could delay dissemination of records that do not require privacy protection.

3. Provide Access to Electronic Court Records Only at the Courthouse

The General Assembly could provide that all or certain types of court records shall be available electronically only at a courthouse. As discussed above, California has a similar rule for certain records, including juvenile and mental health records. This requirement would restrict access to court records, would allow for supervision of access, and would prevent misuse of personal information within the records. However, such a requirement would be difficult to impose in Vermont. Adequate staff and computer resources would need to be allocated to each courthouse, and the necessary funding probably is not available.

4. Require Parties to Proceedings to Redact Unnecessary Personal Information

Currently, the Vermont Rules of Civil, Criminal, and Probate Procedure require the redaction of Social Security numbers included in papers filed with a court. To further shift some of the burden on courts and court administrative officers regarding the redaction of personal information in court records, the General Assembly could require parties to a court proceeding to redact additional unnecessary personal information in certain court filings, such as names of minor children, financial account information, and driver's license numbers. As discussed above, Washington state currently requires such practices for all public records. However, redaction by parties to a court proceeding could lead to the deletion or redaction of information essential to a proceeding.

Appendix B. Federal Public Records Law

State records management requirements often are mandated by federal statute or case law. In fact, recent federal legislation will significantly change records management requirements in Vermont. Many other federal statutes address privacy concerns related to public records management. In addition, federal case law may set constitutional limits on state public records management. As a reference, this section reviews the recent records management requirements enacted by the U.S. Congress and other federal statutes and case law that impact state records management.

A. Intelligence Reform and Terrorism Prevention Act of 2004

On December 7, the U.S. House of Representative approved the conference committee report to the Intelligence Reform and Terrorism Prevention Act of 2004. One day later, December 8, 2004, the U.S. Senate also approved the conference committee report, thereby clearing the measure for the President. The act includes requirements intended to improve the security of personal identifying information. These requirements will apply to all states and will significantly alter records management in Vermont. The records management provisions in the act are described below.

1. Drivers' Licenses

The 9/11 Commission Report recommended that the federal government set standards for the issuance of birth certificates and sources of identification, such as drivers' licenses. In making the recommendation, the Commission specifically noted the rise in the occurrence of identity fraud and the use of identification to verify the identity of terrorists. The Intelligence Reform and Terrorism Prevention Act requires states to meet minimum standards for drivers' license.[1] The specific standards are to be set by rule by the Secretary of Transportation in consultation with the Secretary of Homeland Security. The standards must provide for documentation of identity, verifiability of documents to obtain a driver's license, information to be included on a license, and security standards to prevent tampering, alteration, or counterfeiting.[2] The standards shall be issued within 18 months of enactment, and the Secretary of Transportation shall set the date by which each state must comply with the standards.[3] The act includes a grant program to aid state compliance with the standards. In addition, the act prohibits the display of Social Security numbers on any driver's license issued or reissued one year after the enactment of the act.[4]

2. Birth Certificates

The Intelligence Reform and Terrorism Prevention Act of 2004 directs the Secretary of Health and Human Services to establish by rule within one year of enactment minimum

[1] Pub. L. No. 108-458, 118 Stat/ 3638 § 7212, 108th Cong. (2004).
[2] *Id.*
[3] *Id.*
[4] *Id.* at § 7214.

standards for birth certificates used by federal agencies.[5] The standards shall require certification of a birth certificate by a state, use of safety paper or other secure measure, and other features to prevent tampering or otherwise duplicating the certificate.[6] The standards shall also establish requirements for proof and verification of identity as a condition of issuance of a birth certificate, with additional security measures for the issuance of a birth certificate for a person who is not an applicant.[7] The Act further requires standards for the processing of birth certificate applications to prevent fraud.[8] Within two years of issuance of the rule by the U.S. Department of Health, no federal agency shall accept a birth certificate for any official purpose unless it conforms to the minimum federal standards.[9] Grants will be available to states from the Secretary of Heath and Human Services to assist in conforming with the federal standards.[10]

3. Social Security Cards

As discussed above, the Intelligence Reform and Terrorism Prevention Act prohibits the display of Social Security numbers on drivers' license. In addition, the Act restricts the issuance of multiple Social Security cards and requires the Commissioner of Social Security to issue security requirements to prevent the counterfeiting, tampering, or alteration of Social Security cards.[11] The Commissioner shall also study the most efficient way for ensuring the integrity of issuing Social Security numbers at birth.[12]

B. Federal Statutes

The head of each federal agency is required to make and preserve records containing adequate and proper documentation of the agency's organization, functions, policies, decisions, procedures, and transactions in order to protect the legal and financial rights of the government and persons affected by the agency's activities.[13] Consequently, the federal government generates a large volume of public records, and several federal statutes regulate the privacy, electronic access, and distribution of such records. Among these statutes are the Federal Records Act, the Privacy Act of 1974, the Electronic Communications Privacy Act (EPCA), the Freedom of Information Act (FOIA), the Health Insurance Portability and Accountability Act, the Family Educational Right to Privacy Act, and the Patriot Act. These laws purportedly limit the disclosure and distribution of public records and private information within such records, but exemptions within these laws often enervate the protections they supposedly offer.[14]

---

[5] *Id.* at § 7211.
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *Id.*
[10] *Id*.
[11] *Id*. § 7213.
[12] *Id.*
[13] 44 U.S.C. § 3101.
[14] *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berk. Tech. L.J. 1085, 1112-1115 (2002); Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. Marshall J. Computer & Info. L. 529 (1998).

1. Federal Records Act

The Federal Records Act requires federal agency heads to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[15] Federal agency heads must also establish safeguards against the removal or loss of records,[16] and records may only be destroyed in accordance with the requirements of the Federal Records Act.[17] "Records" are defined as "[a]ll books, papers, maps, photographs, machine readable materials, or other documental materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency."[18]

2. Privacy Act of 1974

The Privacy Act of 1974 regulates the collection of personal information by the federal government and prohibits federal agencies from disclosing any record pertaining to an individual to another person or to another government agency without the consent of the individual to which the record pertains.[19] However, the prohibition on disclosure is rendered powerless by 12 exemptions, including disclosure for routine agency use or disclosure required under FOIA.[20] Federal agencies interpret the routine use exemption expansively and use it to justify disclosure of a record without the individual's consent.[21]

The Privacy Act also prohibits a local, state, or federal government agency from compelling an individual to submit a Social Security number unless disclosure is authorized by Congress, required by federal statute, or required by a records system in place before 1975.[22] If a Social Security number is requested by a federal, state, or local government agency, the agency must inform the individual whether the disclosure is mandatory or voluntary, by what authority the number is solicited, and for what use the agency intends to utilize the number.[23] These requirements could have been a significant tool in the protection of personal and information privacy, but since 1975, Congress has authorized the use of Social Security numbers so often that the prohibition has lost most of its gravitas. Among other uses, Congress now requires or authorizes use of Social Security numbers to receive Medicare or Medicaid, to receive a student loan, to receive welfare benefits, to collect child support, to complete an employment

[15] 44 U.S.C. § 3101.
[16] 44 U.S.C. § 3105.
[17] 44 U.S.C. § 3314.
[18] 44 U.S.C. § 3301.
[19] 5 U.S.C. § 552a(b).
[20] *Id*. at § 552a(b)(1)-(12).
[21] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berk. Tech. L.J. 1085, 1113 (2002), *citing* Matthew Bunker et al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 Fla. St. U. L. Rev. 543, 582 (1993) (discussing the routine use exemption and agency use of the exemption to avoid consent requirements for such uses as academic research). "Routine use" of a public record is defined as "the use of such record for a purpose which is compatible for which it was collected." 5 U.S.C. § 552a(7).
[22] Pub. L. No. 93-579, § 7, 88 Stat. 1896 (Section 7 of the Privacy Act of 1974 was not codified and generally appears as a note to 5 U.S.C. § 552a).
[23] *Id*.

application, to complete a tax return, to apply for a driver's licenses, and to apply for loans.[24] In fact, the use of Social Security numbers is so prevalent that the Privacy Act's disclosure requirements are largely ignored. Nevertheless, a litigant can still bring a Privacy Act action to invalidate an unauthorized use of a Social Security number or to require agency disclosure of the purpose and use of the number.[25]

3. The Electronic Communications Privacy Act (ECPA)

When enacted, ECPA prohibited any person, including federal and state government agencies, from intercepting, using, or disclosing any information obtained from private electronic communications such as e-mail.[26] ECPA, like the Privacy Act of 1974, also contains several exemptions that weaken its efficacy. Under ECPA, a communication is not protected if one party to the communication consents to its interception or if an electronic service provider—such as an Internet service provider—uses an electronic communication for activity that is a necessary incident of the rendition of service.[27] ECPA also only protects the content of the communication, not the circumstances of the communications, such as the identity of the recipient or sender.[28] In addition, the Patriot Act of 2001 included several exemptions to ECPA for government activity. The Patriot Act amendments are discussed below in subdivision 7 of this section.

4. Freedom of Information Act (FOIA)

FOIA is the federal law that requires all federal agencies to make their records available to the public, unless a specific exemption applies.[29] One such exemption is 5 U.S.C. § 552(b)(6), which prohibits disclosure of a public record that includes "personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." In determining whether disclosure of a public record constitutes an invasion of personal privacy, the U.S. Supreme Court held that "a court must balance the public interest in disclosure against the interest Congress intended the exemption to protect."[30] Applying the test, federal courts have interpreted the exemption to apply to Social Security numbers and other similar personal information, such as home addresses, included in federal government records.[31] However, the exemption applies only to the personal information contained within the public

[24] Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. Marshall J. Computer & Info. L. 529, 554 (1998).
[25] *Id.*
[26] 18 U.S.C. §§ 2511-2520; *see also* Lin, *supra* note 8, at 1113.
[27] 18 U.S.C. § 2512(2)(a), (c).
[28] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berk. Tech. L.J. 1085, 1113-1114 (2002).
[29] 5 U.S.C. § 552. Each federal agency shall make available for public inspection any records that an individual requests and reasonably describes. *Id.* § 552(a)(3)(A).
[30] United States Department of Defense v. Federal Labor Relations Authority, 510 U.S. 487, 495 (1994), *citing* Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 776 (1989) (addressing the FOIA exemption under 5 U.S.C. 552(b)(7)(C) for "records or information compiled for law enforcement purposes . . . [which] could reasonably be expected to constitute an unwarranted invasion of personal privacy.").
[31] *See* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. Marshall J. Computer & Info. L. 529, 555-556 (1998).

record. If feasible, FOIA requires the personal information to be deleted or redacted,[32] but any additional information in the record is disclosed as is the "amount of information deleted."[33] In addition, FOIA only applies to federal records disclosed upon citizen request. FOIA does not apply to federal agency or intra-agency review or communications.[34] Thus, the FOIA exemptions that attempt to protect against unwarranted invasions of personal privacy are limited in scope and applicability.

5. Health Insurance Portability and Accountability Act (HIPAA)

In 1996, the U.S. Congress enacted HIPAA to address waste, fraud, and abuse in the health insurance and health care industries.[35] In 2002, the U.S. Department of Health and Human Services (HHS) issued a final rule regarding the exchange of health information and the protection of personal information within a medical file.[36] The HHS rule is intended to protect an individual's personal, medical information from unwarranted or unnecessary disclosure.[37] To achieve this goal, the rule defines when a "covered entity" may disclose individually identifiable health information, which the rule refers to as protected health information (PHI).[38] Among other information, PHI includes a patient's name, address, birth date, and Social Security number.[39] A covered entity is a health plan, health care clearinghouse, or health care provider.[40] State agencies must comply with HIPAA when acting as a covered entity. For example, government health plans and government hospitals are covered entities, but food stamp programs and certain community-related health programs are not.[41]

---

[32] 5 U.S.C. § 552(b).
[33] *Id.*
[34] *Id.*
[35] Pub. L. No. 104-191, 110 Stat. 1936, Aug. 21, 1996.
[36] U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004). HIPAA required HHS to issue the rules if Congress had not enacted privacy legislation within three years of HIPAA's enactment. *See*, Pub. L. No. 104-191 § 264, 110 Stat. 1936, Aug. 21, 1996.
[37] *Id.*
[38] "Individually identifiable health information" is defined in 45 C.F.R. § 164.501 as health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

[39] *Id.*
[40] HIPAA does not apply to entities that do not fall within the definition of covered entity. For example, the Kentucky Attorney General has interpreted HIPAA as not to apply to law enforcement agencies because they are not health plans, health care clearinghouses, or health care providers. Opinion of the Kentucky Attorney General, No. 04-ORD-143 (Aug. 24, 2004). Thus, HIPAA likely would not apply to a state agency with little or no participation in health care. Nevertheless, a state may prohibit the disclosure of personal identifying medical information in state or local public records. For instance, 1 V.S.A. § 317(c)(7) prohibits state and local agencies from disclosing personal medical information contained in public records.
[41] U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004).

A covered entity may not disclose PHI unless the rule permits disclosure, the rule requires disclosure, or the individual authorizes disclosure.[42] The rule requires disclosure when an individual or a representative requests his or her own PHI or when HHS is investigating or reviewing an enforcement action.[43] The rule permits disclosure of PHI in six instances: (1) to the individual; (2) for the covered entity's treatment, payment, and health care operations; (3) if an individual is notified that the covered entity plans to disclose the information, and the individual has the chance to agree or object; (4) as incident to an otherwise permitted use and disclosure; (5) for certain public interests and benefits, such as preventing the spread of disease; and (6) for limited purposes of research, public health, or health care operations.[44]

The HIPAA rule includes numerous exemptions to the limitations on the disclosure of PHI. For instance, covered entities may disclose PHI to "business associates,"[45] which are persons or organizations that perform certain functions for the covered entity, including claims processing, data analysis, and billing.[46] The HIPAA rule requires a covered entity to include in any contract with a business associate conditions that prohibit subsequent disclosure of PHI to another party.[47] However, the rule provides no civil penalties for business associates that violate contracts and disclose PHI to others.[48] Only the covered entity is penalized, and only if the disclosed PHI is traced back to that entity.[49] Moreover, the HIPAA rule is silent regarding an individual's ability to bring a civil suit against a covered entity or business associate that illegally discloses PHI.[50] Consequently, courts may not allow civil lawsuits for wrongful disclosure or distribution of PHI.[51] Criminal penalties do exist for the knowing disclosure of PHI, but, currently, only one person has been convicted of violating the HIPAA rule.[52]

---

[42] 45 C.F.R. § 164.502(a)(1).
[43] *Id.* § 164.502(a)(2); *see also* U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004).
[44] *Id.* part 164, §§ 164.502(a)(1), 164.506, 164.508, 164.510, 164.512, and 164.514.
[45] 45 C.F.R. § 502(e).
[46] *See*, *id*.; U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004).
[47] 45 C.F.R. §§ 502(e), 504(e).
[48] HHS may impose civil money penalties on a covered entity of $100.00 per failure to comply with the disclosure rules. Pub. L. No. 104-191, 110 Stat. 1936, Aug. 21, 1996 (codified at 42 U.S.C. § 1320d-5). The penalty may not exceed $25,000 per year for multiple violations. HHS may not impose a penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it learned of the violation. U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004).
[49] Pub. L. No. 104-191: 42 U.S.C. § 1320d-5; *see also*, James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. Rev. Mich. State. U. Det. C.L. 855, 881 (2002).
[50] James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. Rev. Mich. State. U. Det. C.L. 855, 881 (2002).
[51] *Id.*
[52] United States v. Gibson, No. Cr04-0374 RSM (W.D. Wash Aug. 19, 2004), *at* http://www.usdoj.gov/usao/waw/press_room/2004/aug/pdf_files/cr04_0374rsm_plea.pdf (last visited Sept. 20, 2004).

In addition, although the HIPAA rule purportedly prohibits marketing based on PHI,[53] the rule exempts certain marketing activities. Specifically, the rule allows marketing concerning health care products or services, providers, health plans, treatment of the individual, case management or care coordination for the individual, and alternative treatments, therapies, or health care providers.[54] Disclosure of PHI can be made to these marketers without an individual's consent. Moreover, the rule does not prohibit the exempted marketers from subsequently distributing PHI to other marketers.[55] The rule requires marketing materials to identify that a covered entity is receiving money for the marketer's right to distribute the information,[56] and the material must provide the recipient the opportunity to "opt out" from receiving future marketing material.[57] Privacy advocates argue that these "consumer protections" are inadequate because the individual's PHI has already been distributed and, once distributed, is susceptible to misuse.[58]

6. Family Educational Right to Privacy Act

The Family Educational Right to Privacy Act (FERPA)[59] regulates the disclosure and distribution of student education records.[60] The law applies to any educational agency or institution, including state schools and agencies, receiving funds from any program administered by the Secretary of the U.S. Department of Education.[61] The purpose of FERPA is to protect the privacy of students and parents.[62] The law requires schools or other educational institutions to receive written permission from a parent or an eligible student[63] before disclosing any part of a student's educational records.[64] In addition, parents and eligible students may inspect and

---

[53] 45 C.F.R. § 154.514(e).
[54] *Id*.; *see also* U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule (2003), *at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Sept. 16, 2004).
[55] James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. Rev. Mich. State. U. Det. C.L. 855, 872 (2002).
[56] 45 C.F.R. § 164.514(e)(3).
[57] *Id*.
[58] *See* James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. Rev. Mich. State. U. Det. C.L. 855, 872 (2002).
[59] 20 U.S.C. § 1232g (FERPA is also commonly referred to as the Buckley Amendment).
[60] "Education records" are defined as records that are "(1) Directly related to a student; and (2) Maintained by an educational agency or institution or by a party acting for the agency or institution." 20 U.S.C. § 1232g(a)(3); 35 C.F.R. § 99.3. Education records do not include: records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record; records of the law enforcement unit of an educational agency or institution; records relating to an individual who is employed by an educational agency or institution, that are made and maintained in the normal course of business, relate exclusively to the individual in that individual's capacity as an employee, and are not available for use for any other purpose; records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; made, maintained, or used only in connection with treatment of the student; and disclosed only to individuals providing the treatment." 20 U.S.C. § 1232g(a)(4); 35 C.F.R. § 99.3.
[61] 35 C.F.R. § 99.1(a).
[62] 35 C.F.R. § 99.2.
[63] An "eligible student" means a student who has reached 18 years of age or is attending an institution of postsecondary education. 35 C.F.R. § 99.3.
[64] 35 C.F.R. §§ 99.7, 99.30. Under a recent amendment, the written permission to disclose can be satisfied by an electronic record indicating consent. 35 C.F.R. § 99.30(d).

review the educational records of a student maintained by an educational institution or state educational agency.[65] The parent or eligible student also may request that inaccurate or misleading information in a student's educational records be amended.[66] If the agency or institution does not amend the records, the parent or eligible student has a right to a formal hearing, and if the hearing does not result in an amendment to the record, the parent or student may include in the student's record a statement regarding the contested information.[67]

FERPA does allow disclosure of personal information without the consent of a parent or student. Disclosure is allowed without consent in twelve instances: (1) to other school officials; (2) to other schools where the student is enrolled; (3) to authorized federal and state enforcement or educational authorities; (4) to testing organizations; (5) to parties concerning financial aid applied for by the student; (6) to accrediting organizations; (7) to comply with a judicial order or subpoena; (8) to appropriate officials in a health care emergency; (9) to a victim of a crime of violence of a non-forcible sex offense when the information regards the results of a disciplinary rule; (10) to the parents of a student at a postsecondary school regarding the violation of a federal, state, local, or institutional drug or alcohol law or policy; (11) to state and local officials to whom state law required disclosure prior to 1974; and (12) when the information is designated directory information by an educational agency or institution.[68] An educational agency or institution shall maintain a record of each request for and subsequent disclosure of personal information.[69] Moreover, when personal information is disclosed it is done so on the condition the party receiving the information will not disclose that information to any other party without the consent of the parent or eligible student.[70]

A parent or student who believes personal information has been disclosed or redisclosed improperly may file a written complaint with the Family Policy Compliance Office of the U.S. Department of Education.[71] If the Family Policy Compliance Office finds that a violation has occurred, the office issues a statement to the relevant education agency or institution setting forth the steps it must take to remedy the violation and comply with FERPA.[72] If the educational agency or institution does not comply, the Secretary of Education may withhold further federal payments, issue cease and desist orders, or terminate the agency's or institution's ability to receive federal funding.[73]

---

[65] 35 C.F.R. § 99.10.
[66] 35 C.F.R. § 99.20.
[67] 35 C.F.R. § 99.21.
[68] "Directory information" means information contained in an educational record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes names, address, telephone number, e-mail address, photograph, date of birth, grade level, and enrollment status. 35 C.F.R. § 99.3. A parent or eligible student has the right to refuse to let the agency or institution to disclose any or all of this information. 35 C.F.R. § 99.37. Nevertheless, an educational institution has the right to disclose directory information on former students without giving the student notice and an opportunity to refuse such disclosure. *Id.*
[69] 35 C.F.R. § 99.32.
[70] 35 C.F.R. § 99.33.
[71] 35 C.F.R. § 99.62. A complaint must be submitted within 180 days of the alleged violation and must include sufficient facts to give reasonable cause to believe a violation of FERPA has occurred. 35 C.F.R. § 99.64.
[72] 35 C.F.R. § 99.66.
[73] 35 C.F.R. § 99.67.

FERPA does not provide for a private cause of action to enforce the requirements of the act, and courts have refused to recognize such a right.[74] Similarly, FERPA does not provide for damages to remedy a violation. Until 2002, federal courts were split on whether a parent or eligible student could seek damages for a violation of FERPA under 42 U.S.C. § 1983 of the civil rights act.[75] In 2002, the U.S. Supreme Court held in *Gonzaga University v. Doe*[76] that damages are not available under § 1983 for a FERPA violation because the act specifically does not provide for a personal right of action or a personal right to enforce § 1983.[77] Commentators criticized the decision and argue that it encourages educational institutions to delay strict compliance with FERPA since an institution in violation is given an opportunity to fix the problem prior to any loss of educational funding.[78]

7. Patriot Act of 2001

In 2001, Congress passed the Patriot Act to combat terrorism in the United States and around the world.[79] Several sections of the Patriot Act increased the investigatory authority of law enforcement. This increased investigatory authority, however, arguably leads to reduced privacy protection, especially with regard to electronic communication. For example, the Patriot Act amended the Electronic Communications Privacy Act (ECPA), discussed above, to allow the interception of electronic communications, including e-mail, when such interception may provide or has provided evidence relating to terrorism or the use of chemical weapons.[80] The Patriot Act also amended ECPA to amend the type of tracing devices authorized for use by law enforcement in order to include tracing of electronic communications such as e-mail and Internet use.[81]

In addition to the amendments to ECPA, the Patriot Act authorized the FBI to use national security letters (NSLs) to compel communications companies, such as telephone companies or Internet service providers, to produce customer information when such information

---

[74] Ralph D. Mawdsley, *Limiting the Reach of FERPA Into the Classroom: Owasso School District v. Falvo*, 165 Ed. Law. Rep. 1, 3 (2002), *citing* Frazier v. Fairhaven Sch. Committee, 122 F.Supp.2d 104 (D. Mass. 2000); Hatfield v. East Grand Rapids Pub. Schs., 960 F.Supp. 1259 (W.D. Mich. 1997); Belanger v. Nashua, N.H., Sch. Bd., 856 F.Supp. 40 (D.N.H. 1994).

[75] *Id*., *citing*, as cases supporting a § 1983 claim for damages, Tarka v. Cunningham, 917 F.2d 890 (5th Cir. 1990); Fay v. South Colonie Cent. Sch. Dist., 802 F.2d 21 (2d Cir. 1986); Achman v. Chisago Lakes Indep. Sch. Dist. 45 F. Supp.2d 664 (D. Minn. 1994); Doe v. Know County Bd. Of Educ., 918 F. Supp. 181 (E.D. Ky. 1996); Maynard v. Greater Hoyt Sch. Dist. 876 F. Supp. 1104 (D.S.D. 1995); Belanger v. Nashua N.H., Sch. Dist., 856 F.Supp. 40 (D.N.H. 1994); Norwood v. Slammons, 788 F.Supp. 1010 (E.D. Pa. 1996); and, as cases denying a § 1983 claim for damages, Gundlach v. Teinstein, 924 F.Supp. 684 (E.D. Pa. 1996); Norris v. Board of Educ. of Greenwood County Sch. Corp., 797 F.Supp. 1452 (S.D. Ind. 1992).

[76] 536 U.S. 273 (2002).

[77] *Id*. at 276.

[78] 20 U.S.C. § 1232g(f); 34 C.F.R. §§ 99.66(c)(2), 99.67; *see also* D. Martin Warf, *Loose Lips Won't Sink Ships: Federal Education Rights to Privacy Act After Gonzaga v. Doe*, 25 Campbell L. Rev. 201 (2003); Britta L. Hyllengren, *Constitutional Law—Violations of Family Educational Rights and Privacy Act Create No Personal Rights Under § 1983—Gonzaga University v. Doe*, 37 Suffolk U. L Rev. 563 (2004).

[79] U.S. Congress, Thomas Legislative Information on the Internet, *H.R. 3162: Bill Summary and Status*, *at* http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162: (last visited Oct. 5, 2004).

[80] Pub. Law No. 107-56 § 201, 115 Stat. 272 (2001) (codified at 18 U.S.C. § 2516(q)).

[81] Pub. Law No. 107-56 § 216, 115 Stat. 272 (2001) (codified at 18 U.S.C. §§ 3121-3127).

is relevant to an authorized terrorism or intelligence investigation.[82] The information that must be disclosed includes name, address, and billing records. Communication companies are also prohibited from disclosing the fact that the FBI has sought or obtained information regarding an individual.[83]

Privacy and civil liberties advocates argue that these amendments and other provisions of the Patriot Act violate the First and Fourth Amendments to the U.S. Constitution or infringe on the individual right to privacy. Recently, a federal court in New York agreed with these arguments and enjoined the FBI from issuing NSLs to communications companies and from enforcing the nondisclosure provision.[84] However, the New York court opinion is of limited national application, and the government is almost certain to appeal the decision. In addition, other litigation stemming from the Patriot Act is likely, and there is no guarantee that other courts will agree with the New York court. Thus, if the Patriot Act is reauthorized by Congress in 2005, litigation surrounding the act will continue until addressed by the U.S. Supreme Court.

C. Federal Case Law

1. Right to Inspect Public Records

The U.S. Supreme Court has recognized the common-law right to inspect and copy public records.[85] The Court stated that the justification for the right to inspect public records is the need for government accountability.[86] However, the right to access, especially with regard to court records, is not absolute, and access to records may be denied when the records are to be used for improper purposes, such as to promote scandal or facilitate libel.[87] For court records, the decision on the right of access is left to the discretion of the court.[88] For other public records, state public records law generally supersedes the common law right to access.

In addition to the common law right of access, several federal courts have interpreted U.S. Supreme Court precedent to provide for a First Amendment right to inspect court records. In the 1982 case *Globe Newspaper Co. v. Superior Court*, the Court articulated a test to determine whether a judicial proceeding is open to the public under the First Amendment.[89] Applying the test, the Court held that the public has a right to access criminal trials in order to participate in and serve as a check on the judicial process, but such a right was not absolute. [90] A state may limit access if it has a compelling government interest, and the denial of access is

[82] Pub. Law No. 107-56 § 505(a), 115 Stat. 365 (2001) (codified at 18 U.S.C. §§ 2709).
[83] 18 U.S.C. § 2709(c).
[84] Doe v. Ashcroft, 2004 WL 2185571 (S.D.N.Y. Sep. 28, 2004).
[85] Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978) ("It is clear that the courts of this country recognize a general right to inspect and copy public records and documents"); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1157 (2002).
[86] *Id.* at 598 ("The interest necessary to support the issuance of a writ compelling access [to public records] has been found . . . in the citizen's desire to keep a watchful eye on the workings of public agencies and in a newspaper publisher's intention to publish information concerning the operation of government.").
[87] *Id.*; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1156 (2002).
[88] *Id.* at 599.
[89] Globe Newspaper Co. v. Superior Court, 448 U.S. 555, 605-606 (1980).
[90] *Id*. at 607.

narrowly tailored to meet that government interest.[91] Following *Globe*, the Court found that the right of access extended to pretrial hearings and jury selection.[92] Other lower federal courts applying the *Globe* test extended the right of access to pretrial suppression, due process, entrapment,[93] and, ultimately, court documents and records.[94] The *Globe* test and the First Amendment right of access to court records has not been extended to other types of public records, but legal commentators argue that the rationale behind *Globe* logically extends to all public records, and that such a right is necessary to ensure unfettered communication regarding government and its operations.[95]

[91] *Id*. at 607; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1202 (2002).
[92] *See* Press-Enterprise Co. v. Superior Court, 464 U.S. 501 (1984) (Press-Enterprise I); Press-Enterprise Co. v. Superior Court, 478 U.S. 1 (1986) (Press-Enterprise II); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1202 (2002).
[93] United States v. Criden, 675 F.2d 550, 557 (3d Cir. 1982); United States v. Chagra, 701 F.2d 354, 363 (5th Cir. 1983); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1202 (2002).
[94] United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997); Littlejohn v. BIC Corp F.2d 673, 678 (3d Cir. 1988); *but see* Lanphere & Urbaniak v. Colorado, 21 F.3d 1508, 1512 (10th Cir. 1994) ("there is no general First Amendment right in the public to access criminal justice records."); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1203-04 (2002).
[95] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1203-04 (2002).